НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

ІНСТИТУТ МОДЕРНІЗАЦІЇ ЗМІСТУ ОСВІТИ МІНІСТЕРСТВА ОСВІТИ І НАУКИ УКРАЇНИ

АКТУАЛЬНІ ПРОБЛЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ

Збірник матеріалів
XIV Всеукраїнської науково-практичної конференції

(Київ, 30 березня 2023 року)

Електронне видання

Київ - 2023

УДК 351.746.1

Рекомендовано до друку Навчально-науковим інститутом інформаційної безпеки та стратегічних комунікацій Національної академії СБ України
(протокол від 27.03.2023 року № 7)

Актуальні проблеми управління інформаційною безпекою держави : зб. матер. всеукр. наук.-практ. конференції. Київ : Нац. акад. СБУ, 2023. 618 с.

Конференція «Актуальні проблеми управління інформаційною безпекою держави» проводиться щорічно спільно з Інститутом модернізації змісту освіти Міністерства освіти і науки України.

До збірника увійшли матеріали, в яких висвітлюються актуальні проблеми: протидії інформаційним та психологічним операціям на шкоду суспільству і державі в умовах широкомасштабної війни рф проти України, захисту безпеки людини від негативних інформаційних впливів інформаційного насилля, захисту кібернетичної безпеки об'єктів критичної інфраструктури, а також пріоритетів розвитку системи управління інформаційною безпекою держави за оцінками молодих вчених тощо.

Рекомендовано для здобувачів вищої освіти, аспірантів, наукових і науково-педагогічних працівників, а також всім, хто цікавиться тематикою конференції.

Автори несуть повну відповідальність за підбір, точність наведених фактів, цитат, галузевої термінології та інших відомостей. Матеріали конференції публікуються в авторській редакції.

ВІТАЛЬНЕ СЛОВО

З 24 лютого 2022 року збройним вторгненням російської армії на територію України, розпочався новий етап російсько-української війни, що триває з 2014 року. Наразі Україна є першою країною в світі, яка вимушена давати відсіч агресору в чотирьох доменах збройного протиборства: на суші, воді, повітрі та у кіберпросторі.

В Україні діє доволі складна системи кібербезпеки. Координація діяльності у сфері кібербезпеки як складової національної безпеки України здійснюється Президентом України через очолювану ним Раду національної безпеки і оборони України. Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України здійснює координацію та контроль за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку.

Основними суб'єктами національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України, які відповідно до Конституції і законів України виконують в установленому порядку такі основні завдання:

- Державна служба спеціального зв'язку та захисту інформації України забезпечує формування та реалізацію державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації;
- Національна поліція України забезпечує захист прав і свобод людини і громадянина, інтересів суспільства і держави від кримінально протиправних посягань у кіберпросторі;
- Служба безпеки України здійснює запобігання, виявлення, припинення та розкриття кримінальних правопорушень проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснює контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом та кібершпигунством;
- Міністерство оборони України, Генеральний штаб Збройних Сил України відповідно до компетенції здійснюють заходи з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони);
- розвідувальні органи України здійснюють розвідувальну діяльність щодо загроз національній безпеці України у кіберпросторі;
- Національний банк України визначає порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки банками.

Виконання завдань із забезпечення національної безпеки в інформаційній та кіберсферах, ефективні дії в кіберпросторі вимагають якнайшвидшого створення

та розвитку відповідних складових сектору безпеки та оборони держави, набуття ними необхідних спроможностей розроблення інформаційної та кіберзброї.

Одночасно, спостерігається тенденція щодо зростання інтенсивності розвідувально-підривної діяльності рф у кіберпросторі.

Досвід російсько-українського протиборства в кіберсфері показав важливість та результативність спільної роботи фахівців суб'єктів національної систем кібербезпеки та сил оборони, що може стати прикладом дій з кібероборони та сталим трендом для урядів країн-партнерів України.

Проведення конференції в стінах Національної академії Служби безпеки України може стати першим кроком в унормуванні законодавства щодо кібервійни, яке визначить мінімальні стандарти поведінки в кіберпросторі та правила реагування на кібератаки в світі.

Раді вітати сьогодні у цій залі представників Апарату Ради національної безпеки та оборони України, Верховної ради України, Генерального штабу Збройних сил України, Міністерства оборони України, Служби безпеки України, Державної служби спеціального зв'язку та захисту інформації, Кіберполіції України, Національного університету оборони України, закладів та наукових установ, представників громадськості та міжнародних компаній.

Спільне обговорення та дослідження кібервійни росії проти України матиме серйозні позитивні наслідки для національної безпеки та економіки країни, для суспільства і держави.

Що стосується міжнародних партнерів, Україна має можливість ввести поняття кібервійна і запропонувати його світовій спільноті для удосконалення міжнародних правових актів.

Законодавче врегулювання питання кібервійни допоможе сформувати єдину стратегію протидії викликам у кіберпросторі. Національна академія СБ України поруч з іншими представниками наукового середовища готова долучитись до такого наукового дослідження і узаконення відповідної термінології.

Досвід України, ініційовані дослідження та висновки за результатами допоможуть зберегти стабільність та безпеку в світовому кіберпросторі, що є невід'ємною складовою загальної безпеки в сучасному світі.

Сподіваємось на цікаві та інформативні доповіді та плідну співпрацю на конференції, задля вирішення актуальних питань в сфері кібербезпеки, поширення партнерства державного та приватного середовища, із залученням до дослідження експертів та представників державних органів і наукової спільноти, щоб отримати реальну картину ситуації та розробити ефективні методи протидії кіберагресії не лише в Україні, а і у світі.

СЕКЦІЯ 1
ПРОБЛЕМИ ПРОТИДІЇ ІНФОРМАЦІЙНИМ, ПСИХОЛОГІЧНИМ ТА КОГНІТИВНИМ ВПЛИВАМ рф НА ОСОБОВИЙ СКЛАД ЗБРОЙНИХ ФОРМУВАНЬ СТРУКТУР СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

Андрусишин Ю.І.
к.психол.н.
Національна академія СБУ

ПСИХОЛОГІЧНІ АСПЕКТИ АНАЛІЗУ ІНФОРМАЦІЇ ЩОДО ВИОКРЕМЛЕННЯ АНТИУКРАЇНСЬКИХ ПРОПАГАНДИСТСЬКИХ НАРАТИВІВ

Російська пропаганда, яка десятиліттями поширювалась не тільки серед населення рф, але й всього світу, нажаль, вчасно не отримала реальної оцінки свого значення в агресивній політиці кремля щодо пропагування ворожнечі і російського шовінізму. Відтак, від початку повномасштабного воєнного вторгнення російського агресора Україна протидіє не тільки його загарбницьким зазіханням, а й протистоїть інформаційно-психологічній війні рф, у межах якої активно використовуються антиукраїнські пропагандистські наративи, поширюються фейки, проводяться дезінформаційні кампанії. Наразі, діяльність із протидії російським деструктивним впливам значно активізована, проте не має ще системного характеру, що дещо знижує її ефективність. Системність такої боротьби забезпечуватиметься, зокрема й комплексністю самого процесу аналізу певного контенту, що ураховує напрацювання психологічної науки щодо механізмів та закономірностей дієвості впливів інформації на психіку людини.

Отже, важливості набуває визначення основних складових процесу аналізу певної інформації на предмет наявності у ній ознак антиукраїнського пропагандистського спрямування.

Пропаганда передбачає поширення із використанням маніпулювання будь-якої інформації (правдивої, неправдивої, спотвореної) з метою формування у певної цільової аудиторії необхідних думок, мотивів, поглядів, ставлень, устремлінь. Вона впливає на інтелектуальну сферу, психоемоційний стан, мотиви та поведінку людей й вирізняється цілеспрямованістю (мета, система, структурованість), масовістю (зорієнтованістю на широке коло людей – велика цільова аудиторія), нівелюванням критичності мислення (некритичне сприйняття інформації, що зумовлює безапеляційну віру у все почуте / побачене), дозованістю (підбирається та використовується тільки та інформація, яка відповідає меті і особливостям цільової аудиторії).

Пропаганда сама по собі не має негативного змісту, проте деструктивною вона стає, коли її кінцева мета є руйнівною, а для реалізації використовуються

маніпулятивні технології та відверто нечесні методи, які знижують критичність мислення та націлені на «зомбування» цільової аудиторії задля подальшого легкого управління нею. Тобто, з психологічної точки зору пропаганда працює так: формується інформаційний блок, за допомогою якого особі (групі осіб) посилається прихований сигнал (тригер), в свідомості створюються потрібні (позитивні, негативні) образи, стереотипи й мотиви до певних дій та емоційні реакцій, що їх підсилюють; знижується критичність мислення та відбувається «зомбування» цільової аудиторії задля подальшого легкого управління нею. Саме деструктивність пропаганди зумовлює необхідність розробки дієвого алгоритму аналізу повідомлень з метою мінімізації їх негативного впливу на цільову аудиторію.

З метою виокремлення антиукраїнських пропагандистських наративів аналіз інформації має включати:

- *Виявлення психологічних маркерів пропаганди в інформації.* Це, зокрема:

✓ маркери правдивості, що дозволяють визначити наскільки наративи спираються на факти / дати, об'єктивно відображають реальні події / не суперечать ситуації та узгоджуються з явищами й процесами, що відбуваються у соціумі. З їх допомогою можна простежити, наскільки деструктивна пропаганда викривляє й спотворює об'єктивну дійсність, однобоко та упереджено підходить до висвітлення й пояснення найбільш вагомих суспільно-політичних подій та соціальних явищ. До них відносять: *вигаданість, спотвореність, аргументованість, авторитетність джерела, об'єктивність;*

✓ маркери привабливості, які дають змогу відстежити, наскільки меседжі пропаганди є популярними серед цільової аудиторії та викликають певні емоції (радість, задоволення, агресію, страх тощо). Це, зокрема: *тональність, експресивність, графічність, креолізованість;*

✓ маркери маніпулятивності, що свідчать про здійснення негативного впливу на окрему особистість та масову свідомість, а також демонструють, наскільки пропагандистські наративи використовуються для формування думки й стереотипу поведінки у цільової аудиторії. До них належать такі маркери, як: *поширюваність, повторюваність, гіперболізованість, алогічність, ярликування.*

- *Встановлення психічних закономірностей*, що використовуються з метою перетворення інформації на певну психічну активність. Тобто, якщо в поширенні повідомлення можна побачити певний спосіб обходу звичної для даної ситуації критичності сприйняття, ймовірність наявності деструктивного маніпулятивного впливу в ньому значно зростає. До таких закономірностей можна віднести: необхідність прийняття рішення в обмежений часовий проміжок, використання аффіліативних спонук, уникнення фрустрації як мотиватор активності людини, безапеляційне просування готових алгоритмів дій, наголошення на важливості перебування у зоні комфорту, культурні конотації тощо.

- *Виокремлення в певному контенті ознак/рис антиукраїнської пропаганди*.

До них слід віднести: спрямованість на розхитування морального духу населення, просування «переваги» росії над Україною та співіснування з нею на противагу «конкуренції» та «ворогування»; формування недовіри та упередженого ставлення до української влади через непрофесійність, корумпованість, нелегітимність; формування ореолу святості / виключності рф / російського народу в порівнянні з іншими; посилення ворожнечі / недовіри до інших держав; дискредитація українських історичних особистостей / подій; звинувачення України у російських воєнних злочинах; навішування на українців ярликів «бандерівців»; інкорпорування у свідомість українців комплексу меншовартості тощо.

● *Визначення комплексу технік, що застосовуються з метою посилення впливу повідомлень на цільову аудиторію.* До таких технік можна віднести [1]: «заговорювання», «буденної розповіді», «удар на випередження», «хибної аналогії», «констатації факту», «обхід з флангу», «створення проблеми», керованих коментарів, дезінформаційна сітка в Telegram-каналах, «ефект ореолу», риторичні запитання, відволікання уваги, «переконання», «спіраль мовчання», «зараження», «дублювання акаунтів», підміна понять та ін.

Запропонований підхід до аналізу інформації дозволить не тільки аргументовано визначати у ній наявність пропагандистських ознак, але й давати відповідну оцінку діям окремих каналів її поширення, виокремлювати уразливості / мішені впливу, діяти на упередження.

Тож підсумовуючи вищевикладене, зазначимо, що хоча на сьогодні інформаційно-психологічне протистояння з ворогом неможливо уявити без аналізу пропаганди та дій пропагандистів, відсутність системності у протидії даному явищу може призводити до втрати проактивності – можливостей діяти на упередження.

Аналіз російської пропаганди має базуватися на чіткому визначенні сутності та рис антиукраїнської пропаганди. Це дозволяє передусім чітко визначати основні її наративи, а відтак моніторити інформаційний простір щодо інтенсивності її просування, каналів розповсюдження, охоплення аудиторії, застосованих технологій, а також вчасно вживати заходів щодо протидії негативному пропагандистському впливу, розбудовувати систему проактивного забезпечення стратегічних комунікацій в умовах повномасштабного збройного протистояння.

Література

1. Центр протидії дезінформації при РНБО України: Глосарій: механізми. URL : https://cpd.gov.ua/category/glossary/mechanisms/ (Дата звернення: 20.03.2023).

Баланда А.Л.
доктор економічних наук, професор
НА СБ України
Артюшин Г.М.
доктор педагогічних наук, професор
НА СБ України

ІНФОРМАЦІЙНА БЕЗПЕКА ОРГАНІЗАЦІЇ: ЕКОНОМІЧНИЙ ПІДХІД ДО ЗАБЕЗПЕЧЕННЯ

Економіка інвестицій в інформаційну безпеку є порівняно новою сферою наукових досліджень, їх особливістю є висвітлення проблематики з двох протилежних точок зору: перша – адміністратора системи безпеки, друга – зловмисника. Власне, інвестиції в інформаційну безпеку повинні зменшувати ризики системи, однак це відбувається за рахунок зменшення інших, часто високоприбуткових інвестиційних вкладень. Відмова від такого роду фінансових витрат, в ряді випадків гарантує більші прибутки від діяльності, але їх наслідком стає відсутність дієвого захисту інформаційних активів. Інвестиції в безпеку вважаються виправданими у випадку, коли вкладені кошти є меншими за потенційні втрати, у протилежному випадку, виходячи суто з економічної точки зору вони є абсолютно невиправданими. Однак, такий підхід видається не зовсім прийнятним, оскільки не враховує ймовірність настання несприятливих подій чи реалізації ризиків безпеці. Враховуючи сучасний ландшафт загроз, наслідки відмови від інвестування в інформаційну безпеку можуть виявитися значно дорожчими, ніж очікувані витрати на заходи безпеки. Тому більшість організацій виділяють величезні кошти на забезпечення безпеки власних інформаційних ресурсів, у зв’язку з чим виникає логічне запитання щодо доцільності цих витрат.

Для того, щоб заходи забезпечення інформаційної безпеки мали економічний сенс керівництво організації повинне знайти оптимальний баланс між ймовірністю реалізації ризику та витратами на його зменшення. Як слушно зазначають ряд авторів [1], більшість топ-менеджменту організації розглядають інформаційну безпеку в якості своєрідної «бездонної ями, що ніколи не буде повною», у кращому випадку – це «вимушене зло, що заважає продуктивності». Такий стан речей можна пояснити тим, що менеджери інформаційної безпеки не у змозі адекватно оцінити фінансові витрати та ймовірність реалізації інформаційних ризиків.

Відповідаючи на наведене питання, всупереч думці щодо «бездонної ями», дослідники стверджують, що насправді існує оптимальна точка для витрат на інформаційну безпеку, інвестування нижче чи вище якої вважається недоцільним [2, с. 122]. Спираючись на дослідження оптимальних рівнів інвестицій в безпеку за різних сценаріїв інформаційних атак що надходять одночасно із декількох

зовнішніх джерел, С. Деррік Хуанг побудував їх економічну модель. В основу моделі було покладено принцип максимізації вигоди. Взаємозв'язки між основними змінними (вразливість системи, ймовірність порушення безпеки, потенційні збитки від реалізації ризику атаки і рівень інвестицій у безпеку) досліджуються з використанням аналітичного інструментарію та чисельного аналізу з урахуванням різного роду граничних величин. Зокрема, модель показує, яким чином фірма повинна розподіляти свій обмежений бюджет на безпеку для захисту від двох типів атак (розподілених та цільових) одночасно. Так, фірмі з невеликим бюджетом краще спрямувати більшу частину інвестиційних коштів на заходи протидії одному з класів атак. У випадку, коли потенційні збитки від цілеспрямованих атак та вразливість системи є відносно відчутними, то значну частину бюджету слід виділяти на заздалегідь визначений клас інформаційних атак [3, с. 131].

Потреба в ефективному та результативному бюджетуванні і збалансованих витратах на забезпечення інформаційної безпеки зумовлена низкою різних вимог, починаючи від технологічних і закінчуючи стратегічними питаннями розвитку організації. Виходячи з того, що інформаційну безпеку слід розглядати в якості міждисциплінарного феномена, бюджет повинен відображати повний спектр всіх її проявів (люди, процеси та технології) [4, с. 116].

Концепція переважної більшості інвестиційних проектів має на меті отримання прибутку. Цей прибуток може виражатися у вигляді капіталу, часового ресурсу та визначених переваг (матеріальних і нематеріальних). Однак, методики розрахунків нематеріальних активів є досить складними, а тому більшість сучасних практик націлена на їх трансформацію у грошовий еквівалент. Для того, щоб прийняти безпечне інвестиційне рішення, необхідно володіти інформацією щодо активів аналітичного характеру за такими базовими категоріями: інформація; програмне забезпечення; матеріально-технічне забезпечення; персонал і система управління; вразливість щодо загроз; ймовірність настання збитків у визначеній часовій перспективі. За умови отримання такого роду аналітичної інформації, інвестиційний аспект інформаційної безпеки можна порівняти з більшістю характеристик ефективності інвестицій у цінні папери. На сьогодні вже розроблений якісний інструментарій, що дозволяє провести необхідні розрахунки майбутньої прибутковості інвестицій у цінні папери на основі використання авторегресійних економетричних моделей.

Перевага запропонованого підходу полягає в тому, що для цілей нашого аналізу немає необхідності у точних розрахунках майбутньої прибутковості. У цьому випадку набагато важливіше вміти оцінити його величину на основі аналізу ризиків. Це можна зробити на основі аналізу ймовірності виникнення інцидентів та оцінці їхнього впливу. Для оцінки загальної вартості інциденту необхідно володіти інформацією щодо його можливих наслідків та величини можливих збитків. Інформацію щодо можливих наслідків інциденту доцільно отримати

шляхом експертних оцінок, а щодо ймовірності, то вона встановлюється на основі аналізу спеціалізованих звітів чи цільових досліджень.

Пропонована методика розрахунку ефективності інвестицій у забезпечення інформаційної безпеки на основі аналізу ризиків виходить з умови, що величина вигоди, отриманої від упровадження контрзаходів є різницею між невід'ємним ризиком (до введення засобів контролю безпеки) та залишковим ризиком (після введення контрзаходів). Враховуючи той факт, що упровадження системи контрзаходів призводить до зміни ймовірностей (Р) інцидентів (наприклад, ймовірність витоку даних із системи зменшується внаслідок встановлення антивірусної програми чи ранньому виявленню вторгнення), вплив фактору ризику можна виразити у вигляді добутку [5, с. 47]:

Вплив невід'ємного ризику = Вартість інциденту X *Р(невід'ємний ризик)*

Вплив залишкового ризику = Вартість інциденту X *Р(залишковий ризик)*

Тоді вигода набуває такого вигляду:

Вигода = Вплив притаманного ризику - Вплив залишкового ризику

Ефективність інвестицій в інформаційну безпеку = Вигоди − Витрати на контрзаходи.

Виходячи з наведеного, процес формування кошторису упровадження заходів забезпечення інформаційної безпеки повинен зводитися до розрахунку ймовірності настання того чи іншого інциденту, тобто необхідно показати, яким чином вжиті заходи безпеки змінюють рівень ризиків.

Визначивши вплив невід'ємного ризику (НР), виходячи з його ймовірності, а також вплив залишкового ризику (ЗР), з урахуванням відповідної ймовірності, можна вивести результуючий показник - Потенціал захисту (ПЗ) у вигляді:

ПЗ = (НР - ЗР) / НР

Потенціал захисту буде ідеальним за умови наближення його величини до одиниці, що можливе за незначного впливу залишкового ризику. Ідея цього індикатора полягає в отриманні кількісних характеристик ступеню зменшення ризику внаслідок упроваджених заходів забезпечення інформаційної безпеки. Маючи інформацію щодо операційних витрат чи вартості засобів для зменшення ризиків, можна чітко відстежувати взаємозалежності між динамікою захисних спроможностей організації та змінами величини інвестиційних вкладень у забезпечення інформаційної безпеки.

Витрати на забезпечення інформаційної безпеки можуть слугувати важливим показником в процесі прийняття управлінських рішень, особливо коли вони пов'язані з іншими показниками, наприклад динамікою загальних витрат компанії, кількістю співробітників, еволюцією ризиків, а також факторами, що формують собівартість продукції. Точна відповідь на запитання щодо вартості заходів інформаційної безпеки вимагає врахування всіх реальних витрат організації, оскільки недостатньо просто назвати цифру, її потрібно пояснити і пов'язати з усіма іншими факторами розвитку. Вони можуть визначатися шляхом

упровадження принципів бухгалтерського обліку загальних витрат організації. Для цього всі статті витрат на заходи інформаційної безпеки слід відобразити за такими категоріями: праця, накладні витрати, обладнання, амортизація (прямі витрати); надані внутрішні послуги (непрямі витрати); сервісні послуги; розподіл витрат на інші підрозділи організації. Тобто, витрати на забезпечення інформаційної безпеки пропонується визначати за міжнародними стандартами бухгалтерського обліку з урахуванням можливої актуалізації ризиків.

На стратегічному рівні безпековий бюджет повинен відповідати візії та місії організації, діючому законодавству та нормативним вимогам, а також факторам, пов'язаним із зовнішнім та внутрішнім середовищем функціонування організації [6, с. 1972]. Тактичний рівень бюджетування включає: аналіз ризиків для виявлення загроз; стандарти та всі види комплаєнс контролю. Його основна функція полягає у виявленні найбільш актуальних загроз безпеці інформаційних активів. Він також відіграє важливу роль у прийнятті управлінського рішення щодо розподілу витрат на заходи безпеки. На операційному рівні необхідно враховувати як операційні (доступність робочої сили, ресурси, оптимальні рівні захисту та їх доцільність), так і технологічні (компоненти інфраструктури, засоби управління на апаратному та програмному рівнях) вимоги.

Таким чином, більшість сучасних моделей та підходів щодо бюджетування інформаційної безпеки не враховують загальних характеристик організації та середовища, в якому вона працює. Побудова відповідної моделі повинна виходити з необхідності дотримання балансу між дотриманням діючих безпекових стандартів та оцінці прийнятних рівнів ризику.

Література

1. Solomon G. The influence of organisational culture and information security culture on employee compliance behaviour. *Journal of Enterprise Information Management*. 2021. Vol. 4, no. 34. P. 1203–1228.

2. Shaun W. Integrated framework for information security investment and cyber insurance. *Pacific-Basin Finance Journal*. 2019. № 57. P. 101–173.

3. Huang D.C., Hu Q., Behara R. Economics of Information Security Investment in the Case of Simultaneous Attacks. *The Fifth Workshop on the Economics of Information Security*. 2006. P. 118–146.

4. Diesch R., Pfaff M., Krcmar H. A comprehensive model of information security factors for decision-makers. *Computers & Security*. 2020. № 92. P. 101–147.

5. Sonnenreich W., Albanese J., Stout B. Return on security investment (ROSI)-a practical quantitative model. *Journal of Research and practice in Information Technology*. 2006. Vol. 1, № 38. P. 45–59.

6. Oliva F., Couto M. The integration between knowledge management and dynamic capabilities in agile organizations. *Management Decision*. 2019. Vol. 8, №57. P. 1960–1979.

Беседа Д.В.
к.ю.н., доцент КІБД,
Національної академії СБ України
Сорочинський О.В.
студент Національної академії СБ України

НАЙПОШИРЕНІШІ ВИДИ КІБЕРЗАГРОЗ СЕРЕД УКРАЇНСЬКИХ ГРОМАДЯН

У зв'язку із цифровим прогресом створюється все ширше коло можливостей для кіберзлочинів, які можуть бути направлені на різні сфери життєдіяльності українських громадян та самої держави. Тому доцільним є розглянути те, які види кіберзлочинів є найбільш розповсюдженими серед українських громадян, що дозволить зрозумиіти як виглядає проблема і як з нею боротись.

1. Фішингові сайти – це веб-ресурси, які візуально ніяк не відрізняються від офіційних сайтів, але при вводі особистих даних: логіни і паролі наприклад для авторизації у державних ресурсах, у електроних скриньках або реквізити своїх платіжних карток – це все переходить у руки кіберзлочинців.

2. Використання піратського програмного забезпечення (далі – ПЗ). Це дійсно масштабна проблема не тільки для звичайного користувача, а й для українських державних службовців, що використовують «ламане», «піратське» програмне забезпечення – яке можна безкоштовно завантажити на свій комп'ютер. Але дуже часто такі програми можуть містити у собі шкідливі компоненти. Часто у таких програмах використовуються «кейлогери» – програми, що шпигують за тим, що ви натискаєте на клавіатурі. Або програми-шпигуни, що крадуть файли визначеного типу з комп'ютера користувача і надсилають на персональний комп'ютер зловмисника.

Слід зазначити, що в держорганах це дійсно серйозна проблема. Дуже багато різноманітних держорганів, розпорядників відкритих даних, оприлюднюють на порталі «data.gov.ua». Було проаналізовано 35 тис файлів. Серед них 6,6 тис, тобто 19% файлів мали ознаки того, що були створені на піратському програмному забезпеченні.

Аналогічним методом здійснювалася перевірка «rada.gov.ua», а саме Верховна Рада України. Було завантажено файли супровідних документів зі сторінок близько 6000 законопроєктів що відносяться до IX-го скликання. Після цього було проаналізовано 6841 файлів, і, виявилось, що 1100 файлів (16% були створені на піратському софті.

Це демонструє неусвідомленість проблем нашими державними службовцями, їх безвідповідальність навіть в таких критично важливих установ як ВРУ, працівники якої використовують на своїх комп'ютерах піратське програмне забезпечення. Також це демонструє неусвідомленість зі сторони державної влади, а саме сектору забезпечення кібербезпеки, яка має забезпечувати імпорт

ліцензійних програм.

3. Троянський вірус – це шкідлива програма, яка вміло проникає в систему під виглядом легального додатку або програмного забезпечення. Він може роками перебувати на комп'ютері або смартфоні без відома користувача.

4. DDoS атаки – напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними користувачам, для яких комп'ютерна система була призначена. Яскравим прикладом таких атак є рф, яка систематично використовувала це задля дисфункції різних українських систем, на прикладі українських банків, коли відбувалися атаки майже на всі банки з різною результативністю.

Таким чином, розуміючи те, які саме бувають кіберзлочини і в чому саме полягає їхня суть, громадяни України можуть уникати їх і не ставати жертвами кіберзлочинців, і також значно зменшити результативність цих злочинів .

Література

1. Герасименко В., Бондаренко А. Кіберзахист вищого ґатунку: сотні держустанов використовують піратські програми, що можуть містити шкідливі алгоритми. Texty.org.ua - статті та журналістика даних для людей – Тексти.org.ua. URL: https://texty.org.ua/articles/105460/piratskyj-abo-lamanyj-soft-u-derzhavnykh-ustanovakh/ (дата звернення: 03.03.2023).

2. Види троянських вірусів і чим вони небезпечні. Антивірус BitDefender Україна - Оберіть рішення, які використовують експерти. URL: https://bitdefender.ua/blog/troyanskie-virusy-i-programmy-v-chem-ikh-opasnost/ (дата звернення: 03.03.2023).

3. Про План реалізації Стратегії кібербезпеки України : Рішення Ради нац. безпеки і оборони України від 30.12.2021 р. : станом на 3 лют. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/n0087525-21#Text (дата звернення: 06.03.2023).

Бойченко О.С.
к.т.н., Житомирський військовий інститут імені С.П. Корольова
Кримець Б.В.
Центральне управління охорони державної таємниці та захисту інформації
Генерального штабу Збройних Сил України

ПРОПОЗИЦІЇ З УДОСКОНАЛЕННЯ ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧІВ

На початку XXI століття з метою розширення послуг із захисту інформації та інформаційних ресурсів в інформаційно-комунікаційних системах (ІКС) почав широко застосовуватись електронний підпис, який заснований на відповідних криптографічних механізмах. Це сприяло тому, що у системах електронного

документообігу (СЕДО) в умовах протидії порушникам (зловмисникам) почали надаватися базові послуги (виконуватися функції) або розв'язуватися задачі забезпечення з необхідним рівнем гарантій конфіденційності, цілісності, справжності (автентичності), неспростовності (спостережливості), доступності та надійності.

У Збройних Силах (ЗС) України розроблена та введена в дію Захищена СЕДО, яка використовує технологію електронного підпису та використовує електронні довірчі послуги (ЕДП).

Застосування Захищеної СЕДО дозволило скоротити час на доставку документу, що значно підвищило ефективність управління військами (силами). Поряд з тим у ЗС України існують такі проблемні питання:

відсутність у законодавстві України нормативно-правових актів, які визначають поняття секретного електронного документа (СЕД), його юридичний статус та порядок роботи з ним, а також суб'єктів електронної взаємодії системи обігу секретних електронних документів;

електронні документи, які циркулюють у Захищеній СЕДО нетаємні, а сама система не може бути застосована для передачі СЕД (бойових наказів, розпоряджень);

повільне впровадження технічних рішень, які забезпечать можливість надання кваліфікованих ЕДП в ІКС, де обробляється ІзОД;

відсутність порядку взаємодії інфраструктури відкритих ключів (ІВК) ЗС України з ІВК ЗС держав-членів НАТО.

Тому перед ЗС України постає важливе завдання щодо розробки технології надання кваліфікованих ЕДП в ІКС ЗС України, в яких обробляється ІзОД. Виникнення цього актуального науково-технічного завдання зумовлено об'єктивним протиріччям між високими вимогами до захисту ІзОД відповідно до вимог законодавства України і стандартів НАТО та принциповою неможливістю її захисту за рахунок використання існуючої ІВК у ЗС України.

Одним з можливих способів рішення цього завдання є удосконалення ІВК ЗС України для надання кваліфікованих ЕДП в ІКС ЗС України, де обробляється ІзОД.

Головною вимогою до ІВК ЗС України є забезпечення гарантованої довіри до ЕДП, які надаються в ІКС, де обробляється ІзОД.

Для надання ЕДП в ІКС ЗС України, де обробляється ІзОД, необхідно забезпечити доступ до цієї ІКС за рахунок застосування організаційних та технічних заходів [1]. Організаційні заходи повинні забезпечити обмеження доступу підписувачам та користувачам ЕДП до об'єкту інформаційної діяльності, на якому розміщене автоматизоване робоче місце (АРМ) з можливістю роботи в ІКС, де обробляється ІзОД, відповідно до форми допуску до державної таємниці користувача ЕДП. Технічні заходи повинні бути реалізовані за рахунок використання функцій електронної ідентифікації та авторизації користувачів ІКС,

де обробляється ІзОД.

Під СЕД слід розуміти секретний документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити секретного документа.

З метою удосконалення ІВК ЗС України пропонується:

1) створити розподілену базу даних СЕД ЗС України з впровадженою системою розмежування доступу;

2) створити механізм взаємодії між ІКС, в яких обробляється інформація з різним ступенем секретності;

3) розробити порядок надання кваліфікованих ЕДП в ІКС, де обробляється ІзОД;

4) розробити військові публікації, які регламентують встановлення довіреної ідентифікації між ІКС ЗС України та ІКС ЗС держав-членів НАТО в федеративній мережі місій.

Враховуючи вищенаведене, ІВК ЗС України матиме таку структуру: уповноважений орган у сфері ЕДП у ЗС України, кваліфікований надавач ЕДП у ЗС України, підписувачі та користувачі ЕДП.

Уповноважений орган у ЗС України призначений для організації спеціального зв'язку та захисту інформації у сферах ЕДП та електронної ідентифікації у ЗС України.

Кваліфікований надавач ЕДП у ЗС України – визначений підрозділ, який надає одну або більше кваліфікованих ЕДП в ІКС, де обробляється ІзОД.

Підписувачі та користувачі ЕДП у ЗС України – створювачі електронних печаток, відправники та отримувачі електронних даних, які отримують ЕДП у кваліфікованих надавачів ЕДП у ЗС України.

Безпосередньо функції довірчої сторони виконують програмно-технічні комплекси, які використовуються під час надання ЕДП і являють собою апаратні, апаратно-програмні та програмні засоби кваліфікованого надавача ЕДП у ЗС України.

Враховуючи вище наведене та результати науково-дослідних робіт [2, 3] перспективна схема організації ІВК у ЗС України складається з наведених нижче компонентів.

Сервер взаємодії – окремо виділені спеціальні апаратні та програмно-апаратні засоби, які призначені для унеможливлення витоку СЕД при їх передачі між ІКС різного рівня секретності, у тому числі й у федеративній мережі місій.

Інформаційно-комунікаційна мережа (ІКМ) ІКС, де обробляються СЕД з грифом секретності "Цілком таємно", може бути представлена як ІКС класу 2.

ІКМ ІКС, де обробляються СЕД з грифом секретності "Таємно", може бути виконана як розподілена ІКС класу 3 з каналами зв'язку, які використовуються ЗС України.

ІКМ ІКС, де обробляються електронні документи з грифом обмеження

доступу “Для службового користування”, може бути виконана як ІКС класу 3.

Сервер баз даних – електронно-обчислювальний засіб у серверному виконанні із встановленим спеціалізованим програмним забезпеченням, який виконує функції серверу додатків на базі Web-технологій для забезпечення обміну СЕД між користувачами ІКС, їх зберігання, розмежування доступу до СЕД користувачів та обробки СЕД відповідно до політки безпеки інформації в ІКС за допомогою пристрою розмежування доступу.

Пристрій розмежування доступу – електронно-обчислювальний засіб із встановленим спеціалізованим програмним забезпеченням.

Комутатор – пристрій, призначений для з’єднання декількох АРМ в межах одного об’єкту (центрального або віддаленого).

АРМ – електронно-обчислювальний засіб на основі персональної електронної обчислювальної машини або засобу спеціального зв’язку, на якому встановлений мінімально потрібний комплект програмного забезпечення з обов’язковою наявністю інтернет браузера.

Відповідно до політики безпеки в ІКС на АРМ за допомогою програмних засобів, які розміщені на сервері даних, створюється особистий кабінет користувача ІКС. Передбачається, що авторизований користувач ІКС може мати доступ до свого особистого кабінету з будь-якого АРМ. При цьому ступінь секретності інформації, яку може обробляти користувач ІКС буде обмежена ступенем секретності інформації, яку можна обробляти на відповідному АРМ.

Міжмережевий екран – програмно-апаратний комплекс, який реалізує функцію контролю вхідного і вихідного трафіку в ІКМ ІКС одного рівня секретності.

Програмно-технічний комплекс кваліфікованого надавача ЕДП у ЗС України у закритому контурі – апаратні, апаратно-програмні та програмні засоби призначені для надання кваліфікованих ЕДП в ІКС ЗС України відповідного рівня секретності.

Таким чином, надання ЕДП користувачам ІКС ЗС України буде здійснюватися за грифами секретності СЕД та за рівнем допуску до роботи з державною таємницею відповідного користувача ІКС ЗС України.

Застосування серверів взаємодії дозволить реалізувати взаємодію ІВК ЗС України з ІВК ЗС держав-членів НАТО для здійснення обміну інформацією та розвідувальними даними під час спільних операцій держав-членів НАТО.

Література

1. Про затвердження Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : Постанова Кабінету Міністрів України від 16.02.1998 № 180. URL:https://zakon.rada.gov.ua/laws/show/180-98-%D0%BF#Text (дата звернення:

07.03.2023)
2. Науково-дослідна робота шифр “Фундамент”: звіт про НДР (остаточний), кер. О. Бойченко. Житомирський військовий інститут імені С. П. Корольова, 2019. 119 с.
3. Науково-дослідна робота шифр “Фундамент-ТТЗ”: звіт про НДР (остаточний), кер. О. Бойченко. Житомирський військовий інститут імені С. П. Корольова, 2020. 103 с.

Брановицький В.В.
Житомирський військовий інститут
ім. С.П. Корольова, м. Житомир

ПРОТИДІЯ ІНФОРМАЦІЙНИМ, ПСИХОЛОГІЧНИЙ ВПЛИВАМ рф НА ВІЙСЬКОВОСЛУЖБОВЦІВ ЗБРОЙНИХ СИЛ УКРАЇНИ

В умовах постійного потоку деструктивної інформаційної пропаганди, з боку російської федерації (рф) по відношенню як до населення України, так і до військовослужбовців Збройних Сил України дуже важливо бути інформаційно грамотним і освіченим, вміти розрізняти фейкову інформацію від правди. Адже відверта брехня, перекручення фактів, спотворення історичних подій створюють несприятливі умови для формування антиукраїнської свідомості у людей, яку потім проросійські сили вміло використовують для управління та маніпуляції населенням України. Від початку збройної агресії рф цілеспрямовано застосовує не тільки збройні формування, а ще й комплекс сучасних прихованих методів протиборства, зокрема інформаційно-психологічний вплив, об’єктом якого є не лише населення нашої держави, а й військовослужбовці Збройних Сил України.

Аналіз війн усіх часів показує, що спроби вести інформаційну війну з метою управління чи підкорення як населення так і військових були завжди, але з розвитком технологій особливо з появою видань, а згодом радіо, телебачення та Інтернету це стало робити набагато простіше. Тому інформаційні та психологічні операції є невід’ємною частиною сучасних воєн, а протидія їм є актуальним завданням. Вже котрий рік поспіль Україна перебуває в активній фазі гібридної війни з рф. На початку 2014 року наша держава зіштовхнулася з новітніми викликами і загрозами територіальній цілісності, суверенітету й демократичному ладу в країні. Незаконна анексія Кримського півострова в умовах відсутності збройного опору, військове вторгнення на Донбас й окупація в стислі строки значної території Донецької та Луганської областей, та з 2022 року широкомасштабна війна рф проти України, стали можливими завдяки багаторічним підготовчим діям росії з підриву авторитету та довіри місцевих мешканців до української влади і співгромадян з інших регіонів. На жаль,

результативність російської інформаційної війни ми відчуваємо й по цей час. Однією з причин швидкої окупації південно-східних територій стала дієвість пропагандистської машини рф з усіма її потужними інструментами, особливо в мережі Інтернет. Насичення ресурсів в мережі Інтернет матеріалами психологічного впливу з постійним насадження проросійських наративів, ускладнює процес боротьби в інформаційному просторі.

Наразі, коли Україна успішно протистоїть російському нападу, вкрай актуальним є питання інформаційної безпеки військовослужбовців Збройних Сил України. Адже, не маючи можливості перемогти на полі бою, ворог намагається посіяти "зраду" та розхитати українське суспільство та особовий склад Збройних Сил України. Зокрема, на цим працюють центра зарубіжної військової інформації рф. Упродовж багатьох десятиліть центра зарубіжної військової інформації рф удосконалювали свої інформаційно-психологічні акції та операції вдаючись до нових способів, засобів і методів інформаційно-психологічного впливу. Зважаючи на це, однією з передумов забезпечення національної безпеки України, як в цілому, так і в умовах війни, є вивчення та аналіз спеціальних інформаційних акцій та операцій рф, об’єктом яких є наші військові.

Військовослужбовці Збройних Сил України й надалі отримують з невідомих акаунтів в соціальних мережах повідомлення провокативного характеру, а також повідомлення - погрози. Центра зарубіжної військової інформації рф для досягнення цих цілей застосовуються як візуальні, аудіо та аудіовізуальні матеріали впливу. Психологічний вплив на військовослужбовців Збройних Сил України представляє собою спосіб залучення, утримання та управління їх увагою на спеціально підготовленими матеріалами впливу, що в свою чергу впливає на їх свідомість й направлена на спотворення, дестабілізацію професійних цінностей і мотивів, а у подальшому – на зміну поведінки. Зокрема, серед негативних наслідків психологічного впливу на особовий склад Збройних Сил України є: розмивання відчуття гордості за свою державу, належності до її збройних сил, підрив у переконаності військовослужбовців у необхідності виконувати свій конституційний обов’язок стосовно захисту Українського народу, своєї землі; зниження морально-психологічного стану, створення обстановки невпевненості, сумнівів особового складу щодо власного майбутнього, майбутнього збройних сил і держави, послаблення волі до збройного опору; розкол військових колективів за політичними, релігійними, етнічними, службовими та іншими мотивами; погіршення боєздатності частин і підрозділів за рахунок пониження службової активності, дезертирства, симуляції хвороби, ухилення від виконання наказів командирів, зради, коливань і сумнівів у надійності зброї, у придушення волі, створення спотвореної картини бойових дій, бойової обстановки; невірне сприйняття військовослужбовцями наявних загроз національній безпеці, дійсних планів і намірів противника. З огляду на вказане, доцільним видається зауваження щодо надзвичайно важливого значення захисту особового складу Збройних Сил

України від негативного інформаційно-психологічного впливу противника [1].

Насамкінець, варто зазначити, що потрібно проводити інформаційну роботу як з населенням України так і з військовослужбовцями Збройних Сил України, щодо роз'яснення як протидіяти та розпізнавати неправдиву інформацію, інформаційні вкиди, фейки. Також, одним із можливих шляхів вирішення даної проблеми, повинен бути рівень знань та вмінь кожного військовослужбовця розпізнавати пропаганду, фейки, дезінформацію та інші форми деструктивної інформації, що дозволить захистити його від негативного психологічного впливу ворога. А вироблення «імунітету» до таких впливів у перспективі допоможе досягти і власних цілей при веденні інформаційної війни, оскільки кожна людина стане «воїном» інформаційного простору. Отже, якщо своєчасно не оцінити та не реагувати на інформаційні загрози, які постають перед державою, то згодом наслідки можуть призвести до втрати контролю над країною, шляхом маніпулюванням як населенням країни так і військовослужбовцями.

Література

1. Алещенко В. Інформаційно-психологічна безпека особистості в умовах гібридної війни. Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки. 2022. №49 (1). С. 13–21.

Бровко В.Д.
кандидат технічних наук
Національна академія СБ України

УДОСКОНАЛЕННЯ НАВЧАЛЬНОГО ПРОЦЕСУ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ ЗА СПЕЦІАЛЬНІСТЮ «КІБЕРБЕЗПЕКА»

Аналізуючи зазначені у Законі України «Про основні засади забезпечення кібербезпеки України» завдання суб'єктів забезпечення кібербезпеки можна дійти висновку про те, що у підготовці фахівців для національної системи кібербезпеки викреслюються декілька профілів:

1. Розвиток безпечного, стабільного і надійного кіберпростору як середовища (віртуального простору), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утвореного в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних.

2. Забезпечення захищеності життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового

комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

3. Забезпечення кіберзахисту державних електронних інформаційних ресурсів та об’єктів критичної інфраструктури на основі сукупності організаційних, правових, інженерно-технічних заходів, заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем, а також створення автоматизованих систем управління інформаційною безпекою.

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» Служба безпеки України повинна здійснювати запобігання, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснювати контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом та кібершпигунством, негласно перевіряти готовність об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидіяти кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави; розслідувати кіберінциденти та кібератаки щодо державних інформаційних ресурсів. Інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечувати реагування на кіберінциденти у сфері державної безпеки [1].

Для виконання вищезазначених завдань Службі безпеки необхідні фахівці у сфері кібербезпеки.

У цих тезах автором пропонується перелік спеціалізацій для підготовки професіоналів для національної системи кібербезпеки відповідно завдань, що стоять перед Службою безпеки України:

Організація протиборства та спеціальних операцій у кіберпросторі;

Організація розвідувальної та контррозвідувальної діяльності у кіберпросторі;

Організація контррозвідувальної та оперативно-розшукові діяльність у кіберпросторі;

Організація антитерористичної діяльності в кіберпросторі;

Організація розкриття кіберзлочинів спрямованих проти національної безпеки.

Організація та контроль кіберзахисту електронних інформаційних ресурсів;

Організація та контроль кіберзахисту об’єктів критичної інфраструктури.

Література:

1. Закон України Про основні засади забезпечення кібербезпеки України. (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403) [Електронний ресурс]. – Режим доступу : http://zakon0.rada.gov.ua/laws/show/2163-19.

Вандалович В.П.
Житомирський військовий інститут імені С. П. Корольова
Завада А.А.
к.т.н, с.н.с.,
Житомирський військовий інститут імені С. П. Корольова

АВТОМАТИЗАЦІЯ ПРОЦЕСУ МОНІТОРИНГУ ІНФОРМАЦІЙНОГО ПРОСТОРУ З МЕТОЮ ВИЯВЛЕННЯ ТА ОЦІНЮВАННЯ РІВНЯ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ДЕРЖАВИ

В умовах широкомасштабного вторгнення російської федерації (рф) в Україну суттєво актуалізуються питання, що пов'язані із забезпеченням інформаційної безпеки (ІБ) нашої держави. З цією метою основними засадами державної інформаційної політики з питань забезпечення ІБ є система заходів, спрямованих на:

запобігання інформаційним загрозам (викликам, впливам) шляхом здійснення превентивних заходів із забезпечення ІБ для попередження можливості їх виникнення;

виявлення інформаційних загроз та деструктивних впливів, що полягає у систематичному моніторингу, аналізі й контролі можливості появи реальних або потенційних інформаційних загроз;

впровадження своєчасних заходів з нейтралізації інформаційних загроз (впливів), прогнозування рівня загроз ІБ;

вживання заходів з ліквідації (локалізації) загроз (впливів);

ліквідацію наслідків негативних інформаційних впливів.

В процесі реалізації зазначеної системи заходів важливим етапом є процедура оцінювання реальних загроз ІБ держави в цілому та у воєнній сфері зокрема. При цьому у сфері національної безпеки і оборони така процедура має властиві лише їй специфічні особливості, які передбачають:

по-перше, виявлення негативного впливу на особовий склад Збройних Сил (ЗС) нашої держави, його аналіз за якісними і кількісними показниками, визначення форм та способів інформаційної боротьби на основі базових показників цього впливу (наприклад, інтенсивності, тривалості, поширеності джерел, масштабності об'єктів впливу);

по-друге, встановлення та доведення факту наявності в ньому інформаційних загроз державі у воєнній сфері та оцінювання рівня цих загроз.

Однією з причин актуалізації проявів інформаційних загроз державі є швидкі темпи розвитку та впровадження у повсякденне життя інформаційних технологій, що тісно пов'язані з розвитком мережі Інтернет. Завдяки ній користувачі, у тому числі й військовослужбовці ЗС України, задовольняють власні інформаційні потреби, обумовлені не тільки приватною, а й професійною діяльністю.

Особливу цікавість користувачів в мережі Інтернет сьогодні привертають повідомлення в е-ЗМІ та соціальних інтернет-сервісах (СІС), зокрема у соціальних мережах (СМ). Зважаючи на це зазначені джерела перетворюються на потужний інформаційний ресурс, контентне наповнення якого охоплює практично усі прошарки цільової аудиторії. Залежно від того, як подається такий контент та яке він несе в собі змістовне навантаження, можна стверджувати, що окрім усіх позитивних аспектів від е-ЗМІ та СМ в їх контентному наповненні містяться загрози ІБ держави, у тому числі й у воєнній сфері.

Зазначене підтверджується фактами широкого використання е-ЗМІ та СМ (особливо російська СМ "ВКонтакте") для здійснення деструктивного інформаційно-психологічного впливу (ІПсВ) на населення України та особовий склад ЗС України та інших силових структур нашої держави напередодні подій 2014 року та подальшої прихованої інтервенції військ рф в Україну. Основна мета зазначених ІПсВ – дискредитація вищого військово-політичного керівництва держави, насадження серед місцевого населення паніки, страху та хаосу, зневіри в можливості органів влади та силових структур. А поєднання розповсюдження інформації, що містить ІПсВ, у е-ЗМІ та СМ з телебаченням, радіомовленням, науковою, публіцистичною й періодичною літературою суттєво впливають на розум, свідомість і психіку мільйонів громадян України.

Інформаційні загрози, що містяться в такій інформації, на даний час стали ефективними засобами маніпулювання суспільством, що здатні зумовлювати появу, перебіг і кінцевий результат не лише політичних подій в державі, а навіть глобальних проблем миру й війни в міжнародному вимірі.

Ведення інформаційної боротьби в сучасній гібридній війні, як показує досвід воєнних дій у 2014-2023 роках , незалежно від її форм має ряд переваг:

мінімальний безпосередній ризик отримання невідворотних втрат серед особового складу ЗС та воєнізованих формувань під час та в результаті проведення інформаційних або інформаційно-психологічних операцій (ІПсО);

ефективність впливу на свідомість цивільного населення у зоні бойових дій, нейтральних держав має не менше значення для успіху інформаційної боротьби, ніж вплив на свідомість військовослужбовців.

Інформаційний фон, що складається у суспільстві під час війни, позначається на відношенні населення до політики свого уряду та дій силових органів, сприйнятті власних ЗС та їх можливостей, функціонуванні воєнної економіки та інших сферах, що впливають на хід війни. Більше того, усі зусилля органів військового управління щодо захисту власних військ від ворожої пропаганди та деструктивних ІПсВ можуть бути нівельовані, якщо аналогічна робота з населенням не проводиться чи проводиться на недостатньому рівні, так як суспільне відношення до війни буде невідворотно транслюватись на ЗС.

Враховуючи вищезазначене можна зробити однозначний висновок – автоматизація процесу інформаційного простору з метою виявлення та оцінювання

рівня загроз ІБ держави у воєнній сфері, у тому числі й за результатами моніторингу е-ЗМІ та СМ, є важливим практичним завданням, яке повинно бути вирішене в інтересах забезпечення національної безпеки і оборони держави. При цьому слід акцентувати увагу на тому, що одержувана у результаті оцінка рівня загроз інформаційній безпеці держави у воєнній сфері за результатами моніторингу е-ЗМІ та СМ, є однією зі складових загальної оцінки рівня загроз ІБ. Особливістю оцінки рівня загроз інформаційній безпеці держави у воєнній сфері за результатами моніторингу е-ЗМІ та СМ є те, що вона лише доповнює загальну оцінку рівня загроз ІБ держави у характеристиках повноти та об'єктивності.

В роботі наведено структурно-логічну схему спеціалізованого програмного забезпечення (СПЗ) моніторингу інформаційного простору та функціональну схему зазначеного СПЗ, що розроблені на основі підходів до побудови функціональних моделей складних інформаційних систем.

Запропоновано варіант інтерфейсу СПЗ моніторингу інформаційного простору, що розроблене у середовищі програмування Python та результати його застосування на прикладі е-ЗМІ "Lenta.ru", "Ria.ru" та СМ "ВКонтакте".

Перспективою подальших досліджень можна визначити розроблення методик та алгоритмів комплексного моніторингу інформаційного простору та удосконалення методики визначення загальної оцінки рівня загроз ІБ держави.

Владіміров Є.О.
Національна академія СБ України

АКТУАЛЬНІ ПИТАННЯ ЩОДО ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ В КІБЕРСФЕРІ В УМОВАХ КІБЕРВІЙНИ

Стрімкий розвиток інформаційних технологій поступово трансформує світ. Відкритий та вільний кіберпростір розширює свободу і можливості людей, збагачує суспільство, створює новий глобальний інтерактивний ринок. Водночас переваги сучасного цифрового світу та розвиток інформаційних технологій обумовили виникнення нових загроз національній та міжнародній безпеці.

В Україні, вперше в світі, війна відбувається не лише на землі, морі та у небі, а й в кіберпросторі.

Існує необхідність перегляду тактики взаємодії в кіберпросторі під час відкритої збройної агресії російської федерації, яку вона здійснює, в кіберпросторі та через кіберпростір, фактично розпочавши першу в світі кібервійну, яка є найактуальнішою проблемою інформаційної безпеки нашої держави.

Гібридизація військових дій агресора призвела до необхідності не тільки мобілізовувати існуючи навички та компетенції сил оборони держави, а й розвивати нові напрямки, а саме кібероборону.

Російські кібератаки на українські енергетичні об'єкти, банки, урядові установи та інші критичні інфраструктурні об'єкти є прикладом того, як кіберзброя може використовуватися як ефективний інструмент для впливу на політику, соціально-економічне життя країни, та зокрема на хід ведення бойових дій.

Існує серйозне наукове протиріччя між фактичним веденням кібервійни та відсутністю загальносвітового визначення та законодавства в цій сфері. Це створює складність у визначенні відповідальності за таку діяльність та у визначенні того, які заходи можуть бути вжиті для запобігання її майбутньому виконанню.

Ведення активних упереджувальних та наступальних дій в кіберпросторі – це ті компетенції, які довелося впроваджувати силам оборони, вже під час повномасштабної агресії ворога. Що свідчить про необхідність експертно-аналітичного забезпечення державних управлінських рішень та формування наукового підґрунтя для цілісного та відповідного формування сил та засобів кібероборони держави.

Актуальним є проведення цілісного дослідження першої кібервійни та її впливу на національну безпеку держави, розробка нових підходів та механізмів регулювання кібервійни, щоб захистити світ від нових викликів спільними зусиллями науковців, правових експертів та державних органів

Це дослідження має запропонувати єдину термінологію, критерії за якими будяка кібератака проти національних інтересів може бути чітко визначена, чи є вона проявом військової агресії в кіберпросторі чи ні, і обґрунтовані рекомендації щодо нормативно-правового забезпечення, засобів і сил передової кібероборони нашої держави.

Комплексна міжвідомча науково-дослідна робота з обґрунтування теоретичних засад забезпечення національної безпеки в інформаційній та кібер сферах в умовах кібервійни має бути проведена вищими військовими навчальними закладами: Університетом оборони України та Академією служби безпеки України, в тісній взаємодії з національними суб’єктами кібербезпеки та із залученням громадських професійних організацій та міжнародних партнерів.

Стрельбицька Л.М.
Заслужений працівник освіти України,
д.ю.н., професор кафедри цивільно-правових відносин
Національної академії Служби безпеки України
Гринь М.Д.
магістр права ННІ ІБ СК НА СБУ

КОНТРПРОПАГАНДА: СТРАТЕГІЯ ПРОТИДІЇ НА ТЛІ ПОВНОМАСШТАБНОЇ ВІЙНИ ТА ПІСЛЯВОЄННИХ РОКІВ

На сучасному етапі російсько-української війни важливе місце займає пропаганда, яка є основоположним елементом російської агресії щодо України. Ця агресія має багатовекторний діапазон і складається з економічної, політичної, військової, дипломатично-міжнародної та інформаційної складових. Тому, можна зазначити, що війна російської федерації проти України має гібридний характер і окрім безпосередньої військової агресії у 2014 році та повномасштабного вторгнення від 24.02.2022 передбачає використання низки інформаційно-деструктивних засобів підривної діяльності. Одним з таких засобів є пропаганда.

Діяльність російської пропаганди є цілеспрямованим, комплексним та ефективно організованим процесом, який направляється ворогом на дестабілізацію суспільства шляхом просування деструктивних для українського суспільства та держави наративів. Сьогодні в Україні на законодавчому рівні діє Стратегія інформаційної безпеки[1] та низка інших нормативно-правових актів, які утворюють правову систему протидії інформаційному впливу російської федерації. Проте, аналізуючи особливості трансформації українського суспільства у період 2014-2022 років та після подій 24.02.2022 і до сьогодення, можна зазначити про низький рівень ефективності інформаційної політики української держави в контексті протидії агресору. Сучасна українська система протидії інформаційним загрозам, зокрема і пропаганді, потребує суттєвого вдосконалення та адаптації до нових реалій геополітичного виміру в Європі. Пропаганда держави-агресора є всеохоплюючою та складною за своєю структурою, що значно ускладнює можливість розроблення і застосування ефективних механізмів протидії. Окремим ускладнюючим елементом є ретроспективна парадигма російської пропаганди, яка існувала на території України протягом століть. Це обов’язково необхідно враховувати при побудові сучасної системи протидії російській пропаганді в Україні. Важливим є також і те, що російська пропаганда активно адаптується до розвитку інформаційно-комунікаційних технологій і тому вдало маскується під актуальні сьогодні форми комунікації в ЗМІ, Інтернеті, на телебаченні, тощо.

Основним об’єктом російської пропаганди в Україні є зміна світоглядних установок українського суспільства, зокрема ворог намагається репрезентувати

українцям власне бачення України та українського народу. Тобто, він намагається нав'язати українському суспільству думку про необхідність сприйняття самих себе лише через призму російської моделі світосприйняття. Найбільший акцент, відповідно, російська пропаганда робить на підмінні життєвих цінностей та морально-етичних орієнтирів. Зважаючи на все вищезазначене, Україна вже сьогодні має розробляти Стратегію контрпропаганди, яка буде мінімізувати інформаційно-деструктивний вплив ворога під час повномасштабної війни та у післявоєнний період. Найбільш важливим елементом у перебудові стратегії інформаційної війни з росією стає факт відкритої повномасштабної агресії, який деблокує відкриту контр-діяльність агресору і легітимізує майже будь-які її прояви на міжнародному рівні. Тобто, якщо до вторгнення від 24.02.2022 Україна не хотіла провокувати російську федерацію занадто жорсткими засобами інформаційної протидії або остерігалася міжнародного осуду та ізоляції через ескалацію російсько-українського конфлікту, тощо – то сьогодні, російська федерація веде відкриту агресію і це створює умови для більш радикальних та стратегічно-орієнтованих змін в українському законодавства в сфері запровадження стратегії контрпропаганди.

Стратегія контрпропаганди має складатися з двох важливих елементів, а саме:

1) Модель протидії російському інформаційно-деструктивному впливу;

2) Модель розвитку інформаційно-конструктивного впливу української інформаційної політики;

Така Стратегія повинна чітко визначати не лише загальні тенденції інформаційного протиборства між Україною та росією, але і позначати найбільш суттєві напрямки інформаційної агресії. Це дозволить висвітлити проблемні для українського суспільства наративи на державному рівні, що допоможе громадянам відмежувати значну кількість маніпуляцій і деструктивних повідомлень.

Також важливим є заповнення інформаційного простору україно-центричними наративами. На тлі повномасштабного вторгнення відбулося чимало героїчних подій та проявилося чимало героїчних постатей, які позитивно вплинули на можливості ефективної реалізації української інформаційної політики. Необхідним елементом також є переосмислення історичних подій та осіб, міжнародних зв'язків України зі світом, сенсів української культури та історико-політичної думки, тощо. Стратегія має передбачати розірвання ціннісної парадигми з будь-якою формою російської державності і акцентувати увагу українського суспільства та держави на власному вдосконаленні через раціональне використання інформаційних ресурсів. Така діяльність буде сприяти піднесенню престижу української держави, сформує стійкі моральні орієнтири українського суспільства та побудує модель ціннісної орієнтації українців в турбулентному середовищі зловживання ворогами інформаційно-комунікативних технологій.

Стратегія має відображати інформаційні джерела пропаганди та підкреслювати важливість боротьби з ними, враховуючи аспект дотримання

Загальних прав людини і громадянина[2]. Це необхідно робити для того, щоб Україна не обмежувала права людей на доступ до інформації та вільного вираження думок, не вчиняла тиск на свободу слову – проте, мала можливості виокремлення інформаційно-деструктивних операцій проти національних інтересів України[3] і механізми відповідної протидії.

Важливим є також і визначення стану перманентної боротьби з інформаційною агресією російської федерації, адже у післявоєнний період Україна буде знаходитися у стані інформаційного протиборства, навіть за умови дефрагментації російської федерації. Тому, усвідомлення українським суспільством постійної інформаційної загрози стає обов'язковим елементом побудови ефективного механізму контрпропаганди. Виокремлення і розмежування також потребують методи пропаганди, які використовуються або можуть використовуватися ворогом. А також окремі положення конкретних російських мета-наративів, які можуть впливати на світоглядну модель українського суспільства.

Отже, в контексті необхідності системної та постійної протидії пропаганді російською федерації – Україна має розробити та впровадити Стратегію контрпропаганди. Визначаючи сучасні тенденції та роль України в динаміці світового прогресу – запровадження нормативно-правового акту щодо контрпропагандистської діяльності стане перспективним напрямком подолання інформаційно-деструктивного впливу ворога. Також, це дозволить оптимізувати діяльність контррозвідувальних органів, покращити інформаційний опір суспільства та представників влади, вдосконалити механізми державної інформаційної політики. Найголовнішим же елементом, стане повне відмежування українського суспільства від російської ціннісної моделі світу і його інтеграція до глобальних прогресивних процесів.

Література

1. Рішення РНБО від 15.10.2021 року «Про стратегію інформаційної безпеки» (дата звернення 18.03.2023) URL: https://zakon.rada.gov.ua/laws/show/685/2021#n5

2. Загальна декларація прав людини (дата звернення 18.03.2023) URL: https://zakon.rada.gov.ua/laws/show/995_015#Text

3. Закон України «Про основи національної безпеки» (дата звернення 18.03.2023) URL: https://zakon.rada.gov.ua/laws/show/964-15

Грищук О.М.
Латко І.І.
Житомирський військовий інститут імені С.П. Корольова

ТИПОВІ ПОМИЛКИ ПРОТИДІЇ ПСИХОЛОГІЧНИМ ВПЛИВАМ рф

Питання протидії психологічним впливам на сьогодні є надзвичайно актуальними як в Україні, так і в інших державах. Психологічні впливи під час ведення локальних війн та збройних конфліктів завжди були дієвим інструментом маніпулювання свідомістю цільових аудиторій протиборчих сторін. Росія, як споконвічний ворог України застосовує психологічні впливи протягом багатьох сторічь. Особлива роль психологічних впливів проявилася як на передодні анексії Криму, так і під час широкомасштабного вторгнення. Тому своєчасне виявлення таких впливів та протидія їм і досі залишається актуальним напрямком забезпечення інформаційної безпеки держави.

До сьогодні, як відомо, склалася типова технологія протидії психологічним впливам. По-перше, виявленню підлягає інформаційний привід, який використовується рф для формулювання наративів. По-друге, визначаються ознаки психологічного впливу. Далі обирається спосіб, інструменти та канали протидії. Очевидно, що однією з помилок такого підходу є ефект запізнення. Тобто протидіючі негативному психологічному впливу сторона, яка захищається перебуває в позиції виправдування. Ефект від такого підходу буде більш суттєвим коли зменшити розрив між негативним психологічним наративом та часом початку протидії.

З практики [1–2] відомо, що основними шляхами поширення деструктивних психологічних впливів з боку протиборчої сторони є використання нею засобів масової інформації (телебачення, радіо, преси тощо) та соціальних інтернет-сервісів (блогів, форумів, соціальних мереж). Такі засоби, як правило, використовуються противником для здійснення психологічних впливів на вище військово-політичне керівництво держави, особовий склад Збройних Сил України та військових формувань сил безпеки і оборони, а також на населення [3–4]. Іншою типовою помилкою протидії психологічним впливам можна вважати нечітке визначення відсутність суб’єктів і об’єктів впливу та ефектів, які досягаються противником. Наступною типовою помилкою є відсутність ґрунтовного аналізу психогенних факторів на полі бою, які підсилюють ефект від психологічного впливу.

Таким чином, протидія психологічним впливам рф є важливим практичним завданням для сил безпеки та оборони України, вирішення якого повинно ґрунтуватися на науково обґрунтованих та практично апробованих методиках.

Література
1. Левченко О. В. Система забезпечення інформаційної безпеки держави у воєнній сфері: основи побудови та функціонування: монографія / О. В. Левченко – Житомир : ЖВІ, 2020. – 180 с.
2. Грищук Р. В. Основи кібернетичної безпеки : Монографія / Р. В. Грищук, Ю. Г. Даник ; за заг. ред. проф. Ю. Г. Даника – Житомир : ЖНАЕУ, 2016. – 636 с.
3. Грабар І. Г. Безпекова синергетика: кібернетичний та інформаційний аспект: монографі / І. Г. Грабар, Р. В. Грищук, К. В. Молодецька, за заг. ред. проф. Р. В. Грищука – Житомир : ЖНАЕУ, 2019. – 279 с.
4. Інформаційно-психологічні впливи у кіберпросторі / Ю. В. Баланюк, В. В. Козловський, В. О. Хорошко, Ю. Є. Хохлачова // навчальний посібник за ред. проф. В. О. Хорошко – Київ : НАУ, 2020. – 109 с.

Грубі Т.В.
к.соц.н., доцент,
Національна академія Державної прикордонної служби України
імені Богдана Хмельницького

СУЧАСНІ ТЕНДЕНЦІЇ РОЗВИТКУ ДЕРЖАВНОЇ ПОЛІТИКИ УКРАЇНИ В СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Сучасна Україна повною мірою включена в процеси інформатизації суспільства і формування єдиного світового інформаційного ринку. Особливе місце у цьому спектрі суспільних відносин займають проблеми забезпечення інформаційної безпеки. Поряд із нормативно-правовим напрямом, остання реалізується через систему інститутів публічної влади й громадянського суспільства та регламентується Законом України «Про основи національної безпеки України» від 21.06.2018 р.

Недостатня ефективність існуючої сьогодні державної політики інформаційної безпеки в умовах динамічного впливу сучасних факторів і найбільш гострих форм інформаційного протиборства, вимагає зміни всієї концепції діючої інформаційної політики, з метою її адаптації до сучасних реалій. Серед особливих умов реалізації державної політики інформаційної безпеки визначимо: формування глобального інформаційного суспільства; політичну, соціальну, культурну, інформаційну, психологічну глобалізацію; геополітичну конкуренцію в інформаційному просторі; інформаційно-психологічну війну як складову збройної агресії росії проти України. Останнє стало базисним викликом в контексті забезпечення інформаційної безпеки, адже держава зіткнулася з використанням проти неї роками вибудовуваної у росії пропагандистської системи, що діє одночасно на всіх напрямах (українському, російському,

міжнародному), із використанням можливих засобів масової комунікації. На думку фахівців, проти України російська федерація веде так звану смислову війну.

Смислова війна [3, с. 234] є новим видом когнітивної зброї, складовою частиною сучасної російсько-української війни. Її мета охопити інформаційним впливом не окремий сегмент населення противника, а всі можливі соціальні групи, спроби детермінувати інтерес не до самих фактів, а до їх переосмислення. А кінцевою метою є прагнення сформувати на рівні масової свідомості хибних, не об'єктивних інтерпретацій. Смислова війна спочатку перемагає розум і тільки потім території. Ця війна стала складовою ще гібридної війни у 2014 р.

Інформаційна та смислова війна як складова війни росії проти України може бути віднесена до категорії особливих умов реалізації державної інформаційної політики в контексті соціальної небезпеки даного явища. По відношенню до останнього, у суспільстві ще не вироблена ефективна система організації протидії.

Аналіз сучасної воєнно-політичної ситуації, що складалась навколо України та її території, дає підстави вважати, що наша держава від самого початку проголошення незалежності, стала об'єктом потужних пропагандистських операцій та довготривалого психологічного впливу з боку російської федерації. «Гібридна» війна росії проти України з 2014 р. стала якісно новим підходом ведення воєнних кампаній, ключовим моментом яких є психологічна та інформаційна обробка місцевого населення, застосування жорсткої сили іміджевої дипломатії на підготованому геопросторі держави, що дозволило не лише проводити активну приховану інтервенцію на Сході України, обмежуючись заздалегідь добре підготованими та нечисленними диверсійними групами, однак озброєними сучасною бронетехнікою та іншими ефективними засобами наступу і оборони, але й анексувати на свою користь окремі території, зокрема Крим.

До того ж, в процесах становлення нової української державності на засадах демократії, законності та інформаційної відкритості загострилися протиріччя між потребами суспільства у вільному інформаційному просторі та необхідністю певних обмежень і відповідальності за негативні інформаційні впливи зовнішнього і внутрішнього походження. Визнаємо, що у сучасних умовах жодна держава не може функціонувати в інформаційній ізоляції. Адже інформаційні джерела на території будь-якої країни практично неможливо повністю убезпечити від витоку внутрішньої інформації та від зовнішнього інформаційного впливу. Останнє детермінувало потребу у формуванні дієвих механізмів захисту національних інтересів в інформаційному просторі.

Специфіка форм та методів реалізації державної політики інформаційної безпеки обумовлюється насамперед складними і багатогранними характеристиками самої інформації і інформаційних відносин. Насамперед, це стосується балансу між інформаційними свободами людини і необхідністю державного втручання в інформаційні відносини. Проблема цього балансу є першочерговою, враховуючи відсутність в Україні сталих демократичних

традицій, високу ступінь корумпованості і криміналізації держави і суспільства. Можливо часткове її вирішення полягає у площині реформування інформаційного законодавства та створенні дієвих механізмів захисту громадянами своїх прав. При цьому підкреслимо, що реформування влади в напрямку орієнтації на використання інформаційного ресурсу та регулятивного впливу ще не означає демократизму цієї влади. Навпаки, розвиток засобів масової комунікації та інформаційних технологій надає органам влади можливість здійснювати тотальний контроль щодо своїх громадян та маніпулювати свідомістю мас, що може привести до обмеження громадянських прав і свобод людини, формування нових типів зловживання владою. Таким чином ми підходимо до другого важливого аспекту, який саме і обумовлюється потенціалом демократичного суспільства у вирішенні питань інформаційної безпеки. Це стосується не лише контролю над владою через політичні механізми, але й діяльності великої кількості недержавних суб'єктів, від яких залежать умови інформаційних процесів в Україні. Це і підприємці, і працівники освіти, науки, культури, і політичні, громадські рухи тощо. Водночас, ефективна діяльність недержавного сектору можлива лише за умови демократичної системи влади в державі. Тому дотримання демократичних принципів вимагають від держави переважно застосовувати опосередковані економічні методи регулювання інформаційної сфери, допускаючи безпосереднє адміністративне втручання лише у вичерпному переліку випадків [4]. Але, з іншого боку, широке застосування економічних, опосередкованих методів впливу вимагає наявності значних матеріальних і фінансових ресурсів в державі, що з огляду на військове протистояння України та росії, накладає значні обмеження на можливості їхнього використання.

І, нарешті, третьою вимогою є задекларований принцип адекватності способів і методів захисту інформаційної безпеки конкретним загрозам. Цей принцип так само виступає стримуючим фактором від можливих утисків демократичних принципів та громадянських свобод під приводом захисту інформаційної безпеки. Дотримання принципу адекватності, насамперед, вимагає чіткого законодавчого визначення критеріїв і видів загроз інформаційній безпеці України, можливих дій у відповідь. В свою чергу, використання різних форм та методів регулювання інформаційної безпеки держави обумовлюється, передусім, специфікою об'єкту інформаційної безпеки.

На жаль, на сьогодні в Україні не сформована дієва система реальних гарантів її інформаційної безпеки, відсутній комплекс нормативно-правових актів щодо захисту інформаційних ресурсів та інформаційної інфраструктури. Процес інформатизації носить часто стихійний характер, з переважним ухилом у бік використання засобів інформатизації іноземного виробництва. З метою недопущення інформаційної експансії, діяльність держави в інформаційному просторі має координуватися у сферах реалізації упереджувальної стратегії та тактики, оперативного реагування на інформаційні атаки супротивника та захисту

національного інформаційного простору. В контексті останнього, пріоритетними завданнями інформаційних структур владних органів мають бути: контроль за інформаційними потоками, надання об'єктивної, вичерпної інформації, представлення фахових коментарів та пояснень щодо подій, систематичне висвітлення офіційної позиції посадових осіб та політичних лідерів [1, с. 30-31].

Погоджуємося із позицією вітчизняних науковців, що у перспективі, серед базисних завдань державної інформаційної політики, пріоритетними мають стати: інтеграція України до світового та регіонального європейського інформаційного просторів; створення власної національної моделі інформаційного простору та забезпечення розвитку інформаційного суспільства; модернізації усієї системи інформаційної безпеки держави та формування й реалізація ефективної інформаційної політики; удосконалення законодавства з питань інформаційної безпеки, узгодження національного законодавства з міжнародними стандартами та дієве правове регулювання інформаційних процесів; ефективна взаємодія органів державної влади та інститутів громадянського суспільства під час формування, реалізації та коригуванні державної політики в інформаційній сфері [2].

Наголосимо, що в умовах складних викликів сьогодення, питання забезпечення інформаційної безпеки для України знаходяться на одному рівні із захистом суверенітету і територіальної цілісності. Робота над концепцією інформаційної безпеки України повинна бути спрямована на систематизацію питань, щодо її належного забезпечення, визначення методів і засобів її захисту створення засад для розвитку інформаційного простору країни.

Література

1. Ільницька Уляна Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. *Політичні науки*. Vol. 2, No. 1, 2016. С. 27-32.

2. Копанчук В. О. Інформаційна безпека як складова національної безпеки України: сучасні виклики та механізми протидії негативним інформаційно-психологічним впливам. .URL:http://repositsc.nuczu.edu.ua/handle/123456789/10698. (дата звернення 13.03.2023).

3. Почепцов. Г. Г. Сучасні інформаційні війни. К.: Вид. дім «Києво-Могилянська академія», 2015. 497с.

4. Шамрай В.О. Інформаційна безпека як складова національної безпеки України. URL:http://www.crimeresearch.ru/ (дата звернення 13.03.2023)

Гуськова Е.О.
викладач кафедри стратегічних комунікацій
навчально-наукового центру стратегічних комунікацій
у сфері забезпечення національної безпеки та оборони
Національного університету оборони України

ОРГАНІЗАЦІЙНІ ЗАСАДИ ПРОТИДІЇ ПОШИРЕННЮ РОСІЙСЬКИХ НАРАТИВІВ У МЕДІА ЗАДЛЯ ЗМІЦНЕННЯ СУСПІЛЬНОЇ ДОВІРИ ДО БЕЗПЕКОВОГО СЕКТОРУ

Відколи росія широкомасштабно вторглася на територію Україну, фейки, брехливі твердження та маніпуляції поширюються серед підконтрольних агресору медіа невпинно. путінська пропаганда стала одним з головних елементів війни в Україні. Варто зазначити, що центральною темою кремлівської пропаганди є створення образу нацистської держави. Як стверджують данні американської компанії Semantic Visions, яка займається аналітикою у сфері оборони, кількість повідомлень щодо виправдання військового вторгнення на територію України та зображення України захопленою ультраправими екстремістами у російських медіа досягли безпрецедентного рівня 24 лютого 2022 року. З того часу вони залишаються високими. [1]

Наратив росії про те, що її вторгнення в Україну є спробою «денацифікувати» країну, зазнало критики з боку Антидифамаційної ліги США, Меморіального музею Голокосту та багатьох вчених, які досліджують нацизм. Незважаючи на відсутність доказів того, що в Україні домінують нацисти, ця ідея прижилася серед багатьох росіян. Хибні заяви про Україну фігурують у державних російських ЗМІ і посилюються у стрічках новин сайтів. Ключовою особливістю російської пропаганди є її повторюваність, зокрема і необгрунтованих тверджень про нацизм. За даними Semantic Visions, після вторгнення в 10-20% статей про Україну згадувався саме нацизм.

Лариса Дорошенко, дослідниця Північно-Східного університету, яка вивчає дезінформацію, вважає, що така стратегія, швидше за все, була спрямована на те, щоб виправдати те, що, як сподівався кремль, стане швидким поваленням українського уряду.

Доволі часто мішенню російської дезінформації стають Збройні сили України та сектор безпеки та оборони в цілому. На нашу думку, інформаційна атака обумовлена високим рівнем довіри до українського безпекового сектору. Так, за час війни довіра до Збройних сил України зросла з 65% до 97%, до Президента України Володимира Зеленського – з 36% до 90%. Про це свідчать дані комплексного дослідження Соціологічної групи «Рейтинг» на тему.

Російські новини стверджують, що мовляв українські нацисти використовують некомбатантів як живий щит, вбиваючи українських цивільних

осіб та плануючи геноцид росіян. Наведемо кілька фейків, які країна-терорист поширювала в медіа просторі. Батальйон «Азов» використовується російськими ЗМІ з 2014 року як приклад ультраправої підтримки в Україні. Аналітики стверджують, що зображення групи російськими ЗМІ перебільшує ступінь, у якому її члени дотримуються неонацистських поглядів. Між тим російське телебачення регулярно транслювало у негативному ракурсі батальйон у квітні 2022 року, коли члени групи захищали металургійний завод в обложеному місті Маріуполі.

Ще в 2014 році на російських порталах з'явилася новина про те, що «бандерівець» поїдає руку росіянина. Виявилось що фото зі зйомок російського фантастичного фільму 2008 року «Ми з майбутнього». Світлину можна побачити в соціальній мережі «Вконтакті» в альбомі користувача Максима Мака, який працював художником-реквізитором на зйомках цього фільму . Про те, що рука, яку чоловік тримає біля свого обличчя, це муляж, а сам чоловік – художник-реквізитор, свідчать інші фото з цього ж альбому.

Під час повномасштабного вторгнення російські пропагандисти запустили фейк, що українські жінки-військові нібито поширюють нацистські заклики у застосунку для знайомств Tinder. Розслідувачі фактчекінгового ресурсу StopFake поспілкувалися з однією з дівчат, чиї фото публікували пропагандисти – Шурою Рязанцевою. З'ясувалося, дівчина служить у лавах ЗСУ та не має профілю у Tinder. Світлину для фотофейку росіяни взяли з її Instagram-акаунту.

У деяких випадках російську пропаганду якісно закамуфльовано під виглядом матеріалів відомих західних ЗМІ, таких як BBC, CNN або DW. Особливу роль відіграють мультимедійні фальшивки: відео, фотографії та скріншоти, які насправді є маніпуляцією або ж навіть повною вигадкою. Деякі з таких публікацій стають «вірусними», охоплюючи аудиторію у сотні тисяч, а іноді в мільйони користувачів.

Фальшиве відео ракетного обстрілу Краматорська «від BBC». Після російського ракетного обстрілу краматорського вокзалу, який стався 8 квітня 2022 року і забрав багато життів, було багаторазово поширено відео під логотипом британської телекомпанії BBC. Його встигли переглянути півмільйона користувачів. Поширення відбувалося здебільшого з проросійських облікових записів. У ньому були зображені трупи в Краматорську та впала неподалік ракета. У тексті стверджувалося, що її випустили українські війська по власному народу. Корпорація BBC негайно виступила зі спростуванням та назвало відео «фейком».

13 квітня 2022 року фейкове відео BBC скоординовано поширили численні акаунти. німецькою, англійською, італійською, іспанською, каталонською, індійською та французькою мовами протягом кількох годин. Більшість облікових записів мають одну спільну рису: інформацію про їхні профілі неможливо ідентифікувати з реальними людьми. Було використано весь шаблон BBC: логотип, титри та стиль, щоб надати фейковому відео справжнього вигляду.

Фейкове відео, яке брендують логотипами авторитетних західних ЗМІ, називають «класикою фальшивих прапорів». Ця тактика добре відома і дуже популярна для введення громадської думки в оману. Огортаючи дезінформацію під виглядом надійного медіа-бренду, по-перше, підвищується довіра до інформації, по-друге, дуже легко достукатися до користувачів та сприяти поширенню дезінформації. [2]

Таким чином, фальшиві відео з логотипом відомих ЗМІ можуть навіть призвести до того, що споживач інформації не поставить під сумнів відео повідомлення.

Хто стоїть за цими дезінформаційними атаками? Слід, що веде до справжніх авторів фейкових відео, фотографій чи твітів, не завжди можна відстежити. Однак експерти знаходять вказівки на те, що за виробництвом фальшивок стоять професійні структури росії. Значну частину проросійської дезінформації можна віднести до авторства Агентства інтернет-досліджень (IRA) – російської «фабрики тролів», яка працює з 2012 року. IRA стала відомою через спроби вплинути на президентську виборчу кампанію в США в 2016 році. З 2014 року поширювалися численні хибні повідомлення також про Україну, які приписують IRA.

Аби не потрапити на гачок пропагандистів, фахівці радять розвивати критичне мислення, робити крос-перевірку новини, читати далі заголовка, перевіряти зображення, звертати увагу на грамотність тексту та джерело поширення новини. Чи входить сайт до переліку токсичних, чи навпаки цей сайт є серед «білого списку сайтів» з високим рівнем довіри. Так, до списку найякісніших і відповідальних онлайн-медіа, який підготували експерти IMI на основі моніторингових досліджень, що здійснювалися у період з липня по вересень 2022 року увійшли такі редакції: Суспільне, Громадське, Ліга, Українська правда, Укрінформ, Радіо Свобода, Дзеркало тижня, НВ, та Бабель. За результатами аналізу, рівень дотримання професійних стандартів на ресурсах, які ввійшли до Білого списку, в середньому становить близько 96%.

Для того, щоб споживач інформації міг покладатися не лише на свої знання з медіаграмотності, і швидше виявляти сайти з фейковим контентом, існують спеціальні плагіни для браузера Chrome. На жаль, плагіни вміють обробляти лише англомовні матеріали, а плагіни, які б аналізували інші мови поки що відсутні і є чудовим полем для наукових і IT-розробок. Антифейкові-плагіни тестувалися на відомих сайтах з фейковим контентом, приміром, American News, Infowars, гумористичний The Onion.

Fake News Detector – плагін виявляє фейкові новини або потенційно маніпулятивний контент, зокрема і в Facebook. Поряд з назвою фейкової новини з'являється червоним кольором слово FAKE. Така ж позначка додається поруч із посиланням на потенційно фейкове джерело. Маніпулятивне посилання позначається помаранчевими словами CLICKBAIT або PROBABLY FAKE.

Fake News Detector AI – плагін оцінює сайти на наявність джерел фейкових

новин за допомогою штучного інтелекту. Плагін додає кнопку на панель інструментів браузера. Відкривши сайт, ви можете натиснути на кнопку і отримати повідомлення про те, чи є сайт надійним джерелом інформації.

NewsCracker – плагін також використовує технологію машинного навчання і статистичний аналіз для визначення фейкових новин. Щоб використовувати плагін, потрібно відкрити статтю, яка викликає сумнів, і натиснути на кнопку плагіна, розташовану на панелі інструментів Chrome. Плагін NewsCracker оцінює матеріал за шкалою від 0 до 10. Перевіряючи статтю на предмет потенційної неточності або упередженості, плагін використовує три оцінки – точність, нейтральність тексту і нейтральність заголовка. NewsCracker вважає, що можна довіряти статті, коли її загальний бал вище 8.0, не рекомендується довіряти статті, коли оцінка нижче 6.0. Статті, які отримали оцінку між між 6.0 і 8.0, викликають сумнів. Статті з відомого фейковий сайту americannews.com за допомогою плагіна NewsCracker отримали оцінку нижче 6.0. Матеріали з таких джерел як The New York Times і Washington Post отримали оцінку вище 9.0.

Література

1. How the Russian Media Spread False Claims About Ukrainian Nazis. URL: https://www.nytimes.com/interactive/2022/07/02/world/europe/ukraine-nazis-russia-media.html (дата звернення: 19.03.2022)
2. Фактчек: фейки під логотипами всесвітньо відомих ЗМІ. URL: https://www.dw.com/uk/faktchek-feikovi-novyny-pid-falshyvym-praporom-a-62391942/a-62391942 (дата звернення: 19.03.2022)

Даник Ю.Г.
д.т.н., професор,
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Шестаков В.І.
д.т.н., доцент

РИЗИКИ ДЕСТРУКТИВНИХ КОГНІТИВНИХ ВПЛИВІВ НА РІЗНІ ЦІЛЬОВІ АУДИТОРІЇ ТА ПРОБЛЕМИ КОМПЛЕКСНОЇ ПРОТИДІЇ ЇХ РЕАЛІЗАЦІЇ

В доповіді розглядаються загрози і ризики деструктивних когнітивних впливів на різні цільові аудиторії.

Доведено, що ризики реалізації загроз деструктивних когнітивних впливів залежать від об’єктів, методів, технологій, часових параметрів і каналів впливу тощо. При цьому, самі впливи можуть бути, як свідомими та цілеспрямованими, так і несвідомими, часто випадковими, а також можуть мати змішаний характер. В

сучасних умовах вони найчастіше здійснюються в кіберінформаційному просторі або через кіберінформаційний простір. Вони, в умовах високотехнологічного, інформаційного, цифрового суспільства, стали реальним і дієвим інструментом трансформації систем цінностей, інтересів та світоглядних засад тих, на кого вони спрямовані. Це несе в собі високі ризики реалізації зовнішнього когнітивного управління об'єктами на які такий вплив здійснюється.

Встановлено, що процес когнітивної трансформації різних цільових аудиторій здійснюється з використанням методів ментального, образного, наукового і лінгвістичного (мовного) тощо впливів та має різні рівні складності.. При цьому, незважаючи на достатньо велике різноманіття форм, способів, методів і каналів здійснення деструктивних впливів в когнітивній сфері, впливи через сфери освіти і науки є найбільш ймовірними і небезпечними тобто ризик їх здійснення саме через ці сфери є найбільшим. В цілому, завдячуючи розвитку інноваційних і високих технологій, варіанти реалізації деструктивних когнітивних впливів стають все більш різноманітними. В доповіді розглядаються деякі найбільш характерні і небезпечні з них. Так дослідження варіантів деструктивних когнітивних впливів, показало, що вони в сучасних умовах здійснюється переважно через соціальні мережі, блогосферу, художню, науково-популярну і наукову літературу, релігійну мережу, розважальну і професійно-орієнтовану аудіо і відеопродукцію, рекламу, ЗМІ, а також шляхом введення змін, які сприяють цьому, в наукові теорії, навчальні програми, освітні стандарти.

Інформаційні технології і електронне дистанційне навчання, які, зважаючи на кризові ситуації, стали фактично порятунком для сфери освіти в умовах криз викликаних пандемією і війною стали найбільш потужним інструментом для здійснення комплексних когнітивних впливів. У зв'язку із запровадженим і вимушеним режимом самоізоляції з'явилося і мають свої аудиторії безліч онлайн-сервісів з навчання та саморозвитку – різноманітні курси, віртуальні екскурсії, майстер-класи, які не проходять ніякої експертизи з точки зору когнітивної безпеки.

Тому, надзвичайно важливими є своєчасні аналіз і оцінка ризиків пов'язаних з можливостями, які можуть бути використані деструктивними акторами в цій сфері. Це дозволить забезпечити своєчасне виявлення, запобігання і нейтралізацію ризиків і загроз деструктивних когнітивних впливів. Тому, проведення їх досліджень є актуальним і необхідним для позитивного вирішення нагальних питань забезпечення національної безпеки. Доведено, що під час різноманітних катаклізмів, як окремі особи так і суспільства в цілому стають більш вразливими для зовнішніх деструктивних когнітивних впливів, досліджені їх феномени та запропоновані можливі варіанти виявлення та нейтралізації таких впливів.

У доповіді представлені результати аналізу зумисних та ненавмисних факторів, які можуть вплинути на реалізацію загроз національній безпеці пов'язаних з деструктивними когнітивними впливами в кіберінформаційному

просторі або через кіберінформаційний простір куди перенеслися значна кількість сфер людської життєдіяльності.

Це є особливо актуальним, в умовах стрімкого розвитку штучного інтелекту, інформаційних і кібертехнологій та сучасних кризових ситуацій.

Даниленко В.М.
д.і.н., професор,
Національна академія СБ України

УКРАЇНСЬКА КУЛЬТУРА ЯК ІНФОРМАЦІЙНИЙ ЧИННИК НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Повномасштабне російське вторгнення в Україну призвело до своєрідного інформаційного вибуху у сфері історії українсько-російських відносин. Ретроспективна інформація в царині економіки, політики, культури динамічно актуалізувалась і стала фундаментальною основою світоглядного переформатування українського суспільства у ставленні до Росії як до держави-терориста та до її населення (народу) як співучасника військової агресії.

Переосмислення московської політики щодо України відбувається швидкими темпами і віддзеркалюється у засобах масової інформації, насамперед у мережі Інтернет, закріплюється у національних та міжнародних нормативно-правових актах. Об'єктивне інформування української та світової громадськості про минуле і сучасне України та її територій, спростування дезінформацій, у тому числі ідеологем радянської та російської історіографії, визначено одним із завдань забезпечення інформаційної безпеки України [1]. Протягом останніх років з'явилися грунтовні друковані видання з результатами досліджень українських істориків, філософів, політологів, які розкривають ідеологічне спрямування численних російських міфів про українську історію та культуру і доводять, що різновидом російсько-української війни є війна за свідомість, за культурну спадщину [2]. У найновішій праці колектив відомих українських науковців (І. Гирич, Б. Гуменюк, Л. Масенко, В. Огнев'юк, В. Огризко, О. Палій, В. Піскун, П. Полянський та ін.) представив трактування рашизму як ідеології й суспільної практики сьогодення [3].

Відкрите цинічне посягання на землі й культурну спадщину України з боку російських політиків у новітню добу дістало пряме підтвердження у статті президента рф, опублікованій російською та українською мовами на кремлівському сайті в липні 2021 р. під назвою «Про історичну єдність росіян та українців». Це був інформаційний пролог нового етапу загарбницької неоколоніальної й геноцидної війни Росії проти України. Російське керівництво відкрито проголосило завдання остаточно й назавжди вирішити «українське

питання» – завершити багатовікову московську експансію на українських землях, повністю асимілювавши українців і ліквідувавши їх національну ідентичність.

У розв'язаній Росією війні проти України зіткнулися не тільки війська, але й ідеології та культури. Культуролог Сергій Палаш слушно вважає, що у нинішньому російсько-українському протистоянні зійшлися західна культура в особі України і традиційна російська культура, яка представляє окрему цивілізацію, отже, йде війна культур, цивілізацій [4].

У боротьбі московитів проти України впродовж минулих століть незмінно використовувались ті ж засоби, що й у нинішній війні. Інформаційна складова поєднувала риторику про необхідність захисту православ'я (тепер – «русского мира»), видавала агресію за внутрішній конфлікт, за потребу захисту від зовнішнього впливу, а культурну спадщину українців і їх самих, як окремий від росіян народ, – за позбавлені історичної основи уявлення.

Російський месіанізм та експансіонізм, втілений у теорію «русского мира» й збройну агресію проти України, спростував велич і духовні цінності російської культури і натомість рельєфно висвітлив переваги культури української, на якій зросли національні герої.

Український народ і його захисники перебувають в епіцентрі світових подій і служать щитом для країн демократії, надихаючим прикладом героїзму для людства. Для воїнів у лавах Збройних Сил України, волонтерів, усіх, хто протистоїть небезпечному ворогу, національна культура – явище не абстрактне, а цілком конкретне. Втрати близьких і рідних, руйнування батьківських домівок, від народження знайомих і дорогих пам'яток культури, в яких зберігався генетичний код рідного краю, родини і нації, спонукають до безкомпромісної жертовної боротьби з російським агресором.

Значна роль у підвищенні обороноздатності держави належить національному спротиву. Надання обороні України всеохоплюючого характеру передбачає низку завдань, зокрема, участь у інформаційних заходах, спрямованих на підвищення обороноздатності держави та на протидію інформаційним операціям агресора (противника) [5].

Руйнування природної спадщини, матеріальної й нематеріальної культури, подібно до часів нацистської окупації в роки Другої світової війни, зачепили усі регіони України. Кількість пограбованих і вивезених у Росію предметів лише державного музейного фонду України обчислюється десятками тисяч. Пошкоджено або повністю зруйновано близько 1300 об'єктів культурної інфраструктури [6]. Не може не викликати спротиву таврування рашистською пропагандою українських державних символів, переслідування і вбивства російськими військовими українців за мову, національні традиції, звичаї й уподобання.

Українська культура виступає важливим інформаційним чинником в російсько-українській війні, яка точиться за українську історичну й культурну

спадщину, національну ідентичність, саме існування українців як державотворчої нації. Ницість і агресивність північних сусідів консолідували українське суспільство, покликали до життя прийняті на найвищому рівні рішення про стратегію національної безпеки України. Забезпечення всебічного розвитку української культури та утвердження української громадянської ідентичності є стратегічною ціллю Стратегії інформаційної безпеки України. Справедливим буде також законодавче закріплення положення про те, що збереження культурної спадщини та національної пам'яті, духовних цінностей українського народу – один із пріоритетів національної безпеки.

Література

1. Стратегія інформаційної безпеки. Рішення Ради національної безпеки і оборони України, затверджене Указом Президента України від 28 грудня 2021 року № 685/2021. Інтернет-ресурс : https://www.president.gov.ua/documents/6852021-41069.

2. Брехуненко В., Ковальчук В., Ковальчук М., Корнієнко В. «Братня навала». Війни Росії проти України XII–XXI ст. – Київ, 2016. – 248 с.; Брехуненко В. Війна за свідомість. Російські міфи про Україну та її минуле. – Київ, 2017. – 280 с.

3. Заборонити рашизм. За заг. ред. В. Піскун. – Київ : Київ. ун-т ім. Б. Грінченка, 2023. – 252 с.

4. Палаш С. Війна культур / Інтернет-ресурс : https://lb.ua/blog/serhiy_palash/508153_kulturna_viyna.html.

5. Закон України «Про основи національного спротиву». Інтернет-ресурс : https://zakon.rada.gov.ua/laws/show/1702-20#n294.

6. Інтернет-ресурс :https://risu.ua/povernennya-vikradenih-rosiyeyu-kulturnih-cinnostej-mozhe-trivati-rokami-minkult_n137553.

Данильян О.Г.
д.філос.н., професор,
Національний юридичний університет імені Ярослава Мудрого
Дзьобань О.П.
д.філос.н., професор,
Національний юридичний університет імені Ярослава Мудрого

ІНФОРМАЦІЙНІ ВПЛИВИ ЧЕРЕЗ ЗМІ ЯК БАЗОВИЙ ЕЛЕМЕНТ ІНФОРМАЦІЙНОЇ ВІЙНИ РОСІЇ ПРОТИ УКРАЇНИ

Інформаційна війна – це цілеспрямований вплив на суспільну свідомість противника для досягнення інформаційної переваги, політичних чи військових цілей шляхом заподіяння шкоди інформації та інформаційним системам

супротивника. Наше уявлення з цього питання виходить із того, що, по суті, інформаційна війна, перш за все, є технологією системного впливу на масову та суспільну свідомість, тобто маніпулятивною технологією. Однак у порівнянні з технологіями соціально-психологічного та ідеологічного маніпулювання, інформаційна війна виступає найдосконалішим, найскладнішим за структурою (поєднує різні технології та способи маніпулятивного впливу) видом інформаційного впливу, і, водночас, найдеструктивнішим за наслідками. Цілями такого впливу є зміна суспільної свідомості супротивника, досягнення над ним інформаційної переваги для подальшої зміни його поведінки.

Основним методом інформаційної війни є поширення дестабілізуючої інформації, яка розповсюджує песимізм, страх і пасивність, зневіру у політичному керівництві держави тощо. До основних способів цього методу варто віднести:

- суб'єктивну інтерпретацію подій (часто за рахунок демонстрації жертв своїх злочинів, які видаються за злочини супротивника);
- апеляцію до бінарного мислення, у якого сприймаються або лише позитивні, або лише негативні події. Подібний тип мислення створює ідеального «солдата» інформаційної війни»;
- визначальний характер бездоказових висновків, як підстави яких може використовуватися вже нібито «доведений» фрагмент міфологічної медіа-картини світу;
- побудова абстрактних узагальнень на основі поодиноких випадків та перенесення окремих деталей на оцінку всієї події в цілому;
- перебільшення можливих наслідків подій, що розглядаються.

Сучасні дослідники виділяють зазвичай наступні групи прийомів психологічного впливу:

- «психологічний тиск» з метою придушення здібності раціонально мислити (багаторазове повторення однієї й тієї ж помилкової тези, апеляція до авторитетів, маніпуляція фактами, вибірковий підбір інформації, створення психологічного дискомфорту тощо);
- «непомітне проникнення у свідомість» – «метод пряника», на противагу попередньому «методу батога» – через неявне поширення цінностей через культуру, насамперед через масову, моду, розваги, мистецтво (чутки та плітки, створення псевдофольклору, оприлюднення художніх творів з метою дискредитації опонентів тощо);
- «приховане порушення та спотворення законів логіки» – різні софістичні методи полеміки. Даний метод особливо ефективний по відношенню до малоосвічених верств населення, яким важко зрозуміти, де в побудовах криється логічна помилка. Інформаційні впливи – крайнє вираження взаємозв'язку ЗМІ та політики;
- «навмисне відволіканні від значущої інформації». Найбільш показовим у цьому відношенні є сучасна війна Росії проти України, де зазначений прийом

проявляється у тому, що російські й деякі західні проросійські ЗМІ дають дозований (як би «між іншим») огляд подій в українських населених пунктах тільки після початку широкого резонансу у світових ЗМІ, а агресивні і вкрай жорстокі дії Росії проти цивільного населення України розглядалися виключно викривлено, однобоко, з активними спробами звинуватити в усьому «українських неонацистів». Такі «відфільтровані» російською цензурою повідомлення подаються на тлі «видатних здобутків» російської економіки і «історичної визвольної місії» російської армії.

Досвід війни Росії проти України свідчить, що застосування Росією інформаційно-психологічної зброї у медіапросторі шляхом агресивного впливу на свідомість і підсвідомість здійснюється за наступними основними напрямками:

- забезпечення прийняття військово-політичним керівництвом України бажаних для Росії рішень і спонукання до виконання нав'язуваних політичних, економічних і воєнних кроків;
- підрив легітимності української політичної влади;
- підрив міжнародного авторитету України, створення її негативного іміджу з метою недопущення широкомасштабної військової, економічної та фінансової допомоги європейських країн та США;
- дестабілізація ситуації у цілому в Україні, провокування політичних протестів, соціальних конфліктів, підрив морально-психологічного стану українського населення;
- підрив обороноздатності України та боєздатності її Збройних Сил;
- підтримка дій внутрішніх деструктивних сил і колаборантів, спрямованих на знищення чи завдання шкоди українській державі і суспільству, у тому числі шляхом корумпування влади й політичної еліти;
- створення негативного образу українця шляхом розповсюдження фейків про «неонацизм», «бандерівців», діаметрально протилежне істинним подіям висвітлення військових злочинів російської армії;
- заміна соціально-культурної ідентичності всього населення України або його частини, нав'язування сумнівів стосовно національних цінностей та засад державотворення.

І цей перелік можна продовжувати й конкретизувати.

Інформаційно-психологічна зброя як інструмент інформаційної війни спрямовується Росією на придушення, знищення, дезорганізацію, дезорієнтацію, дезінформацію, дезадаптацію об'єкта впливу.

Гібридні атаки в інформаційній площині здійснюються і через традиційні медіа (телебачення, пресу, радіо), і через соціальні онлайн-мережі. Причому, з інформаційними атаками в соціальних медіа традиційні методи боротьби не дають бажаних результатів. У такому разі необхідно шукати інші засоби і передусім необхідно працювати на випередження, формуючи відповідний рівень критичного мислення в суспільстві.

Для реалізації визначених завдань провідне значення має досконале знання та розуміння процесів, що відбуваються в межах національного інформаційного поля, знання й розуміння того, як реагує індивід на будь-які прояви інформаційної агресії і як він сприймає різні джерела інформації.

Щоб нейтралізувати наслідки інформаційної війни сторона-жертва агресії має використовувати такі ж технології і методи, як і сторона-агресор, тобто, застосовувати технології інформаційної війни аналогічним способом, але вже у своїх цілях (для відбиття інформаційних атак агресора).

Проблема нейтралізації наслідків інформаційної війни з необхідністю корелюється з проблемою інформаційної безпеки, яка, у даному контексті, має розглядатися крізь призму проблеми пристосування суб'єкта інформаційних відносин до умов, пов'язаних з кібератаками та іншими агресивними інформаційними впливами.

Діміч А.В.
доцент, д.ю.н.,
доцент кафедри УІАЗ ОСД ННІ ІБСК

ОКРЕМІ ЧИННИКИ, ЩО ВПЛИВАЮТЬ НА ЛОГІСТИЧНЕ ЗАБЕЗПЕЧЕННЯ СУБ'ЄКТІВ ДЕРЖАВНОЇ БЕЗПЕКИ УКРАЇНИ

Логістичне забезпечення суб'єктів державної безпеки України у ході ведення бойових дій є ключовим фактором виконання стратегічних і тактичних концепцій та невід'ємною умовою досягнення перемоги. Логістичне забезпечення спрямоване на підвищення ефективності забезпечення Збройних Сил України за рахунок скорочення витрат на їх забезпечення та підтримання у бойовій готовності [1], зменшення часу поставки військової техніки, боєздатного озброєння до військових частин (підрозділів), які виконують поставлені завдання та захищають незалежність України.

Окрім військових, економічних і технічних факторів окремі науковці виділяють ще соціальні та геополітичні, які впливають на систему логістичного забезпечення Збройних Сил України [2]. На думку автора, ще здійснюють свій вплив географічні, кібернетичні, міжнародні та інші чинники. А тому актуальність даного дослідження є своєчасним для подальшого розвитку логістичного забезпечення суб'єктів державної безпеки України.

У аспекті питання, що розглядається важливо акцентувати увагу на економічному факторі, який є одним із визначальних чинників, оскільки після російських обстрілів кричної інфраструктури України збільшилися темпи спаду національної економіки в листопаді 2022 р. до листопада минулого 41 %. У цілому на 2022 р. прогноз падіння ВВП Уряд погіршив з 32 до 33,2 %. Також за даними

Державної служби статистики, інфляція у листопаді 2022 р. 26,5 % у річному вимірі, і в 2023 р. на значне її сповільнення очікується. Водночас, суттєвою підтримкою України є міжнародна фінансова допомога, яка складає від початку війни понад 113 млрд євро, ця сума охоплює військову, фінансову та гуманітарну допомогу від урядів іноземних держав [3].

У сьогоденних умовах ведення бойових дій в Україні, геополітичний фактор має суттєвий вплив на логістичне забезпечення суб'єктів державної безпеки України. Лідерами серед постачальників важкої зброї Україні є США, Великобританія та Польща, але поставку зброї та інших матеріально-технічних ресурсів для потреб армії ускладнено через закриття повітряного простору та морських портів «Маріуполь», «Бердянськ» й «Скадовськ».

Окрім цього, важливим вбачається й інформаційно-технічний чинник. Зокрема, в реаліях сьогодення цьому сприяє сухий порт (логістичний хаб) – це мультимодальний логістичний центр із інфраструктурою, що дозволяє власнику вантажу користуватися всіма перевагами морського порту, але на суші. Наприклад, на Рівненщині вже з березня 2021 р. працює сухий порт Одеської компанії Imtrex, на заході України – Західний контейнерний термінал тощо. У період дії правового режиму воєнного стану в Україні їхні логістичні можливості набувають вагомішого значення, зокрема і для перевалки зернових. І ці термінали працюють як на експорт, так і на імпорт. В умовах, коли через морські порти України отримати вантажі майже неможливо, розглядається можливість вивантаження в інших портах Чорного моря, наприклад у Румунії, і доставку в Україну залізницею через західний кордон. Важливим є і той факт, що це стосується і доставки до України озброєння та іншої військової техніки.

Таким чином, для ефективного функціонування системи логістичного забезпечення суб'єктів державної безпеки України необхідно враховувати усі чинники, що впливають на її своєчасність. Відсутність стратегії розвитку у сфері логістичного забезпечення суб'єктів державної безпеки України, недооцінювання її ролі у підтримці національної економіки, а також низьку якість кадрового потенціалу сприятиме неефективному управлінню матеріально-технічними ресурсами країни.

Література

1. Основні положення логістичного забезпечення Збройних сил України [Електрон. ресурс]: наказ МОУ від 11 жовтня 2016 № 522. – Режим доступу: http://www.mil.gov.a/ministry /normativnopravova-baza/nakazi-ministra oboroniuk raini/nakazi-ministerstva-oboroni-ukrainiza-2016-rik. html.

2. Тесніков О.М. Фактори впливу на функціонування системи логістичного забезпечення ЗСУ в умовах війни / Тесніков О.М., Фурсова В.А. // Економіка та суспільство. № 42. 2022.

3. Міжнародна допомога Україні перевищила 113 мільярдів євро [Електрон. ресурс]: – Режим доступу: http://www.ukrinform.ua/rubric-economy/3654202-miznarodna-dopomoga

Єрьоміна Л.В.
старший викладач КІБД
Національної академії СБ України
Андрійчук М.О.
студент Національної академії СБ України

МІФ РОСІЇ ЩОДО ЗАХІДНОЇ ЧАСТИНА УКРАЇНИ ЯК СПІРНОЇ ТЕРИТОРІЇ

Протягом багатьох років росія проводила політику русифікації українців на ґрунті того, що росіяни та українці це нібито один народ. Коріння даного твердження можна знайти ще у міфі «Русь = росія». Суть даного міфу полягає у тому, що на думку багатьох росіян, Руссю є центральна частина України та південна частина Білорусі спираючись на старі географічні та політичні карти Русі, тим самим виділяючи інші частини території нашої держави як спірні між різними народами.

Така політика необхідно для того, щоб заявити права на східну, південну та центральну частину України, проведення пропаганди, що коли ці території повернуться до росії, то західна частина України буде розділена між Польщею, Угорщиною та Румунією або буде виділена як окрема держава. Це можна вважати політикою залякування, яка здійснюється з метою посіяти розбрат, підсилити сепаратистські рухи національних меншин на нашій західній території.

Для росіян надзвичайно травматично усвідомлювати, що їх предки довгий період часу займали навіть не друге, а скоріше третє місце в історії Русі, та найчастіше вони були васалами різних кочових племен (хазарів, половців та Золотої Орди). Для них втішною є думка, що коли прийшла Золота Орда, вони були не єдині, хто був васально залежний від орди та платив данину, а також ними роздувається міф, що центр Русі перейшов з Києва до Володимиро-Суздальського князівства (тодішня назва Московського князівства). Хоча саме в цей період часу ті, хто вцілів від розорення земель Русі зміг знайти прихисток в Галицькому та Волинському князівствах. В подальшому саме Роман Мстиславович (князь Волинський, той хто об’єднав Галич та Волинь) намагався вести боротьбу як політичну так і військову проти загарбників у вигляді Золотої Орди, тим самим руйнуючи міф росіян, що центр Русі перейшов до них, оскільки неможливо перемогти народ, якщо хтось продовжує боротися, якщо народ бореться – він існує. В подальшому його нащадок Данило Галицький продовжив справу свого батька. Він намагався об’єднати удільних князів, які вціліли після приходу Золотої

Орди, та заручився підтримкою західних країн та католицької церкви Ватикану, прийняв корону монарха католицького тим самим надавши Галицько-Волинському князівству в статус королівства, тому його держава в західних латинських джерелах отримала назву «Королівство Русь». Саме тому ми справедливо вважаємо, що новий центр Київської Русі став Галич та Волинь.

Міф про «бандеровцеві нацистів», також частина пропаганди московітів, яка спрямована на розкол українців. Суть міфу полягає у тому, що коли українські землі були окуповані військами Вермахту, ОУН та УПА були колабораціоністами та боролися з партизанськими рухами червоної армії.

Насправді, ще до початку Другої Світової війни Організація українських націоналістів вже вела діяльність по боротьбі з польською окупацією аж до 1939 року, та подальшу боротьбу з радянським режимом у 1939-1941 роках. Після нападу 22 червня 1941 Німеччини на срср, слідом за фронтом, що швидко рухався на схід, були відправлені невеликі загони оунівців («похідні групи») по 7-12 вояків, які формували українські органи місцевого самоврядування та поліцію. Слідом за цим націоналісти розгорнули масштабне повстання в тилу червоної армії. Партизани ОУН нападали на відступаючі підрозділи червоної армії і НКВС, закликали населення не допомагати червоноармійцям, нападали на в'язниці з політичними ув'язненими. 30 червня 1941 року у Львові ОУН під проводом Степана Бандери та спільно з Ярославом Стецьком проголосили «Акт відновлення Української Державності». Цей акт був негативно сприйнятий німцями, оскільки вони не планували створювати державу, лише завойовувати, тому всіх учасників акту що перебували у Львові було затримано та заслано в концтабори. Саме це можна вважати початком війни українського народу проти Вермахту, з 1942 року ОУН почали формування власні збройні підрозділи та об’єднали сили з підрозділами Тараса-Бульби Боровця. Це були перші підрозділи УПА під проводом Бульби та в подальшому під проводом ОУН. Попри те, що Друга Світова війна майже для всього світу закінчилась 1945 року, для українців вона тривала до кінця 50-х, за деякими джерелами до 60-х.

І справді, наші землі дуже часто були спірними між великою кількістю країн, та ніхто не зміг їх повністю підкорити, утримання цих земель давалось дуже великою ціною. Так було за часі Речі Посполитої – коли ставались постійні козацькі повстання, найвдаліше із яких отримало назву «Визвольна війна українського народу (революція Хмельницького)», так було під час та після Першої Світової війни, коли колишні бійці легіону УСС під керівництвом Українського Генерального Військового Комісаріату (УГВК) захопили владу у Львові та утворили Західну Українську Народну Республіку (ЗУНР) (більш детальніше про ці події був знятий документальний фільм «Легіон – хроніка УГА 1918-1919»), навіть сьогодні ми боремося не за якийсь окреми край, а за єдину Українську державу.

Тож тепер ми можемо сміливо говорити, що вся московська пропаганда, яка

направлена на українців західної частини нинішньої України, є причиною того, що ворог усвідомлює, що за будь-яких умов не зможе ні підкорити, ні знищити бунтівний народ, який протягом всієї історії свого існування прагнув до власної державності.

Література

1. Правда і міфи про наступницю Київської Русі URL: https://armyinform.com.ua/2020/09/14/pravda-i-mify-pro-nastupnyczyu-kyyivskoyi-rusi/ (дата звернення 5.03.2023).
2. Шість російських історичних міфів про Україну Миколи Рябчука. URL: https://localhistory.org.ua/texts/kolonki/ukrayina-v-rosiiskii-istorichnii-mifologiyi-mikola-riabchuk/ (дата звернення 5.03.2023).
3. Кирило Галушко. «Історична правда» про те як Росія привласнила історію Русі та Київську митрополоію. URL: https://risu.ua/istorichna-pravda-pro-te-yak-rosiya-privlasnila-istoriyu-kiyivskoyi-rusi-ta-kiyivsku-mitropoliyu_n120600 (дата звернення 7.03.2023).
4. Історія легіону українських січових стрільців. URL: https://uk.wikipedia.org/wiki/ (дата звернення 9.03.2023).
5. Історія Західної Української Народної Республіки. URL: https://uk.wikipedia.org/wiki/ (дата звернення 5.03.2023).
6. Легіон-хроніки УГА 1918-1919. URL: https://www.youtube.com/watch?v=ysGCsSxVl4o (дата звернення 9.03.2023).

Єрьоміна Л.В.
старший викладач КІБД
Національної академії СБ України
Красін В.К.
студент Національної академії СБ України

ОКРЕМІ ПИТАННЯ ЗАХИСТУ ВІД ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ

У зв’язку з останніми подіями використання інформаційних технологій також можна вважати одним із видів збройної боротьби . Саме тому важливим фактором є психологічні операції, які опереджують боротьбу завдяки військово-технічним засобам і переносять протиборство у інформаційній простір. Сьогодні це дуже актуальне питання, тому що Україна стала ціллю Російської Федерації у інформаційній війні. Безпека нашої держави та суспільства залежить від військових, психологічних, інформаційних засобів. Перевагу в інформаційній боротьбі матиме та сторона, котра матиме національну ідею.

Мета інформаційно-психологічного впливу полягає в тому, щоб завдати шкоди інформаційно-технічній складовій країни та її сектору оборони і безпеки. Дезінформувати та деморалізувати керівництво держави, особовий склад військ і населення.

Завданням інформаційно-психологічного впливу є підрив морально-психологічного стану військ, погіршити суспільно-політичну обстановку і деморалізувати народ.

Вплив інформаційної зброї відбувається у межах інформаційно-психологічних операцій. Саме ці операції впливають на психіку особистості, що може спричинити необхідні зміни в поведінці об'єкта. На думку деяких американських спеціалістів, існує декілька форм інформаційно-психологічних операцій: проти населення, військ і командування збройних сил противника.

З початку повномасштабного вторгнення росії найпоширенішими формами інформаційно-психологічного впливу на особовий склад військ та місцеве населення є друкована, радіо- та усна пропаганда, соціальні мережі, Інтернет.

Недавнім прикладом використання інформаційного впливу для тиску на керівництво нашої держави та дестабілізації суспільно-політичної обстановки стало контрольоване поширення російською стороною в зарубіжних ЗМІ інформації про зосередження біля українського кордону нових потужних угруповань ЗС рф та загрози ескалації ситуації.

Виникає необхідність здійснити захист від інформаційно-психологічного впливу. Спрямований він буде на власну аудиторію, свої війська, особовий склад військ і означатиме запобігання небезпеці противника. Вітчизняний і зарубіжний досвід свідчить, що організувати ефективний захист від негативного інформаційно-психологічного впливу противника неможливо без урахування суспільно-політичних, соціально-психологічних, нормативно-правових, науково-прагматичних, організаційно-управлінських і матеріально-технічних умов.

Захист від негативного інформаційно-психологічного впливу виконує такі функції як: викриття політичної та ідеологічної спрямованості інформаційно-психологічного впливу противника, виявлення намірів, мети і завдань противника та їх роз'яснення об'єктам впливу, розвінчання способів і прийомів, які застосовує противник під час негативного інформаційно-психологічного впливу, показ його соціально-психологічних механізмів, пояснення ефекту, який очікує отримати противник внаслідок свого інформаційно-психологічного впливу, форм, методів і засобів, за допомогою яких поширює інформацію, та способів протидії, об'єднання певних соціальних груп, військових колективів перед загрозою інформаційної, а можливо і військової агресії, виховання у особового складу єдності, здатності протистояти негативному інформаційно-психологічному впливу противника.

Відповідно до функцій, основними завданнями захисту від негативного інформаційно-психологічного впливу противника є:

- виявлення негативних чинників воєнно-політичної, суспільно-політичної та бойової обстановки;
- визначення мети, завдань, форм, методів і спрямованості інформаційно-психологічного впливу противника, роз'яснення їх особовому складу;
- упорядкування використання теле- і радіоприймачів особовим складом;
- ретельний відбір осіб для роботи на засобах зв'язку та з бойовими документами;
- створення груп з особового складу підрозділів для збору та знищення інформаційно-пропагандистських матеріалів;
- налагодження співпраці з органами державної влади та місцевого самоврядування для організації захисту від негативного інформаційно-психологічного впливу противника;
- аналіз адекватності сприйняття особовим складом негативного інформаційно-психологічного впливу, виявлення осіб, які зазнали негативного інформаційно-психологічного впливу противника, організація роботи з ними;
- аналіз та оцінювання ефективності захисту від негативного інформаційно-психологічного впливу противника.

Отже, ефективність захисту від негативного інформаційно-психологічного впливу противника залежить від скоординованої, своєчасно спланованої та організованої діяльності командування, штабу, начальників родів військ і служб у взаємодії з відповідними органами інших структур сектору безпеки і оборони та правоохоронних органів, органами державної влади та місцевої влади.

Література

1. Білошицький В.І., Гангал А.В., Стукан С.О., Бех С.М. Морально-психологічне забезпечення у Збройних Силах України: навчально-методичний посібник. 2-ге видання, доповнене і перероблене. Київ: НТУУ "КПІ імені Ігоря Сікорського", 2020. 138 с.

2. Осьодло В.І., Будагьянц Л.М. Соціально-філософські та психологічні аспекти сучасних війн: монографія. К.: Видавнийчий дім "АртЕк", 2018. 408

Єрьоміна Л.В.
старший викладач кафедри ІБД
Національної академії СБ України

ДО ПИТАННЯ ОКРЕМИХ ІНФОРМАЦІЙНИХ ЗАГРОЗ У ВОЄННІЙ СФЕРІ

Умови життя в яких опинилась наша держава змушують нас розглядати питання безпеки під іншим кутом зору. Якщо ще рік тому світ навколо нас, як нам здавалось, був безпечним, то сьогоднішні загрози несуть небезпеку значно більшу

ніж в умовах мирного часу.

Сутність інформаційних загроз полягає у намірах, діях або явищах, які шляхом інформаційного впливу на соціальні об'єкти, інформаційну інфраструктуру та інформаційні ресурси можуть ускладнити (унеможливити) реалізацію національних інтересів держави (функцій її державних органів). Сьогодні загрози інформаційній безпеці держави слід розглядати як сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства і держави в інформаційній сфері.

Загрози національній безпеці України та відповідні пріоритети державної політики у сферах національної безпеки і оборони визначаються у Стратегії національної безпеки України, Стратегії воєнної безпеки України, Стратегії кібербезпеки України, інших документах з питань національної безпеки і оборони, які схвалюються Радою національної безпеки і оборони України і затверджуються указами Президента України [1].

У зазначених нормативно-правових актах теж розкрито сфери життєдіяльності суспільства і держави, які вразливі до інформаційних загроз, зокрема: зовнішньополітична, державної безпеки, воєнна, внутрішньополітична, економічна, соціальна та гуманітарна, науково-технологічна, екологічна.

Зазвичай, найбільш небезпечними ризиками для будь-якої держави є ті, які впливають на воєнну сферу. Виходячи із Стратегії воєнної безпеки України, ключовими ризиками інформаційній безпеці держави у воєнній сфері слід вважати:

• ухвалення стратегічно помилкових рішень у воєнній сфері, сфері оборони і військового будівництва на підставі неякісного аналізу реальних і потенційних воєнних загроз національній безпеці;

• недостатні інвестиції в розвиток сил оборони, неефективний розподіл видатків на оборону України та витрачання державних ресурсів на утримання безперспективного озброєння, військової та спеціальної техніки;

• неспроможність забезпечити відсіч і стримування збройної агресії проти України з боку Російської Федерації традиційними формами і способами збройної боротьби, зважаючи на незрівнянну різницю у воєнних потенціалах [2].

Отже, з метою попередження і протидії існуючим та ймовірним загрозам інформаційній безпеці стратегічне завдання держави полягає у створенні та функціонуванні механізму забезпечення інформаційної безпеки. Він передбачає послідовну системну діяльність, сукупність заходів і державно-правових інституцій, що покликані гарантувати безперешкодну реалізацію національних інтересів держави в інформаційній сфері, відповідних інтересів людини і суспільства, попередження інформаційних конфліктів та оперативне їх подолання, особливо в умовах дії правового режиму воєнного стану в Україні.

Література
1. Про національну безпеку України : Закон України від 21.06.2018 № 31-ВР. Київ : Парламентське вид-во, 2018. 241 с.
2. Стратегія воєнної безпеки України: введена у дію Указом Президента від 25.03.2021 р. № 121/2021 https://zakon.rada.gov.ua/laws/show/121/2021#n15

Єфіменко І.В.

АКТУАЛЬНІ ПИТАННЯ ЩОДО ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ В ІНФОРМАЦІЙНІЙ СФЕРІ В УМОВАХ КІБЕРВІЙНИ

Питання національної безпеки в інформаційній сфері в умовах кібер війни під час повномасштабної російської агресії є таким самим гострим і надважливим, як питання захисту територій і життя громадян України. І про Закон України «Про національну безпеку» зазначаючи, що державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки та кібербезпеки України.

Про це свідчить також кількість, якість та наслідки атак, що були здійснені в кібер просторі проти України до і після 24.02.2024 року.

Важливо розуміти, що інформаційний простір є найглобальнішою сферою національної безпеки і оборони України, частиною якої є кібер простір, а кібер війна є однією зі складових інформаційної війни.

Під час повномасштабного вторгнення рф Україна зіштовхнулась з усіма можливими кібер атаками збоку ворога. Прояви кібер війни фізичні – знищення технічного ресурсу, семантичні – знищення і підміна інформації, синтаксичні – знищення програмного забезпечення, завдали значної шкоди державі. І ми спостерігаємо, що так чи інакше інформаційна сфера в кібер війні є одночасно і об’єктом, і полем бою, і зброєю.

І якщо злами телебачення, соціальних мереж, радіо тощо, з використанням ІПСО мають на меті дестабілізацію і деморалізацію суспільства, то викрадення інформації про громадян з джерел державних установ, несуть не лише інформаційну, а і фізичну загрозу особистості.

Враховуючи значення інформаційного простору, необхідне глибоке вивчення і аналіз всіх кібер атак, що відбулись під час повномасштабного вторгнення рф. Задля встановлення причинно-наслідкового зв'язку між агресію рф в віртуальному світі і фізичному просторі, з метою подальшого супроводження матеріалів злочинів рф в міжнародному правовому полі. Задля вивчення вразливостей інформаційної сфери і формування надійного захисту в рамках питання загальної національної безпеки як під час повномасштабної агресії так і в мирні часи.

Заболотний С.В.
Національний університет оборони України імені Івана Черняховського

ФУНКЦІОНАЛЬНА СТІЙКІСТЬ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ У ВОЄННІЙ СФЕРІ

Аналіз системи забезпечення інформаційної безпеки держави у воєнній сфері показав, що рівень її функціональної стійкості залежить від багатьох чинників та умов. Основними із них є ті, що відображають внутрішній взаємозв'язок функціональної стійкості із кінцевим результатом стратегії її забезпечення. Такими стратегіями можуть бути шляхи перерозподілу існуючих інформаційних ресурсів в умовах кризових або позаштатних ситуацій, які кожного дня мають місце в інформаційному просторі України [1].

В таких умовах забезпечення інформаційної безпеки держави у воєнній сфері шляхом визначення вимог до її функціональної стійкості дозволить досягнути такого стану за яким кожен суб'єкт національної безпеки буде реагувати на конкретну небезпеку в сфері своєї відповідальності.

Особливу увагу в цій ситуації звернемо на те, що на етапі оцінювання інформаційного простору не повинні вводитися додаткові вимоги, оскільки це створить новий елемент не сформованих небезпек та сформує базу позаштатних ситуацій в яких здійснюється перерозподілом уже існуючих ресурсів. Завдання полягає у виявленні вже існуючих небезпек і формуванні масиву показників за якими у потрібний момент часу можна визначити стан забезпечення інформаційної безпеки держави у воєнній сфері. В цьому і є принципова відмінність задачі забезпечення інформаційної безпеки держави у воєнній сфері через її функціональну стійкості на відміну від задачі побудови нових елементів у системах моніторингу інформаційного простору [2].

Тому функціональну стійкість системи забезпечення інформаційної безпеки держави у воєнній будемо розглядати, як модель представлення знань та правила з погляду людини як засобу прямого опису способу логічного виведення для рішення завдань у предметній області. При цьому відмінною рисою представлення знань з високою модульністю є простота доповнення, модифікації й анулювання. Крім того, з боку існуючих та прогнозованих небезпек є можливість визначення простого й точного механізму використання знань із високою однорідністю, описаних по одному синтаксису. Ці дві відмінні риси є причинами настільки широкого поширення методу представлення знань правилами. В наведеному підході пропонується розглянути базові структури системи забезпечення інформаційної безпеки держави у воєнній сфері та різні аспекти, що стосуються практичної реалізації встановлення її функціональної стійкості.

Функціональна стійкість системи забезпечення інформаційної безпеки держави у воєнній є система яка складається із трьох основних компонентів.

Перший з них – це набір правил, використовуваний як база знань, тому його ще називають базою правил. Наступним компонентом є робоча пам'ять (або пам'ять для короткочасного зберігання), у якій зберігаються передумови, що стосуються конкретних завдань предметної області, і результати висновків, отриманих на їхній підставі, і, нарешті, треба механізм логічного виведення, що використовує правила відповідно до вмісту робочої пам'яті. Як правило, використовують дві групи подібних правил. На практиці для побудови діючих; систем необхідні різноманітні додаткові засоби. У деяких випадках недостатньо запису, а робочу пам'ять лише одного зразка й виникає необхідність керування даними, що уточнюють зміст. У таких випадках досить часто використовується спосіб представлення конкретних даних, як в інформаційному так, і кіберпросторі за допомогою алгоритму:

опис об’єкту;

опис відмінностей в системах, які порівнюють небезпеки в інформаційному просторі;

опис баз знань, які класифікують можливі варіанти рішень.

При цьому способі представлення конкретних даних про небезпеки в інформаційному просторі, окремо заздалегідь формуються спрогнозовані рішення із існуючих елементів системи забезпечення інформаційної безпеки держави у воєнній сфері. Одним з переваг, пов'язаних із впровадженням способу представлення конкретних даних, є уточнення змісту небезпек для кожного суб’єкта національної безпеки України.

Головним моментом в системі забезпечення інформаційної безпеки держави у воєнній сфері є дослідження (перевірка) наявності спеціальних даних, що стосується умовної частини правила функціональної стійкості. Оцінка функціональної стійкість системи забезпечення інформаційної безпеки держави у воєнній методом пошуку й зіставлення має у відомому змісті широку область практичного застосування, однак в окремих випадках така пряма оцінка виявляється недостатньою.

На основні зазначеного маємо ряд фактичних припущень, зокрема щодо формування передумов до формування функціональної стійкості систем забезпечення інформаційної безпеки держави у воєнній сфері.

Перша – заздалегідь визначені небезпеки формують не повноту у даних, тому за такого висновку (зокрема зворотного) велике значення має функція запиту на актуальність інформації. Ця функція особливо необхідна в системах, що вирішують різні проблеми за допомогою діалогу людини з машиною, наприклад у системі консультацій.

Друга – при використанні наведеного підходу відповідно до умов розширюються можливості, щодо оперативної зміни способів представлення конкретних даних в інформаційному просторі.

Тому розглянутий підхід щодо опису функціональної стійкості систем

забезпечення інформаційної безпеки держави у воєнній можна вважати не класичними. Подібні підходи являють собою відношення висновку, установлене між змістом всіх можливих небезпек виявлених в інформаційному просторі та поділом кожної з них на складові для конкретизації прогнозованих рішень.

В існуючій системі забезпечення інформаційної безпеки держави у воєнній майже завжди буває ситуація коли відсутня чітка інформація або дані. У такому випадку звичайно розглядаються дві категорії нечіткостей: нечіткість безпосередніх даних і нечіткість висновку; при цьому, коли висновок виводиться за допомогою декількох правил, що включають і нечіткі, виникає проблема визначення ступеня нечіткості всього висновку.

Отже, функціональна стійкість системи забезпечення інформаційної безпеки держави у воєнній має логічний процес із заздалегідь визначеними способами представлення конкретних даних, як в інформаційному так, і кіберпросторі. Інакше кажучи, наведені припущення, використовувані для доказу останнього висновку, і всі вихідні дані, дотичні їх, можна представити за допомогою конкретних часткових графів. Використовуючи частковий граф, можна описати процес висновку стану функціональної стійкості системи забезпечення інформаційної безпеки держави у воєнній. При цьому можна вказати правила, застосовувані для одержання спеціального висновку (наприклад, останнього або проміжного висновку), і дані, на підставі яких застосовуються ці правила, а також указати, невиконання якої умови спричиняє неуспішне застосування правила.

Література

1. Пелещишин А. М. Процеси управління інтерактивними соціальними комунікаціями в умовах розвитку інформаційного суспільства : монографія / Ю.О. Сєров, О.Л. Березко, О.П. Пелещишин, О.Ю. Тимовчак-Максимець, О.В. Марковець; за заг. ред. А.М. Пелещишина. – Львів : Видавництво Львівської політехніки, 2012. – 368 с.

2. Козоріз К.І. Соціально-психологічне забезпечення оптимізації формування готовності військовослужбовців до виконання завдань вартової служби // Вісник Київського національного університету ім. Тараса Шевченка. Військово-спеціальні науки. – 2005. – №9. – С. 86-89.

Завада А.А.
к.т.н, с.н.с.,
Житомирський військовий інститут імені С. П. Корольова
Беспалко І.А.
к.т.н.
Житомирський військовий інститут імені С. П. Корольова

МЕТОДИКА МОНІТОРИНГУ ТА ВІЗУАЛІЗАЦІЇ ДИНАМІКИ ПОШИРЕННЯ ІНФОРМАЦІЙНИХ ПОВІДОМЛЕНЬ ЗА ДАНИМИ МЕРЕЖІ ІНТЕРНЕТ

Інформаційний фон, що утворюється у суспільстві під час бойових дій чи воєнного конфлікту, позначається на:

ставленні населення до політики свого уряду;

довіри до органів управління та до дій силовиків;

до комплектування армії;

функціонування воєнної економіки та інших сфер, що впливають на хід війни.

Виявлення та оцінювання рівня загроз (РЗ) інформаційній безпеці держави у воєнній сфері від деструктивних психологічних впливів, що здійснюються противником з використанням можливостей мережі Інтернет, залишається надзвичайно актуальним завданням.

Однією зі складових цього завдання є аналіз поширення інформаційних повідомлень (контенту), що містять деструктивний вплив за даними мережі Інтернет для оцінювання створюваного ними РЗ (ефективності з точки зору противника). Крім того, супроводження проукраїнського контенту (для оцінювання його ефективності), який створюється та розповсюджується в мережі Інтернет у рамках організації інформаційної протидії обумовлює виникнення й іншого актуального завдання щодо лінгвістичного аналізу зазначеного контенту для визначення його теми, основної мети та цільової аудиторії, на яку насамперед він спрямований.

Одним з проявів реакції на контент цільової аудиторії є його поширення та різні варіанти реагування, наприклад, “лайки”, “дизлайки”, “репости”, “перегляди”, “коментарі” та ін., які можна віднести до первинних показників динаміки поширення інформаційних повідомлень.

У роботі запропоновано систему показників для аналізу динаміки поширення інформаційних повідомлень у мережі Інтернет, що базується на зазначених вище первинних показниках та показниках рядів динаміки їх зміни.

Подано розроблений загальний алгоритм функціонування автоматизованої системи відслідковування та візуалізації динаміки поширення інформаційних повідомлень за даними мережі Інтернет, що складається з чотирьох часткових алгоритмів:

взяття інформаційного повідомлення на супроводження,

оновлення первинних показників динаміки поширення повідомлення,

визначення показників рядів динаміки

візуалізації отриманих результатів.

Також наведено результати перевірки адекватності функціонування розроблених алгоритмів на основі реальних даних з мережі Інтернет.

Запропоновані підходи лягли в основу розробленого спеціалізованого програмного забезпечення (СПЗ), застосування якого дозволяє автоматизувати роботу оператора щодо:

супроводження визначених інформаційних повідомлень, розміщених на відкритих ресурсах мережі Інтернет;

аналізу показників динаміки їх поширення, поєднаних у систему.

За результатами роботи у СПЗ передбачено можливість оператору:

автоматичне формування звітного документ у форматі “doc”;

попереднє формування змісту зазначеного звітного документа з використанням підсистеми візуалізації;

задавати та редагувати різні рубрикатори інформаційних повідомлень, за якими оператор визначає напрями реалізації інформаційних загроз органам військового управління через відкриті джерела інформації мережі Інтернет, або напрями реалізації протидії цим загрозам.

Таким чином, оператор має можливість кращого налаштування СПЗ під свої потреби, при цьому одні й ті ж самі інформаційні повідомлення можуть бути класифіковані різними операторами з використанням різних рубрикаторів, враховуючи їх потреби.

Перспективним напрямом подальших досліджень є:

підвищення рівня автоматизації аналізу контенту, зокрема, текстової інформації шляхом розроблення й впровадження в роботу СПЗ методів автоматичного семантичного аналізу текстів та визначення їх змісту;

розроблення та впровадження надійних методів і алгоритмів автоматичного реферування текстових документів;

використання автоматичного перекладу з іноземної мови для моніторингу іншомовних ресурсів у мережі Інтернет.

Заїка Н.В.
фахівець відділу технічного захисту інформації,
Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації
Чумаченко С.М.
д.т.н., с.н.с.,
лауреат Державної премії в галузі науки і техніки,
Голова громадської організації «Асоціація фахівців цивільного захисту»,
професор кафедри інформаційних технологій,
штучного інтелекту і кібербезпеки,
Національний університет харчових технологій,
Попель В.А.
начальник відділу науково-технічної експертизи, Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації,

ОЦІНЮВАННЯ РІВНЯ БЕЗПЕКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ НА ОСНОВІ КОМПЛЕКСУ ЗАСОБІВ ЗАХИСТУ ЇЇ ОБ'ЄКТІВ ВІД БПЛА

Анотація. В роботі проведено аналіз відомих підходів до оцінювання рівнів безпеки і обробки ризиків, пов'язаних із застосуванням терористами та ворогом безпілотних літальних апаратів для розвідки, пошкодження та віддаленої кібератаки по об'єктам критичної інфраструктури.

До чинників, що призводить до похибок оцінки цих ризиків, є вирішення задачі своєчасного виявлення безпілотних літальних апаратів. Проблеми виявлення та розпізнавання цілей обумовлені їх малими розмірами та масо-габаритними характеристиками, що ускладнює їх виявлення навіть на малих відстанях. Це стосується як радіолокаційних засобів розвідки, так і оптико-електронних. Крім того, сам процес виявлення цілей залежить від ступеню його автоматизації. Процес ураження цілей залежить від точності наданих координат БПЛА засобам ураження, точності прицілювання цих засобів та їх тактико-технічних характеристик.

Пропонується розглянути інформаційну модель оцінки ефективності комплексу засобів захисту об'єктів критичної інфраструктури за критерієм ефективність-вартість, що допоможе приймати обґрунтовані рішення щодо побудови оптимальних схем захисту критичної інфраструктури і боротьби з безпілотними літальними апаратами.

Ключові слова: критична інфраструктура, ефективність, рівень ефективності, безпілотний літальний апарат, радіолокаційна станція, радіоелектронна боротьба, критерій, ваговий коефіцієнт.

Постановка проблеми. Безпілотні літальні апарати (БПЛА), або дрони є досить новими видами озброєнь на полі бою, починаючи з 1980-х років їх активно

використовують збройні сили провідних країн світу і вже з'явилися результати їх ефективного застосування в останніх воєнних конфліктах.

Бурний розвиток БПЛА призвів до появи багатьох їх різновидів - від розвідників до ударних дронів «камікадзе», які відрізняються за розмірами та цільовим навантаженням. Відеокадри, що передають дрони-розвідники, і закладені у їх бортовий комп'ютер алгоритми маневрування та виявлення нових шляхів наближення до цілей, збільшують ризики ураження або проведення результативної атаки по об'єктам критичної інфраструктури (ОКІ). Застосування групи дронів-ретрансляторів – збільшує небезпечну зону віддаленої атаки.

Аналіз останніх досліджень і публікацій. Аналіз публікацій за напрямом протидії БПЛА показує, що наукових статей з даної тематики досить багато. У переважній більшості робіт в цій області переважають надмірно оптимістичні висновки щодо успішності ураження всіх видів БПЛА сучасними засобами ППО та РЕБ [1-3]. Разом з тим, різке та різноманітне вторгнення БПЛА в сучасні бойові дії, їх стрімкий технологічний розвиток виявили проблему ефективної боротьби з ними, особливо з малими БПЛА, яка на даний час залишається надзвичайно складною. Тільки одиниці держав світу мають частково в наявності та розвивають засоби, які спроможні достатньо ефективно протидіяти застосуванню сучасних БПЛА.

Встає питання у об'єктивному порівнянні ефективності технічних рішень захисту критичної інфраструктури і боротьби з сучасними та перспективними БПЛА з обґрунтуванням їх вартості.

Поява нового виду озброєння – БПЛА та їх застосування в останніх воєнних конфліктах виявили суттєві недоліки зенітних комплексів, що стоять на озброєнні в різних країнах. Аналіз характеристик зенітних комплексів протиповітряної оборони провідних країн світу показує, що багато різноманітних заявлених комплексів протиповітряної оборони нібито здатні вражати як БПЛА, так і крилаті ракети «повітря-земля», літаки, вертольоти. Однак, треба усвідомлювати, що боротьба з БПЛА різних класів суттєво відрізняється. Так, дійсно БПЛА великих та середніх розмірів (типу Predator и Reaper від General Atomics) виявляються, супроводжуються та вражаються з досить високою ефективністю, а з БПЛА малих розмірів виникають суттєві проблеми. В [2] відмічається, що для виявлення малорозмірних БПЛА необхідно застосовувати спеціалізовані засоби розвідки, що мають кращі можливості виявлення та супроводження малорозмірних БПЛА, створювати спеціалізовані канали першочергової передачі розвідувальної інформації про дії малорозмірних БПЛА.

Мета статті - дослідження науково-методичного апарату для оцінювання ефективності системи захисту ОКІ від БПЛА та проведення техніко-економічного аналізу запропонованих технічних рішень ведення боротьби з ними за критерієм ефективність-вартість.

Викладення основного матеріалу. Кожна технічна система (комплекс)

захисту ОКІ й боротьби з БПЛА, як складна система, повинна мати у своєму складі ряд технічних складових (підсистем), поєднаних у єдине ціле.

Кожна складна система складається з підсистем, що мають своє цільове призначення. Умовно, у складі складних технічних систем виділяють за призначенням інформаційну, керуючу, виконавчу підсистеми та підсистему забезпечення. Їх спільна робота і повинна забезпечити ефективну роботу всієї системи захисту ОКІ і боротьби з БПЛА.

Зрозуміло, що кожна з наведених підсистем повинна працювати належним чином, з відповідною ефективністю. Їх розробка та виготовлення потребують певного фінансування та визначають кінцеву вартість всієї складної системи. Таким чином, виникає потреба оцінки ефективності складної системи захисту ОКІ і боротьби з БПЛА шляхом оцінки ефективності роботи складових підсистем з оцінкою їх вартісних показників. Вважається, що «ефективністю» є спроможність системи утворювати системний ефект, але така спроможність має кількісну міру. Виходячи з цього, ефективність технічної системи безпеки ОКІ і боротьби з БПЛА (протидії) можна оцінити як результат (або рівень) функціонування всіх чотирьох підсистем, який прагне до максимального значення, за формулою:

$$\mathrm{E}_{\mathrm{TC}}^{\text{захисту}} = \mathrm{E}_j(i) = \ E_1^{B1} \times E_2^{B2} \times E_3^{B3} \times E_4^{B4} \to max, \qquad (1)$$

де E_1^{B1} , E_2^{B2} , E_3^{B3} , E_4^{B4} - відповідно, ефективності інформаційної, керуючої, виконавчої підсистем та підсистеми ресурсного забезпечення;

$B_1, .., B_4$- вагові коефіцієнти критеріїв ефективності інформаційної, керуючої, виконавчої підсистем та підсистеми ресурсного забезпечення,

$$\sum_{j=1}^{4} B_j = 1.$$

Вагові коефіцієнти B_j цільових (часткових) критеріїв ефективності наведених підсистем зазвичай визначаються методом експертних оцінок (і тільки при неможливості проведення експертного опитування, ваги усіх часткових критеріїв приймаються рівновагими $B_j = 1/4$).

За результатами оцінки ефективності способів протидії БПЛА доцільним є подальше порівняння способів за критерієм «ефективність - вартість». Оцінка використання декількох способів протидії зводиться до формування єдиного критерію шляхом згортки цільових критеріїв кожної з підсистем.

Авторами запропонована шкала оцінки ефективності системи безпеки ОКІ і боротьби з БПЛА, що наведена у таблиці 1.

Таблиця 1. Шкала оцінки ефективності системи боротьби з БПЛА і КР

Рівень ефективності	**Значення показника**

Дуже ефективна	$E_{ТС}^{захисту} \geq 0,8$
Ефективна	$0,8 > E_{ТС}^{захисту} \geq 0,6$
Недостатньо ефективна	$0,6 > E_{ТС}^{захисту} \geq 0,4$
Неефективна	$0,4 > E_{ТС}^{захисту} \geq 0,2$
Дуже неефективна	$E_{ТС}^{захисту} < 0,2$

Висновки. Засоби боротьби та протидії з БПЛА доцільно розглядати з системних позицій. Кожна з чотирьох підсистем, що входять до складу технічної системи безпеки ОКІ і боротьби з БПЛА , вносить свій внесок у ефективність цієї системи, що у свою чергу допомагає виявляти найбільш ефективні способи боротьби та протидії в різних умовах обстановки.

Література

1. Cang Liang, Ning Cao, Xiaokai Lu, Youjie Ye. UAV Detection Using Continuous Wave Radar // 2018 IEEE International Conference on Information Communication and Signal Processing (ICICSP), 28-30 Sept. 2018, Singapore. DOI:10.1109/ICICSP.2018.8549736

2. Sineglazov V.M. Complex structure of UAVs detection and identification // Electronics and Control Systems, 2015, no. 3 (45), C. 28 - 32.

3. Igor Korobiichuk, Yuriy Danik, Oleksyj Samchyshyn The estimation algorithm of operative capabilities of complex countermeasures to resist UAVs // Simulation: Transactions of the Society for Modeling and Simulation Innternational, 7 August 2018, vol. 95, pp. 569 – 573. DOI: 10.1177/0037549718791264.

Зайцев М.П.
Національний університет оборони України імені Івана Черняховського

АНАЛІЗ ШЛЯХІВ ЗБІЛЬШЕННЯ ЕФЕКТИВНОСТІ ЗАХОДІВ ІНФОРМАЦІЙНОЇ ОПЕРАЦІЇ В КРАЇНАХ-ЧЛЕНАХ НАТО

Особливістю сучасної інформаційної операції є те, що поряд з телебаченням на перші позиції висунувся Інтернет. Стара газетна пропаганда повністю відійшла під напором телебачення та Інтернету. Інтернет дає можливість не просто швидкого реагування, а саме реагування в тій точці, яка потребує корекції. Відбувається троллізація інформації, важливе місце займає не сам факт, а його інтерпретація та здійснення впливу на інформаційні потоки.

В сучасному світі інформаційної операції стрімко ускладнюється (розповсюдження широкополосного Інтернету, соціальних мереж, втрати звички до телебачення, старінню базової аудиторії), за прогнозами експертів через 2-3

роки мобілізаційний потенціал телебачення різко скоротиться. І в такому хаотизованому середовищі в рази збільшиться роль одиночних, самостійних ресурсів. Нові технології відкривають дорогу для принципіальної нової генерації інформаційних бійців – людей здібних вести аудіовізуальну пропаганду [1].

На даний час спостерігається вся більша залежність населення та громадської думки від організованих інформаційних операцій, що надходять через Інтернет, а простота доступу, вільне розповсюдження та отримання інформації робить Інтернет ефективним засобом інформаційно-психологічного впливу. Основні державні та недержавні організації зайнялися інформаційним простором нового типу – соцмережами, які формуються самими учасниками та до яких рівень довіри та уваги більше чим до традиційних ЗМІ [2].

Інтернет все активніше і масштабніше використовується в інтересах інформаційного протиборства сторін, які є учасниками різних конфліктів. Він надає широкі можливості в плані надання впливу на формування громадської думки, прийняття політичних, економічних і військових рішень, впливу на інформаційні ресурси противника і поширення спеціально підготовленої інформації (дезінформації) [3].

Активне використання мережі Інтернет для ведення інформаційних операцій обумовлено наявністю низки істотних переваг перед звичайними засобами і технологіями.

Оперативність. Розміщення і регулярне оновлення інформації на окремих сторінках, в інтернет-виданнях і різного роду новинних розсилках, форумах і конференціях не вимагає значного часу на підготовку матеріалів в електронному вигляді. При цьому користувачі отримують її в режимі реального часу (на відміну, наприклад, від читачів періодичних видань). Крім того, цілеспрямований вплив на інформаційні ресурси противника може здійснюватися не тільки в заздалегідь запланований час, але і в міру виникнення необхідності.

Економічність. Є наслідком залучення невеликої кількості персоналу і матеріальних засобів для вирішення поставлених завдань. Так, наявність мінімально підготовленого користувача персональної ЕОМ, підключеної до телефонної лінії, нерідко буває цілком достатньо. Крім того, застосування комп'ютерних технологій для виведення з ладу систем управління противника в певних умовах може призвести до більш значного ефекту при істотно менших витратах в порівнянні з використанням традиційних засобів (вогневого ураження, радіоелектронної боротьби).

Скритність джерела впливу. Як правило, акт агресії в глобальній мережі важко відрізнити від дії звичайних комп'ютерних хуліганів. Підготувати та провести кібератаку з використанням Інтернету може досить широке коло осіб – від військових і розвідувальних структур іноземних держав до партизанських формувань, злочинців, промислових конкурентів, хакерів або просто озлоблених людей. Відстежити ж джерело досить складно.

Дистанційний характер впливу на комп'ютерні системи в різних регіонах світу. В оглядах порушень мережевої безпеки регулярно повідомляється про виявлені наслідки ефективних дистанційних впливів на комп'ютерні мережі різних країн.

Масштабність можливих наслідків. Крім впливу на формування громадської думки, на позиції офіційних осіб, які приймають найважливіші рішення, використання глобальної мережі для деструктивних впливів може призвести до порушення нормальної роботи або тривалого виведення з ладу життєво важливих об'єктів і систем в окремих районах, країнах або регіонах.

Комплексність подачі інформації та її сприйняття. На Інтернет-сторінках розміщується як текстова, так і графічна інформація в найбільш зручному для сприйняття вигляді, а її обсяг може бути в багато разів більше, ніж у будь-якого друкованого видання, радіопередачі або телевізійної програми. Використання ж сучасних мультимедійних технологій, що дозволяють демонструвати документальні свідчення, фото- та відеоматеріали при спеціально підібраному супроводі (коментарі, музика), надає на користувачів додаткове емоційний вплив [4].

Доступність інформації. За наявними даними, загальна кількість користувачів Інтернету перевищила 2 млрд осіб. У лічені миті вони отримують доступ до інформації, наявної на серверах різних країн, минаючи прикордонні, цензурні й інші бар'єри. При цьому будь-який користувач може розмістити власну інформацію (нерідко безкоштовно) на серверах, зареєстрованих в інших державах, або організувати розсилки повідомлень по всьому світу.

На даний час існують наступні напрямки використання мережі Інтернет для здійснення ІПВ, а саме:

поширення спеціально підібраною інформації (дезінформації);

розміщення інформації на окремих сторінках або в електронних версіях періодичних видань та мережного мовлення (трансляції передач радіо- і телестанцій).

пропаганда своїх позицій;

заміна інформаційного змісту сайтів, яка полягає в підміні сторінок або їх окремих елементів в результаті злому;

семантичні атаки, які полягають у зломі сторінок і наступному акуратному (без помітних слідів злому) розміщенні на них завідомо неправдивої інформації;

психологічне кодування користувачів Інтернету.

Враховуючи перелічені вище фактори, постійно зростаючу роль Інтернету в суспільстві та наявність підключення до мережі Інтернет у переважній більшості населених пунктах ОРДЛО слід вважати, що збільшення ефективності ведення ІПВ на СІС противника можливо досягти через мережу Інтернет.

Таким чином, на даний час існують різноманітні варіанти ведення інформаційної операції. Поряд з класичними, як листівки, аудіопропаганда, теле-,

радіопропаганда, пропаганда через друковані ЗМІ, з'явився і новий спосіб – ведення ІПВ через мережу Інтернет. Форми і способи ведення ІПВ на противника постійно змінюються та вдосконалюються, як методологічно, так і технічно, збільшується їх ефективність.

Література

1. NATO Standard AJP-3.10 ALLIED JOINT DOCTRINE FOR INFORMATION OPERATIONS. Edition A Version 1. DECEMBER 2015.

2. NATO Standard AJP-3.10.1 ALLIED JOINT DOCTRINE FOR PSYCHOLOGICAL OPERATIONS, 2014.

3. Бурячок В.Л., Толубко В.Б., Хорошко В.О., Толюпа С.В. Інформаційна та кібербезпека: соціотехнічний аспект: Підручник. – К.: ДУТ, 2015. – 288 с.

4. Донбас і Крим: ціна повернення : монографія / за заг. ред. В. П. Горбуліна, О. С. Власюка, Е. М. Лібанової, О. М. Ляшенко. – К. : НІСД, 2015. – 474 с.

Іванов О.Ю.
к.ю.н.,
Національна академія Служби безпеки України

ДО ПРОБЛЕМИ ІСТОРИЧНОЇ ОСВІЧЕНОСТІ ОСОБОВОГО СКЛАДУ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ В УМОВАХ ВІЙНИ

Непрості історичні умови, у яких нині перебуває Україна, вимагають комплексного підходу до формування та реалізації державної політики. Одним із напрямів останньої є безпековий, який наразі пронизує всі сфери суспільства, зокрема з огляду на наявні гібридні загрози. Відповідно, високий рівень підготовки фахівців сектору безпеки і оборони стає вкрай затребуваним. Узгодження набутих ними під час навчання компетентностей із актуальними викликами вітчизняній державній безпеці немислиме не лише без ґрунтовної спеціальної, але й загальної гуманітарної підготовки. Серед іншого, на сьогодні знання історії із розряду загальноосвітньої підготовки переходять до справжніх інструментів, які стають у пригоді при стримуванні російської агресії. Позаяк владна система цієї держави визначається істориками як архаїзована, історичні знання стають нічим іншим, як емпіричним матеріалом для прогнозування її подальших зовнішньополітичних кроків. Разом з тим, активне використання фальсифікацій історичних фактів застосовується російськими політиками та журналістами для пропагандистського впливу на народ України. Зазначене дозволяє стверджувати про прямий вплив історичного складника на якість вищої освіти майбутнього співробітника вітчизняної спецслужби.

Сучасна наука знає таку категорію, як публічна (або практична) історія.

Виникнення цього терміна відносять до наукового дискурсу в США середини 1970-х рр., хоча окремі елементи такого явища були відомі давно. Публічна історія позиціонує процес творення історичної пам'яті як спільну справу професійних істориків і суспільства, постійну комунікацію між ними. Деякою мірою спрощена подача історичних знань має сприяти популяризації їх серед широких кіл населення. Важливими для історика як професіонала стають не лише навички, пов'язані зі збиранням емпіричних даних і їхньою науковою обробкою, а і вміння публічного виступу, комунікативні компетентності, змога ефективно донести необхідні наративи до найширших верств населення з тим, аби сформувати відповідну вимогам поточного моменту історичну пам'ять. Тут не йдеться про тоталітарні підходи, пов'язані з посиленням цензури, а якраз про творення колективних ідеалів як основи потужної демократичної системи. Для посттоталітарних суспільств (зокрема, і для України) такий підхід видається вкрай важливим для консолідації суспільства в умовах очищення історичного минулого від штучних нашарувань попередньої епохи. Зокрема, з огляду на це публічна історія стала предметом обговорень і в аудиторіях на історичних факультетах вітчизняних провідних вищих навчальних закладів.

Технології публічної історії як такої цікаві майбутнім співробітникам вітчизняної спецслужби з огляду на важливість інформаційного протиборства як елемента російсько-української гібридної війни. За допомогою них вони матимуть змогу осмислювати реалії сьогодення із залученням історичних закономірностей і більш ефективно оцінювати розвиток потенційних загроз державній безпеці України та міжнародній безпеці, що походять від російського зовнішньополітичного курсу. У зв'язку з цим слід визнати за доцільне розробку і запровадження на другому (магістерському) рівні вищої освіти для здобувачів вищої освіти вищих навчальних закладів зі специфічними умовами навчання інтегрованої навчальної дисципліни під назвою «Публічна історія». Структурно вона має включати такі навчальні модулі: «Історична політика держави і формування історичної пам'яті», «Діяльність істориків у публічному просторі», «Інститути громадянського суспільства та їх вплив на історичну культуру населення». Окрім вивчення теоретичного матеріалу, для здобувачів вищої освіти слід виробити комплекс практичних завдань, які б передбачали створення ними конкретних розробок (есе, відео, публіцистичні статті, презентації) з інтерпретацією окремих фактів історичного минулого до сучасних суспільно-політичних умов.

Якісне засвоєння курсу публічної історії вимагає також і доволі потужної емпіричної бази. У зв'язку з цим викладання дисциплін історичного профілю на першому (бакалаврському) рівні вищої освіти необхідно узгодити з такими потребами. Зокрема, слід відійти від класичного підходу, за якого навчальна діяльність здобувачів вищої освіти на заняттях із відповідних предметів зведена головним чином до сприйняття інформації від викладача і відтворення її під час

контрольних заходів. Публічна історія передбачає первинність діяльності того, хто «споживає» історичні відомості, як їх безпосереднього «відкривача». Тому основними формами навчальної діяльності мають стати пошук та інтерпретація історичних відомостей відповідно до умов сьогодення, а також надання оцінок наявних публікацій з історичної тематики. Роль викладача в цьому випадку має бути більше координаційною, а не як безпосередньо джерела інформації. Разом з тим, доповнення таких форм роботи проведенням семінарських і практичних занять в ігровій формі (моделювання історичних подій, командні ігри тощо) та активним залученням здобувачів вищої освіти до участі в наукових форумах і конкурсах неодмінно сприятиме розвитку їхніх комунікативних навичок як украй важливих фахових компетентностей. Такий підхід дозволить ефективно використати потенціал історичних дисциплін навіть із залишенням без змін виділеного на їх вивчення навчального часу: результативність самостійної роботи та мотивація до неї зростуть доволі суттєво.

Таким чином, у сучасних умовах слід вести мову не про підготовку фахівців сектору безпеки і оборони засобами історичної науки, а про вкрай важливу роль останньої як передумови забезпечення якості вищої освіти за. Використання потенціалу такого відносно молодого наукового напряму, як публічна історія, сприятиме формуванню ряду важливих фахових компетентностей, зокрема комунікативних. Перегляд сталих підходів до викладання історичних дисциплін у вищих навчальних закладах зі специфічними умовами навчання забезпечить можливість використання знань з історичних дисциплін для безпосередньої оцінки суспільно-політичної ситуації та прогнозування її розвитку.

Іванов Ю.А.
д.ю.н., доцент,
Національна академія СБ України

ДЕЯКІ АСПЕКТИ ПРОАКТИВНОГО ПІДХОДУ У ПРОТИДІЇ РОСІЙСЬКИМ ДЕСТРУКТИВНИМ ІНФОРМАЦІЙНИМ ВПЛИВАМ

Від початку повномасштабного вторгнення військ рф в Україну, попри розгортання бойових дій, технології гібридної російської агресії, зокрема в інформаційній сфері, не лише не відійшли на другий план, а й набули ще більших масштабів, трансформувалися змістовно відповідно до воєнних реалій.

За таких обставин протидія російським деструктивним інформаційним впливам має відбуватися у проактивному форматі, що передбачає як безпосередню нейтралізацію ворожих пропагандистських вкидів, так і протиставлення їм масованої проукраїнської контрпропаганди. При цьому, динаміка процесів, що відбуваються на полі інформаційного протиборства,

вимагає перманентного корегування та вдосконалення цієї роботи.

Так, зокрема, у стратегічному вимірі вкрай важливо постійно нарощувати акценти на неминучості деокупації українських територій й широко висвітлювати тематику їх реінтеграції та поствоєнного відновлення, пропагуючи при цьому відповідні державні програми та громадські ініціативи. Це є необхідним, серед іншого, і в контексті стимулювання майбутнього повернення громадян України, яких обставини війни змусили виїхати за кордон. Із зазначеним повністю корелює офіційно окреслена на державному рівні позиція стосовно того, що Україна прагнутиме не простого відновлення довоєнного стану, а якісного стрибка у своєму розвиткові, орієнтуючись у формально-юридичному сенсі, передусім, на досягнення параметрів, необхідних для набуття повноправного членства в Європейському Союзі. Знаковим практичним кроком у вказаному напрямі стало отримання Україною статусу кандидата на вступ до цієї впливової інтеграційної інституції [1].

Контрпропагандистські зусилля мають базуватися на врахуванні того незаперечного факту, що під прицілом агресивної російської пропаганди перебувають не лише тимчасово контрольовані рф українські території, а й уся Україна, а також у цілому європейський та світовий інформаційний простір. Так, зокрема, пропагандисти рф невпинно торпедують європейську та євроатлантичну єдність у практичних питаннях надання допомоги Україні. При цьому вони активно паразитують на тих чи інших розбіжностях у позиціях держав, передумови для яких, насправді, цілеспрямовано формувалися державою-агресором протягом багатьох років, в тому числі шляхом штучного втягування країн у економічну залежність від рф, повзучої інфільтрації в їх політико-правове середовище проросійських ідеологем й «стимулювання» з цією метою місцевих політиків та політичних сил (такі дії позначають влучним терміном «експорт корупції» [2]). Як наслідок – в Європейському Союзі, до прикладу, наразі не завжди вдається швидко приймати потрібні узгоджені рішення щодо підтримки України [3]. Окремі такі випадки й будь-які щонайменші паростки не проукраїнських проявів у країнах антипутінської коаліції, яка сформувалася після 24.02.2022, російська пропаганда подає у гіпертрофованому спотвореному вигляді, маючи на меті представити це як начебто домінуючу тенденцію чи системне явище. Як один із засобів для цього масово використовують фейкові сторінки чи сторінки-клони у соцмережах, які начебто належать авторитетним особам, в тому числі українським військовим, дублюють телеграм-канали військових частин Збройних Сил України, до яких у суспільстві сформувався надзвичайно високий рівень довіри [4].

На українських територіях, які тимчасово контролюють окупанти, вони вдаються до вже відпрацьованого сценарію, який передбачає максимальну монополізацію інформаційного простору шляхом блокування трансляції українських телевізійних і радіопрограм, захоплення належного зареєстрованим в

Україні операторам мобільного зв'язку обладнання й налаштування його виключно на роботу в російських мережах. Тим самим ворог намагається створити умови для безперешкодної «обробки» населення задля досягнення його лояльності. А за відсутності бажаного результату в хід ідуть репресивно-каральні методи. Водночас, завдяки сучасним технологіям повністю ізолювати населення від непідконтрольних рф джерел інформації ворогу, як правило, не вдається. Тож певні канали комунікації з українцями, котрі перебувають в окупації, залишаються. Цим необхідно неодмінно користуватися, передусім, задля того, щоб виказувати людям підтримку, інформувати про те, що держава робить і буде робити усе можливе для якомога швидшого вигнання окупантів. Паралельно мають надходити й відповідні сигнали колаборантам про те, що відповідальність неминуча, переконливим підтвердженням чому є заходи щодо таких осіб, які активно реалізуються СБ України [5], а також показова доля зрадників, для яких наслідки їхньої колабораційної діяльності настали значно швидше, аніж вони могли очікувати [6].

Проявом наступальних дій держави щодо нейтралізації небезпечного проникнення російських пропагандистських інституцій в український соціум стало виявлення й документування органами СБ України відверто антидержавницьких дій цілої низки представників орієнтованої на московський патріархат УПЦ, котрі, як з'ясувалося, й в умовах повномасштабної війни будували свої звернення до вірян на відверто проросійських наративах, керуючись при цьому продукованими у рф настановними документами [7].

У вимірі втілення на практиці проактивного підходу до протидії деструктивним інформаційним впливам рф на європейський і світовий політикум надзвичайно важливою є дипломатична компонента, адаптована до специфіки воєнного часу. Ідеться, зокрема, про застосування нестандартних підходів для максимально можливого використання в інтересах нашої перемоги різноманітних міжнародних майданчиків, таких як Генеральна Асамблея та Рада Безпеки ООН, зустрічі лідерів країн «G 7», Світовий економічний форум в Давосі та ін. Особливе місце у цій системі заходів посідають украй значущі, хоч в силу обставин і нечисленні, закордонні поїздки Президента України. У цьому аспекті необхідно відзначити, передусім, промову українського лідера, проголошену наприкінці 2022 року у Конгресі США.

Іншою не менш вагомою складовою міжнародного блоку контрпропагандистських зусиль є організація численних приїздів в Україну представників зарубіжних країн та міжнародних інституцій, у ході яких швидко розбиваються вщент об реальність насаджувані офіційною москвою та російськими пропагандистами міфологеми. Ефект від таких візитів в інформаційному протиборстві посилюється ще й тим, що вони відбуваються на тлі зростаючої міжнародної ізоляції рф.

Викладене не вичерпує, звісно, всієї проблематики проактивної протидії

російським деструктивним інформаційним впливам, окреслюючи лише загальну тезу щодо важливості органічного поєднання фахової власної української наступальної інформаційної політики із заходами, направленими проти ворожого пропагандистського контенту, проти осіб, що його продукують, а також проти засобів його поширення.

Література

1. Україна отримала статус кандидата на членство в ЄС / Урядовий портал. 23.06.2022. URL :https://www.kmu.gov.ua/news/ (дата звернення 17.03.2023).

2. Khodorkovsky Mikhail B. A Time and a Place for Russia. The New York Times. Jan. 28, 2010. URL: https://www.nytimes.com/2010/01/29/opinion/29iht-edkhodorkovsky.html. (accessed 17.03.2023).

3. Угорщина заблокувала виділення Україні 500 млн. євро військової допомоги ЄС / Українська правда. 19.01.2023. URL : https://www.pravda.com.ua/news/2023/01/19/7385656/ (дата звернення 17.03.2023).

4. Кремлівська пастка: як пропаганда рф імітує українських військових у соцмережах / Радіо Свобода. 15.03.2023. URL : https:// www.radiosvoboda.org (дата звернення 17.03.2023).

5. До суду передано вже понад 300 справ проти колаборантів – Голова СБУ. / УНІАН. 05.03.2023. URL: https://www.unian.ua (дата звернення 17.03.2023).

6. У тимчасово окупованому Мелітополі підірвано автомобіль колаборанта Івана Ткача. Він помер у лікарні. / UKRINFORM. 15.03.2023. URL:https://www.ukrinform.ua (дата звернення 17.03.2023).

7. «Колаборанти в рясі»? Що чекає на Українську православну церкву (не) Московського патріархату / Українська правда. 12.12.2022. URL : https://www.pravda.com.ua/news/2022/12/12/7380422/ (дата звернення 17.03.2023).

Іванова Н.Г.
д.психол.н., професор
Національна академія СБУ

АКТУАЛЬНІ ПИТАННЯ ПРОТИДІЇ ВОРОЖИМ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИМ ВПЛИВАМ НА УКРАЇНСЬКИХ ВІЙСЬКОВОСЛУЖБОВЦІВ

Використання в сучасному суспільстві інформації як зброї, що набуло особливого звучання з початком повномасштабного вторгнення рф в Україну, показало важливість розбудови дієвої системи протидії негативному впливу на особовий склад збройних формувань структур сектору безпеки і оборони України. Актуальності додає і розроблення й апробація ворогом нових інформаційних

технологій, прийомів, технічних засобів, методів здійснення психологічного впливу, а також спрямована на охоплення великих територій і мас людей у найкоротші терміни технологізація такого інформаційного протиборства. Цілеспрямоване використання в конфлікті «психологічної зброї», насамперед, інформаційно-психологічних впливів з метою формування необхідних поглядів, переконань, ціннісних спрямувань, уявлень, мотивів (підбурювання до певних дій), зниження рівня боєздатності та деморалізації особового складу в кінцевому підсумку орієнноване на нівелювання здатності (когнітивної, емоційної, поведінкової) чинити опір ворогові всупереч наявній ситуації, логіки розвитку подій і власному розуму. Відтак, в умовах збройного протистояння інформаційно-психологічні впливи стають більш агресивними, а спроможність протидіяти таким впливам набуває все більшого значення.

Отже, метою нашої публікації ставимо виокремлення основних елементів системи протидії інформаційно-психологічним впливам як важливої складової інформаційно-психологічної безпеки особистості, підрозділу, інституції й держави.

Під інформаційно-психологічними впливами розуміють реалізацію психологічних технологій в інформаційних ресурсах задля розповсюдження інформації, зорієнтованої на зміну емоцій, почуттів, мотивів та поведінки військовослужбовців. Основними шляхами розповсюдження інформаційно-психологічних впливів є соціальні мережі, безпосередня комунікація, використання рідних/близьких, місцевого населення для поширення певного контенту. Головним об’єктом такого впливу є певні соціальні групи (масова свідомість) або окрема людина (її свідомість). Негативні інформаційно-психологічні впливи противника зорієнтовані на зниження рівня боєздатності підрозділу та деморалізацію особового складу.

В умовах воєнних дій про поширення інформаційно-психологічних впливів свідчать такі маркери: циркуляція дезінформації, активізація ворожої пропаганди, поширення чуток (фейків), зміна психоемоційного стану особового складу. В разі уразливості особового складу та недостатньої дієвості превентивних заходів в підрозділі можуть також проявлятися і окремі з потенційних негативних наслідків:

- паніка в підрозділі,
- прояви агресивної поведінки,
- підбурювання до деструктивної поведінки особового складу,
- наростання незадоволення особового складу,
- саботаж.

Дієва система протидії негативним інформаційно-психологічним впливам (комплексу інформаційних, психологічних та організаційних заходів, зорієнтованих на прогнозування, виявлення, нейтралізацію та профілактику негативних інформаційно-психологічні впливи противника) дозволить мінімізувати можливість настання цих загроз, а відтак підвищить ефективність

виконання поставлених перед підрозділом завдань.

Така система протидії негативним інформаційно-психологічним впливам включає в себе:

- *запобігання негативним інформаційно-психологічним впливам* (в межах якого здійснюється постійна комунікація та своєчасне інформування щодо особливостей впливу інформації на бійця; моніторинг особового складу підрозділу щодо прогнозування ймовірних мішеней інформаційно-психологічних впливів (панікерів, токсичних осіб тощо); психологічна підготовка особового складу з розвитку стійкості до інформаційно-психологічних впливів);
- *виявлення негативних інформаційно-психологічних впливів* (зокрема: встановлення маркерів поширення інформаційно-психологічних впливів; прогнозування їх потенційних наслідків; оцінювання інформації – визначення мети, цільової аудиторії, джерел, каналів поширення; перевірка достовірності інформації);
- *нейтралізація негативних інформаційно-психологічних впливів* (це, передусім: оперативна комунікація з особовим складом; роз'яснення справжніх цілей та наслідків інформаційно-психологічних впливів; роз'яснення ступеня загрози інформаційно-психологічних впливів для життя особового складу та боєздатності підрозділу; мотивування особового складу до перевірки та нерозповсюдження деструктивної інформації).

Цей комплекс дій має на меті не тільки прогнозувати, виявити та нейтралізувати деструктивні інформаційно-психологічні впливи, а й здійснити так звану профілактику (у тому числі завдяки психоедукації), забезпечити збереження високого морально-психологічного духу особового складу, підтримання мотивації особового складу до успішного виконання завдань.

Таким чином, ефективна діяльність особового складу підрозділу в умовах збройного конфлікту залежить, у тому числі, й від спроможності захистити психіку військовослужбовців від деструктивних інформаційно-психологічних впливів ворога. Дієвість такої протидії зумовлюється системним підходом у реалізації комплексу заходів, які:

- з одного боку, нейтралізують цілеспрямований деструктивний зовнішній вплив на особистість (те, що й виступає тригером негативних змін),
- з іншого – формують базис для спроможності «чинити опір», тобто виступають складовими ресурсності підрозділу, що визначають резилієнтність особового складу до дій ворога.

Ця система протидії інформаційно-психологічним впливам базується на закономірностях функціонування людської психіки та комунікативних процесів в соціумі. Вона представлена безперервним процесом моніторингу, аналізу, оцінювання, прогнозування, інформування та комунікації.

Іванченко Є.О.
Служба безпеки України

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ РЕСУРСІВ МЕСЕНДЖЕРІВ ТА СОЦІАЛЬНИХ МЕРЕЖ В ІНТЕРЕСАХ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Характерною особливістю сучасності є та обставина, що до активної участі в інформаційних процесах у дуже стислі строки долучилися широкі маси користувачів, що в переважній більшості не мають відповідного рівня підготовки до участі в суспільно корисній інформаційній діяльності. Для значної частини учасників інформаційних обмінів самовираження в Інтернеті поки що є значущим як процес. І тому сьогодні інформаційний простір перевантажений випадковою, низькоякісною інформацією, що ускладнює використання суспільно значущих ресурсів. Однак останнім часом з розвитком інформаційних технологій, удосконаленням загальносуспільної системи соціальних інформаційних комунікацій в Україні ми спостерігаємо характерний також і для інших країн світу процес самоорганізації вітчизняного інформаційного простору, формування системи соціальних інформаційних мереж [3, с. 34].

Сучасні виклики та загрози зумовлені застосуванням Російською Федерацією технологій гібридної війни та перенесенням театру воєнних дій у площину інформаційного простору, перетворили його на одну з ключових арен протиборства. Аналіз способів ведення останніх збройних конфліктів свідчить, що у військовій справі настав новий етап розвитку, коли ефективність сучасних засобів ураження все більше визначається не стільки вогневою міццю, скільки ступенем інформаційної безпеки. У змісті військових дій все більше зростає значимість інформаційного протиборства і перевага у ступені інформованості стає неодмінною умовою перемоги у війні [2, с. 4].

Розвиток цифрових технологій та цифровізації в цілому обумовлює використання мережі Інтернет майже у всіх сферах. У сучасному світі неможливо уявити спілкування без використання Інтернет-месенджерів. Месенджери стали частиною суспільного життя мільйонів людей і використовуються не лише в якості інструменту для спілкування, а й для маркетингу, бізнесу та навчання. Вони є у кожного користувача смартфона, а для передачі даних використовують цифрові канали зв’язку.

Із розвитком технічних та програмних можливостей доступу до мережі Інтернет виникає питання захисту інформації при її зберіганні та передачі. Важливою складовою захищеності та безпеки інформації є етап передачі інформації цифровими каналами зв’язку, адже саме на цьому етапі існують ризики перехоплення даних. Під час перехоплення пакетів даних, які прямують незахищеними (або частково захищеними) каналами зв’язку, створюються передумови для спотворення чи блокування інформації, а також для перехоплення

персональних, конфіденційних та/або даних з обмеженим доступом [1].

Також необхідно мати на увазі, що під час встановлення тих чи інших додатків на смартфони чи інші засоби телекомунікації та зв'язку, програмні продукти можуть вимагати доступу до певної інформації на використовуваному пристрої, насамперед геолокації, списку контактів, акаунтів у соціальних мережах та поштових скриньок.

За наявними даними, більшість шпигунських програм «вшиваються» саме в мобільні додатки, які цікавлять конкретну аудиторію. Тому необхідно бути уважним під час встановлення додатків, особливо якщо робити це з невідомих та неперевірених сервісів.

У зв'язку з цим, метою унеможливлення завантаження на особистий пристрій програм-шпигунів необхідно дотримуватись таких основних правил:

– встановлювати додатки лише з офіційних та перевірених сервісів (ChromeStore, Addons та PlayMarket для Android, AppStore для OS);

– заборонити операційній системі смартфона (планшета, ПЕОМ) автоматично встановлювати додатки з невідомих джерел шляхом здійснення відповідних налаштувань пристрою;

– періодично здійснювати чистку усіх особистих пристроїв від додатків, які не використовуються та ряд інших заходів.

Необхідно також звернути увагу, що загострення ситуації навколо кордонів Україні з рф, тимчасово окупованої території України АР Крим та ОРДЛО, а також активізація етапів гібридного протистояння (хакерські атаки на державні інформаційні ресурси) чітко окреслює позиції рф як держави, що використовує силовий підхід до вирішення проблем.

Для ефективного забезпечення національної безпеки України, в умовах протистояння агресивній зовнішній політиці, захист інформації, що поширюється цифровими каналами зв'язку, та ідентифікаційних (персональних) даних користувачів є одним з пріоритетних завдань.

За офіційними даними, в Україні до початку бойових дій проживало близько 44,13 млн громадян. З них близько 246 тис. – військовослужбовці ЗС України (станом на початок 2022 року). Майже у кожного з них є хоча б один Інтернет-месенджер та сторінка у соціальній мережі, що використовується для спілкування у робочих цілях. У ході такого спілкування відкритими цифровими каналами зв'язку поширюються наступні дані: персональні ідентифікаційні дані; інформація щодо проходження військової служби (підрозділ, звання, завдання, поточні задачі, дані про дислокацію та ротацію тощо); дані для службового користування або ж дані з обмеженим доступом.

Найпопулярнішим месенджером в Україні у 2021 році був Viber, яким користувалися 99% власників смартфонів у віці від 13 до 55 років, далі йшов Facebook Messenger і Telegram, у той час, як WhatsApp та Skype поступово втрачають користувачів. Останнім часом набуває популярності Threema, особливо

серед військовослужбовців ЗСУ та правоохоронних структур України [1].

Як бачимо, інформація у сучасному світі являє собою стратегічний ресурс. Її спотворення, перехоплення або блокування може призвести до серйозних наслідків, а в умовах стрімких світових змін набувають актуальності існуючі та формуються нові загрози національній безпеці України.

Враховуючи викладене вище, слід констатувати, що розвиток електронних технологій дозволяє мільйонам людей вільно користуватись мережею, що дає змогу використовувати їх творчий потенціал для вирішення інтелектуальних, наукових, суспільно значимих питань.

Отже, використання інформаційних ресурсів месенджерів та соціальних мереж в інтересах національної безпеки залишатиметься актуальною на подальшу перспективу. Проблеми захисту інформації в інформаційній сфері досі остаточно не розв'язане і може вирішуватись в результаті комплексного підходу до даної проблематики, що включає в себе спільну роботу розробників мережі, користувачів і держави.

Література

1. Використання месенджерів як елементів цифрової розвідки: проблематика та шляхи вирішення. URL: https://intelmag.com/digitalization/17454-vykorystannya-mesendzheriv-yak-elementiv-czyfrovoyi-rozvidky-problematyka-ta-shlyahy-vyrishennya/ (Дата звернення: 05.02.2023).

2. Методичні рекомендації з використання соціальних мереж у Збройних Силах України. URL: https://ela.kpi.ua/bitstream/123456789/18028/1/30_p14.pdf (Дата звернення: 02.02.2023).

3. Соціальні мережі як чинник розвитку громадянського суспільства: монографія / О. С. Онищенко, В. М. Горовий, В. І. Попик та ін.; НАН України, Нац. б-ка України ім. В. І. Вернадського. Київ, 2013. 220 с.

Іжко О.В.
Національний університет оборони України імені Івана Черняховського

ПІДХОДИ ЩОДО ОЦІНЮВАННЯ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ ПРОТИВНИКА

Аналіз "Теорії осмисленої дії" показав, що її основа складає процеси оцінювання поведінки соціальної групи та описує взаємозв'язки між змістом психологічного впливу і можливою поведінкою цільової аудиторії у визначеній соціальній групі. Особливе місце в оцінюванні цільової аудиторії займають поведінкові її наміри. Самі наміри формуються не тільки установками, але й впливом певних суспільних норм, яких дотримується цільова аудиторія [1].

Відповідно до основних положень Стратегії інформаційної безпеки України одним з основних шляхів її реалізації є “розробка методологічних підходів оцінювання інформаційно-психологічного впливу”. Це впливає на розвиток Сил оборони України та вимагає запровадження універсальних механізмів планування для всієї системи забезпечення інформаційної безпеки. В першу чергу процедур виявлення негативного інформаційного-психологічного впливу, що дозволять синхронізувати інформаційну протидію всіх складових Сектору безпеки та оборони України. Цільові аудиторії у своїй більшості мислять раціонально та використовують доступну їм інформацію, щоб передбачити наслідки своїх дій, перш ніж вони вирішать щось зробити. Після аналізу всіх попередніх досліджень [2] виникла необхідність обґрунтувати модель, яка могла до певної міри передбачати та пояснювати поведінку і соціальну установку цільової аудиторії.

Структурно особливості інформаційно-психологічного впливу з боку противника на особовий склад Збройних Сил України можна описати наступники етапами:

у пункті постійної дислокації військової частини (з’єднання) з використанням таких засобів впливу, як телебачення, радіо, Інтернет, мобільний зв’язок, газети, журнали, листування, поширення чуток, вербальне і невербальне спілкування, вплив з боку родини та близького оточення, наочні форми впливу;

під час здійснення маршу до району виконання завдань використовуються такі засоби, як радіо, мобільний зв’язок, невербальне спілкування, наочні форми впливу;

у районі виконання бойових завдань використовуються всі ті засоби впливу, що і в пункті постійної дислокації військової частини (з’єднання), і додатково здійснюється шантаж військовослужбовців через погрози родинам;

під час виконання бойових завдань інформаційно-психологічний вплив з боку противники на особовий склад Збройних Сил України здійснюється за допомогою використання гучномовних засобів впливу, вербального і невербального спілкування, наочних форм впливу та поширення чуток.

Наведене вище визначає особливості інформаційно-психологічного впливу противника на особовий склад Збройних Сил України під час підготовки і виконання завдань.

На відміну від МВС України та окремих силових структур держави Збройних Сил України відповідно до чинного законодавства мають структури для проведення психологічних операцій або акцій, спрямованих проти противника, які і безпосередньо здійснюють протидію інформаційно-психологічному впливу противника.

Сутність і зміст оцінювання інформаційно-психологічному впливу полягає:

– по-перше, необхідно визначити склад організаційного ядра протидіючих сил, мету їх дій, засоби, які вони використовують для здійснення інформаційно-психологічного впливу, та зміст і спрямованість цього впливу на різні категорії

військовослужбовців ВВ під час підготовки і виконання службово-бойових завдань;

– по-друге, визначити, або спрогнозувати негативні наслідки інформаційно-психологічного впливу на свідомість і психіку різних категорій військовослужбовців, рівень морально-психологічного стану та професійної діяльності;

– по-третє, вжити організаційні заходи щодо зменшення або локалізації негативного інформаційно-психологічного впливу на військовослужбовців, підготувати та довести до особового складу контрматеріали, використовуючи методи і форми виховної роботи з урахуванням особистісних особливостей військовослужбовців, та здійснити аналіз ефективності проведених контрзаходів.

Таким чином, запропонований підхід дозволяє оцінити в кількісному вимірі рівень інформаційно-психологічного впливу на певну цільову аудиторію за певний проміжок часу. Це допоможе відповідному органу військового управління відносно об'єктивно прогнозувати можливі наслідки та адекватно і на випередження реагувати (протидіяти) негативним процесам. Тому цю методику необхідно розглядати як невід'ємний елемент підсистеми моніторингу ситуації у загальному контурі системи протидії негативному інформаційно-психологічного впливу на особовий склад.

Література

1. Биченок М.М. Формалізація та оцінювання інформаційних загроз національним інтересам / М.М. Биченок, В.М. Шемаєв // Труди університету. - № 1 (100). – К.: НУОУ, 2011. – С. 54 – 61.

2. Військовий стандарт ВСТ 01.004.004 – 2014 (01) "Інформаційна безпека держави у воєнній сфері. Терміни та визначення".

Іжутова І.В.
к.держ.упр.,
Національний університет оборони України
Шубін В.В.
ТОВ "ІТ-Інтегратор"

АКТУАЛЬНІ АСПЕКТИ "ПРОТИДІЇ" ІНФОРМАЦІЙНИМ ТА ПСИХОЛОГІЧНИМ ВПЛИВАМ рф

Підходи до інформаційних та психологічних впливів змінюються разом із розвитком технологій, які не стоять на місці. Так само, на нашу думку, потрібно змінювати й дефініції та уникати використання саме терміну "протидія", концентруватися на формуванні психологічної оборони населення, його стійкості до інформаційних та психологічних впливів. Якщо ми сформуємо максимально

стійке суспільство, здатне аналізувати інформацію, яка подається, суспільство, яке не впускатиме в себе таку інформацію, що спрямована на зміну його поведінки, примушення до дій, реагування, потреба у так званій протидії зникне сама по собі через непотрібність та неактуальність.

Це питання нерозривно пов'язане із комунікаціями, а в них ми завжди наголошуємо на необхідності застосування проактивності. Отже, такою проактивністю у випадку інформаційних впливів і буде стійкість. Звісно, що на її формування потрібен час, але при її досягненні вдасться уникнути багатьох інформаційних проблем, мати більш зріле суспільство, здатне критично ставитися до інформації, уникати роздмухування необґрунтованої "зради", поширення дезінформації та фейків.

Що ж для цього потрібно і чому це так важливо? В країні було вжито декілька кроків, спрямованих на підвищення рівня медіаграмотності громадян, але вони не дали бажаних результатів, а широкомасштабне вторгнення рф в Україну лише проявило проблематику, пов'язану з необхідністю розвивати цей напрям, загострило її.

Важливим аспектом є забезпечення просвітницької діяльності за цим напрямом.

Обов'язкове інтегрування занять-тренінгів (занять в ігровій формі) з медіаграмотності на всіх рівнях освіти сприятиме насиченню інформаційного поля цією тематикою.

Демонстрація коротких навчальних сюжетів з медіаграмотності в громадському транспорті, на вулиці, по телебаченню, в громадських місцях або у вигляді реклами, на нашу думку, могло б допомогти підвищити цей рівень. Психологічно людина сприймає інформацію краще, коли вона відчуває свою свободу, не відчуває зобов'язання та примусу її вивчати та запам'ятовувати.

Розповсюдження інформації такого характеру в малих групах в соціальних мережах та месенджерах також сприятиме формуванню захисного щиту на локальному рівні, адже саме на ньому виникає багато проблем через швидке споживання інформації у вузьких колах. Ці групи, як правило, закриті, тому інформація в них користується довірою, її максимально всі переглядають і роблять це саме в ненав'язливій формі.

Противник, зокрема, активно використовує їх для здійснення інформаційного та психологічного тиску, тому цей простір може бути активно використаний на користь розвитку медіаграмотності.

Отже, потрібно відходити від поняття протидія інформаційному впливу до формування стійкого суспільства, резистентного до інформаційного та психологічного втручання. Починати процес розвитку стійкої особистості необхідно зі школи і забезпечувати просвітницький процес протягом всього життя, таким чином досягаючи "life-long learning". Крім того, форму освіти з медіаграмотності потрібно обирати відповідно до аудиторії, зважаючи на те, як

вона краще сприймає інформацію: гра, відео, задачі, реклама тощо.

Кацалап В.О.
к.військ.н., доцент
Національний університет оборони України імені Івана Черняховського

СИНТЕЗ ПРОТИДІЇ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ ПРОТИВНИКА НА ОСОБОВИЙ СКЛАД ВІЙСЬК (СИЛ)

У державному механізмі реагування, пов'язаному із впливом на соціальне середовище, чи не найскладнішим є завдання моніторингу ситуації з метою визначення кількісних параметрів стосовно соціальних груп, зокрема, оцінки рівня психологічного впливу на особовий склад Сил оборони України.

У свою чергу, рівень рівня психологічного впливу на особовий склад Сил оборони України залежить від ряду чинників, одним із головних серед яких є чинник інформаційно-психологічного впливу на певну соціальну групу (цільову аудиторію).

Тому формування інформаційних установок у свідомості людей здійснюється шляхом тематичного інформаційно-психологічного впливу на цільову аудиторію, який може бути як позитивним, так і негативним, залежно від оцінки характеру такого впливу.

З точки зору забезпечення інформаційної безпеки особи, суспільства, держави негативний характер інформаційно-психологічного впливу викликає потребу всебічного захисту та реабілітації цільової аудиторії, яка зазнає такого впливу, а також проведення упереджувальних заходів для його унеможливлення або зниження рівня ефективності, що у сукупності складає сутність процесу протидії такому впливу [1].

Зазначений процес стає особливо важливим та актуальним для особливого періоду, коли інформаційно-психологічний вплив противника проявляється найбільш характерно. Для періоду воєнного стану необхідно проводити упереджувальні заходи для здійснення протидії на основі моніторингу інформаційного простору воєнної сфери, коли явища цілеспрямованого та акцентованого впливу ще немає, але є ситуація можливого виявлення викликів і загроз щодо зовнішнього інформаційно-психологічного впливу на особовий склад військ (сил) [2].

Для визначення подальших шляхів наукового дослідження щодо удосконалення системи протидії негативному інформаційно-психологічному впливу на особовий склад військ (сил), зокрема аналіз світового досвіду побудови таких систем необхідно інтегрувати потенціал ряду структурних підрозділів Міністерства оборони України та ЗС України. Результати такого аналізу

засвідчать, що першочерговим елементом для ефективного функціонування такої системи має бути методична складова, що дозволяє виявляти та кількісно оцінювати рівень негативного інформаційно-психологічного впливу на визначені цільові аудиторії, до сьогодні в науковому середовищі в достатньому обсязі ще не опрацьовано.

Отже, в результаті цих досліджень необхідно сформувати потребу наукового обґрунтування методичних засобів виявлення і оцінювання у кількісному вимірі рівня негативного інформаційно-психологічного впливу на особовий склад військ (сил) як основи ефективного функціонування підсистеми оцінювання рівня негативного інформаційно-психологічного впливу на особовий склад військ (сил) та органи військового управління у загальній системі протидії такому впливу.

Науковим методом вирішення цього завдання може бути метод на основі анкетування фахового середовища України та статистичної обробки висловлювань задіяних експертів. При цьому пропонується 5 класифікацій будь яких повідомлень або контенту з подальшим оцінювання рівнів негативного інформаційно-психологічного впливу на особовий склад військ (сил):

інформаційні явища ;

інформаційні факти;

відомості;

дані;

інформація.

Пропонується за допомогою експертного середовища визначити класи та підкласів інформаційних процесів (дій, фактів), які можуть спостерігатися в інформаційному просторі держави та впливати на морально-психологічний стан військ (сил). Визначено “вагу” кожного з таких процесів на шкалі від 0 до 100, в результаті чого створено можливість кількісно оцінити сукупний інформаційний процес, що впливає на свідомість особового складу за певний проміжок часу, тобто “зважену” інтенсивність сукупного негативного інформаційного процесу.

Синтез протидії інформаційно-психологічного впливу противника на особовий склад військ (сил) спрямований на:

завершення розробки методики, тобто визначення критеріальних рівнів оцінки негативного інформаційно-психологічного впливу на особовий склад військ (сил) та органи військового управління;

визначення основних вимог до системи протидії негативному інформаційно-психологічному впливу на особовий склад військ (сил) та органи військового управління в частині виявлення і оцінки рівня негативного інформаційно-психологічного впливу;

обґрунтування загальної структури перспективної системи протидії негативному інформаційно-психологічному впливу на особовий склад військ (сил) та органи військового управління (в частині виявлення і оцінки рівня негативного інформаційно-психологічного впливу);

розробку пропозицій щодо реалізації державної інформаційної політики в Міністерстві оборони України та ЗС України з метою проведення упереджувальних заходів щодо протидії негативному інформаційно-психологічному впливу на особовий склад військ (сил) та органи військового управління.

Література

1. Військовий стандарт ВСТ 01.004.004 – 2014 (01) "Інформаційна безпека держави у воєнній сфері. Терміни та визначення".

2. Організаційно-методичні рекомендації з формування оперативно-стратегічних і оперативно-тактичних вимог до перспективних зразків (комплексів, систем) озброєння та військової техніки (затверджено начальником Генерального штабу Збройних Сил України 26.11.2019 р.).

Kovalchuk L.V.
doctor of technical science, professor,
State Service of Special Communications and Information Protection of Ukraine
Lysenko N.V.
State Service of Special Communications and Information Protection of Ukraine

SMALL SUBGROUP ATTACKS ON ELLIPTIC CURVE CRYPTOSYSTEMS IN CASE OF INCORRECT USAGE OF ALGORITHM

All elliptic cryptosystems, such as encryption, key encapsulation, digital signature, key exchange, are built in group of large prime order n (such as $\log n \geq 128$). This is base requirement for cryptosystem security [1, 2, 3]. But actually, working with elliptic curve group, we only choose some subgroup of large prime order in group of elliptic curve points, whose order usually is not prime. Practical implementation of operations for prime order elliptic curve has some problem, so such type of elliptic curves is not wide-used in practice.

The problem can be solved by using complete addition laws. Such law exists also for prime-order curves [4, 5], but it is much more faster and simpler for such types of elliptic curves, which always has non-prime order – such as (complete and twisted) Edwards curves [6, 7], Hessian curves [7], Jacobi quartics [8] or Jacobi intersections [9, 10]. All curves of these types have a so-called *cofactor* in their orders, usually denoted as h. In other words, the order of such curve E is $|E| = h \cdot n$, where n is large prime and h is always divisible by 3 – for Hessian curves, and is always divisible by 4 – for other curves mentioned above.

Though many authors believe that advantages of non-prime-order group, such as points of Edwards curve, outweigh their disadvantages, there exist some classes of attacks, to which such groups are vulnerable. And first of all these are so-called *small-*

subgroup attacks.

Subgroup of small order, or small-subgroup, always exists if the group order is dividable on small prime number or its power. If, for example, we consider Edwards curve, its order is always divisible on $h = 2^k$, for some $k \geq 2$. So such curve always has points of order at least 2 and 4.

The main idea of small subgroup attacks is the following [11r]: if, performing some algorithm, we multiply some curve point P of prime order on some number u, and T is some point of small order, such that $\operatorname{ord} T | u$, than $u \cdot (P + T) = u \cdot P$. So in attack the adversary may change some point P, where $\operatorname{ord} P = n$, with point $P + T$, and, under some trivial condition, such changing may not be noted.

Such attack may be applied to both encryption algorithm and signature algorithm, in particular, like [12] or [13], and in the worst case may be cause to leakage of several least bits of private key.

Here we describe attack on signature algorithm, similar to [12], and describe how we can prevent it.

Briefly, we can describe signature procedure according to [12] in the next way. Let P be base point of elliptic curve E over F_{2^m}, $Q = -dP$ be some public key for some person, d be corresponding private key, M be signed message, $H : V^* \to V_l$ be cryptographic hash.

Digital signature procedure according to DSTU 4145:

1. Generate random e, $2 < e < n - 2$.
2. Calculate $R = eP = (x_R, y_R)$, where $x_R, y_R \in F_{2^m}$.
3. Calculate $f = H(M)$ and convert it into element of F_{2^m}.
4. Calculate $y = f \cdot x_R$ (as field elements).
5. Calculate $s = (e + dr) \bmod n$.
6. Create signature $S = (r, s)$.
7. Send (M, h, S) to Verifier.

Digital signature verification procedure according to DSTU 4145:

1. Signature $S' = (r', s')$ (it may be different from S) convert into 2 numbers r', s'.
2. Calculate elliptic curve point $R' = s'P + r'Q = (x'_R, y'_R)$.
3. Calculate $f' = H(M')$
4. Calculate $\tilde{r} = f' \cdot x'_R$.
5. Check if $r' = \tilde{r}$.

Note that algorithm described in DSTU also has some intermediate checking of parameter correctness, and now we are going to show that such checkings are necessary

to resist small subgroup attacks.

1. If we don't check correctness of public key Q (that $\mathrm{ord}\,Q = n$), than adversary may use somebody's else signature, created earlier, and prove that this is his signature with public key $Q' = Q + T$, where $\mathrm{ord}\,T \mid \mathrm{lcd}(h, r)$.

2. If signer uses some untrusted party to create base parameters and doesn't check correctness of base point P, adversary may give him point $P' = P + T$, where $\mathrm{ord}\,T \mid h$. Then adversary can recover several bits of his private key, having his public key.

One of recommendation to avoid such situations is to include information about P and Q into hash-value, as it is used to do in non-interactive zero-knowledge proofs in so-called "Fiat-Shamir heuristic" approach to calculate non-interactive Verifier's challenge. For example, to use $f = H(M \,||\, P \,||\, Q)$ instead of $f = H(M)$.

References

1. Michel Abdalla and David Pointcheval. Simple password-based encrypted key exchange protocols. Topics in cryptology–CT-RSA 2005, pages 191–208, 2005.

2. Dan Boneh, Shai Halevi, Mike Hamburg, and Rafail Ostrovsky. Circular-secure encryption from decision diffie-hellman. In Advances in Cryptology–CRYPTO 2008, pages 108–125. Springer, 2008.

3. Dan Harkins. Dragonfly: A pake scheme, 2012. http://www.ietf.org/ proceedings/83/slides/slides-83-cfrg-0.pdf.

4. Daniel Bernstein and Tanja Lange. Complete addition laws for elliptic curves, 2009. http://cr.yp.to/talks/2009.04.17/slides.pdf.

5. Joppe W. Bos, Craig Costello, Patrick Longa, and Michael Naehrig. Selecting elliptic curves for cryptography: An efficiency and security analysis. Cryptology ePrint Archive, Report 2014/130, 2014. http://eprint.iacr.org/.

6. H.M. Edwards. A normal form for elliptic curves. Bulletin-American Mathematical Society, 44(3):393, 2007.

7. Reza R Farashahi and Marc Joye. Efficient arithmetic on hessian curves. In Public Key Cryptography–PKC 2010, pages 243–260. Springer, 2010.

8. Olivier Billet and Marc Joye. The jacobi model of an elliptic curve and side-channel analysis. In Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, pages 34–42. Springer, 2003.

9. H¨useyin Hı¸sıl, Kenneth Wong, Gary Carter, and Ed Dawson. Faster group operations on elliptic curves. Cryptology ePrint Archive, Report 2007/441, 2007. http://eprint.iacr.org/.

10. P-Y Liardet and Nigel P Smart. Preventing spa/dpa in ecc systems using the jacobi form. In Cryptographic Hardware and Embedded Systems? CHES 2001, pages 391–401. Springer, 2001.

11. Mike Hamburg. Decaf: Eliminating cofactors through point compression. Rambus Cryptography Research, mhamburg@cryptography.com, (This is a minor

revision of a CRYPTO 2015 paper, c©2015 IACR), https://www.shiftleft.org/papers/decaf/decaf.pdf
12. DSTU 4145:2002
13. DSTU 9041:2020

Козюра В.Д.
к.т.н., доцент
Національна академія Служби безпеки України
Хорошко В.О.
д.т.н., професор
Національний авіаційний університет

ДЕЯКІ АСПЕКТИ АНАЛІТИКО-РОЗВІДУВАЛЬНОЇ РОБОТИ В ДІЯЛЬНОСТІ СЛУЖБИ БЕЗПЕКИ ОРГАНІЗАЦІЇ

Аналітико-розвідувальний напрямок в діяльності служби безпеки організації можна визначити як один з основних видів діяльності, що передбачає збір, узагальнення та обробку інформації, яка стосується конкурентних організацій, установ, працюючих в спільній галузі, про умови ведення бізнесу, а також про конкурентні дії з підґрунтям кримінальної спрямованості. Функції по роботі за вказаним аналітичним напрямком може виконувати відділ забезпечення зовнішньої діяльності підрозділу інформаційно-аналітичної роботи підприємства завданнями якого є:

– виявлення фактичних можливостей розголошення, витоку та реалізації способів несанкціонованого доступу до конфіденційної інформації;

– оцінка надійності та ступеня захищеності підприємства від внутрішніх та зовнішніх загроз;

– прогнозування можливих проявів зацікавленості конкурентів до конкретних матеріалів та розробок підприємства;

– виявлення обставин та причин, що сприяють витоку комерційної інформації;

– участь в аналізі, розробці та впровадженні комплексних економічно та науково обґрунтованих заходів щодо захисту інтересів підприємства.

Глибокий детальний та ретельний аналіз діяльності своїх конкурентів, обов’язок відділу забезпечення безпеки зовнішньої діяльності, якому він повинен приділяти особливу увагу.

В той же час поряд зі збором інформації про конкурентів служба безпеки повинна блокувати намагання збору інформації про діяльність власного підприємства. Для цієї мети організовується контррозвідувальний відділ в складі підрозділу інформаційно-аналітичного забезпечення.

В сучасних умовах роль та значення контррозвідки служби безпеки підприємства обумовлені наступними обставинами: в першу чергу, прагненням деяких підприємців усунути або нейтралізувати своїх конкурентів за допомогою засобів економічного шпигунства, по-друге, підвищеним рівнем криміналізації населення, і як наслідок вирішення своїх потреб певними категоріями громадян злочинним шляхом.

При проведенні інформаційно-аналітичної роботи необхідно забезпечити виконання наступних завдань:

– забезпечити своєчасне надходження надійної та всебічної інформації по ключовим питанням, що становлять зацікавленість для підприємства;

– здійснення постійного аналізу подій в зовнішній конкурентній сфері та в галузі в цілому, які можуть мати значення для інтересів підприємства;

– забезпечення безпеки власних інформаційних ресурсів;

– опис сценаріїв дій конкурентів, які можуть впливати на поточну сферу інтересів підприємства;

– забезпечення ефективності та виключення можливості дублювання інформації при збиранні, аналізі та розповсюдженні.

Діяльність інформаційно-аналітичного підрозділу служби безпеки підприємства має бути направлена на прогнозування ситуацій, а також формування відповідних інформаційних напрацювань, необхідних для ефективного прийняття управлінських рішень.

Виходячи із вказаного, метою контррозвідувального підрозділу є протидія розвідувальним заходам конкурентів та припинення правопорушень з боку кримінальних груп або окремих осіб, які посягають на інтереси підприємства. На відміну від розвідки, об'єктом контррозвідувальної діяльності є не зовнішнє, а внутрішнє середовище функціонування підприємства. Це середовище включає в себе наступні елементи:

– керівний склад підприємства (директор, його заступники, фінансовий директор і т.д.) як потенційні об'єкти розвідувальних заходів та/або злочинів з боку конкурентів;

– особи з допоміжного персоналу, що мають доступ до комерційної таємниці;

– співробітники підприємства, з боку яких потенційно існує небезпека надання зацікавленій стороні таких відомостей, які допоможуть їм вчинити злочин проти підприємства;

– співробітники служби безпеки;

– раніше судимі особи з числа працівників підприємства;

– співробітники підприємства, родичі яких працюють у конкуруючих установах та організаціях;

– працівники, які раніше працювали на підприємства та були звільнені з нього;

– особи, які в силу своїх посадових обов'язків регулярно приймають

відвідувачів підприємства.

Визначення мети та об'єкта контррозвідувальної діяльності дозволяє визначити коло можливих завдань підрозділу контррозвідки:

– боротьба з економічним шпигунством;

– припинення злочинів проти всіх співробітників на їх робочих місцях та окремих груп співробітників;

– надання сприяння правоохоронним, судовим і контрольно-наглядовим органам в документуванні протиправних дій осіб, які вчиняють кримінальні злочини та адміністративні правопорушення.

Реалізація завдань підрозділом контррозвідки відбувається через виконання наступних функцій:

– постійне інформування керівництва підприємства про причини, що породжують та умови, які сприяють вчиненню правопорушень з боку персоналу;

– збір відомостей і документів у цивільних та кримінальних справах по напряму роботи підприємства;

– виявлення осіб з числа персоналу, які сприяють зацікавленим особам (які не працюють на підприємстві) у вчиненні ними злочинів;

– документування дій осіб, затриманих за адміністративні правопорушення;

– викриття економічних (промислових) шпигунів з числа персоналу;

– інформування керівників підприємства та інших співробітників про злочини які плануються до здійснення щодо них;

– пошук безвісти зниклих співробітників підприємства;

– створення умов, що виключають підслуховування розмов в службових кабінетах;

– встановлення обставин розголошення відомостей, що становлять комерційну таємницю;

– з'ясування біографічних та інших даних, що характеризують особистість про співробітників підприємства (з їхньої письмової згоди) при укладенні ними трудових контрактів;

– пошук втраченого співробітниками майна, що належить підприємству.

Аналіз загроз є одним з найважливіших напрямів аналітичної роботи та являє собою узагальнену модель захисту від загроз, яким піддається об’єкт захисту.

Таким чином, фактичне проведення аналітичної роботи, результати її діяльності визначають структуру та склад системи захисту інформації та напрям її удосконалення. При відсутності ґрунтовної аналітичної роботи стає практично неможливим виявлення та контроль каналів несанкціонованого доступу до конфіденційної інформації підприємства.

Козюра В.Д.
к.т.н., доцент
Національна академія Служби безпеки України
Юрх Н.Г.
Національна академія Служби безпеки України

ВДОСКОНАЛЕННЯ ОРГАНІЗАЦІЇ ЗАХИСТУ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Система захисту інформації на об'єктах критичної інфраструктури – це організована сукупність нормативно-правових, організаційних та інженерно-технічних напрямків, методів (створення перешкод на шляху загрози, надання управляючих впливів на елементи системи, що захищається, маскування системи та інформації, регламентація дій при накопиченні та обробці інформації, примус і спонукання), засобів (фізичних, апаратних, програмних, криптографічних та стеганографічних) та заходів, що знижують вразливість інформації і перешкоджають несанкціонованому доступу до інформації, її розголошенню або витоку.

Організація ефективного функціонування системи забезпечується наступними важливими вимогами:

- особиста відповідальність керівників організації, співробітників в частині, що стосується цілісності носіїв, конфіденційності інформації, упорядкування переліку конфіденційних даних та інших документів, що охороняються;
- здійснення доступу співробітників до конфіденційної інформації згідно встановлених правил;
- створення служби забезпечення безпеки, що має на меті впровадження системи захисту, яка реалізовується згідно зі встановленими правилами та нормативним забезпеченням.

Виходячи з цінності інформації володільці інформаційних ресурсів на власний розсуд визначають ступінь захищеності власних ресурсів, типи систем, необхідні засоби та способи захисту. Охоплення структурою системи захисту має включати не лише інформаційні системи, а також наявний управлінський комплекс об'єкта в сукупності функціональних та виробничих підрозділів, звичного документообігу.

Комплексність системи безпеки є її основною характеристикою. Під цим розуміється наявність в ній обов'язкових складових, які охоплюють всі напрямки захисту інформації. Співвідношення складових, їх наповненості забезпечує неповторність побудови системи захисту інформації стосовно окремого об'єкта і гарантують унікальність системи, що створює складний бар'єр для подолання.

Для правового елемента системи захисту інформації основою є норми інформаційного права, що передбачають юридичне закріплення відносин об'єкта

та держави з приводу правомірності використання системи захисту інформації, обов'язків підприємства та персоналу щодо дотримання встановлених володільцем інформації обмежувальних і технологічних заходів захисного характеру, а також відповідальності співробітників за порушення порядку захисту інформації. Цей елемент передбачає:

- наявність в організаційних документах підприємства, правилах внутрішнього трудового розпорядку, контрактах, укладених зі співробітниками, наявність в посадових і робочих інструкціях положень та зобов'язань щодо захисту інформації;
- формулювання та доведення до відома всіх співробітників установи положення про правову відповідальність за розголошення конфіденційної інформації, несанкціоноване поводження або фальсифікацію документів;
- роз'яснення співробітникам підприємства, положення щодо добровільності прийнятих ними на себе обмежень, пов'язаних з виконанням обов'язків по захисту інформації.

Організаційний елемент системи захисту інформації включає в себе необхідність:

- формування та організації діяльності служби безпеки;
- складання та регулярного оновлення переліку інформації, що захищається на підприємстві;
- порядку захисту інформації підприємства від випадкових або навмисних несанкціонованих дій персоналу;
- ведення всіх видів аналітичної роботи;
- використання методів відбору персоналу для роботи з інформацією, що захищається, методики навчання та інструктування співробітників;
- формування напрямків та методів виховної роботи з персоналом та контролю дотримання співробітниками порядку захисту інформації;
- створення технології захисту, обробки та зберігання документів підприємства у всіх видах;
- створення системи розмежування доступу співробітників до інформації, що захищається;
- встановлення порядку захисту інформації при проведенні нарад, засідань, переговорів, прийому відвідувачів, роботі з представниками сторонніх організацій, засобів масової інформації;
- створення системи охорони території, будівлі, приміщень, обладнання, транспорту та персоналу підприємства;
- обладнання та атестації приміщень та робочих зон, виділених для роботи з конфіденційною інформацією, ліцензування технічних систем і засобів захисту інформації та охорони, сертифікації інформаційних систем, призначених для обробки інформації, що захищається;
- організації пропускного режиму на території, в будівлі та приміщеннях

підприємства, ідентифікації персоналу і відвідувачів;

- дій персоналу в екстремальних ситуаціях;
- організаційних питань придбання, установки та експлуатації технічних засобів захисту інформації та охорони;
- організаційних питань захисту персональних комп'ютерів, інформаційних систем, локальних мереж;
- роботи з управління системою захисту інформації;
- формування критеріїв та порядку проведення оціночних заходів по встановлення ступеня ефективності системи захисту інформації.

Організаційний напрям захисту є головним напрямом створення комплексної системи безпеки підприємства. На думку більшості фахівців, заходи організаційного захисту інформації складають 50-60% в структурі більшості систем захисту інформації.

Інженерно-технічний елемент системи захисту інформації призначений для пасивної та активної протидії інформаційним та кіберзагрозам й формування кордонів охорони території, будівлі, приміщень та обладнання за допомогою комплексів технічних засобів. Вартість засобів технічного захисту та охорони суттєва, попри це значення цього елементу при захисті інформаційних систем важко переоцінити. Елемент включає в себе:

- створення інженерного захисту від проникнення сторонніх осіб на територію, в будівлю та приміщення (паркани, ґрати, сталеві двері, кодові замки, ідентифікатори, сейфи та ін.);
- засоби захисту технічних каналів витоку інформації, що виникають при роботі ЕОМ, засобів зв'язку, копіювальних апаратів, принтерів, факсів та іншого обладнання, при проведенні нарад, засідань, переговорів з відвідувачами та співробітниками, диктування документів і т.п.;
- засоби захисту приміщень від візуальних способів технічної розвідки;
- засоби забезпечення охорони території, будівлі та приміщень (засоби спостереження, оповіщення, охоронної та пожежної сигналізації);
- засоби виявлення приладів та пристроїв технічної розвідки (підслуховуючих та передавальних пристроїв, таємно встановленої мініатюрної звукозаписної та телевізійної апаратури і т.п.).

Програмно-апаратний елемент системи захисту інформації призначений для захисту важливої інформації, що піддається обробці та зберігається на комп'ютерах, серверах, на робочих станціях локальних мереж та різних інформаційних системах. Деякі елементи цієї системи захисту можуть застосовуватися також як додаткові засоби в інженерно-технічному та організаційному захисті. Елемент включає в себе:

- автономні програми для забезпечення захисту інформації та контроль ступеня її захищеності;
- програми захисту інформації, що працюють в комплексі з програмами

обробки інформації;

- програми захисту інформації, що працюють в комплексі з технічними пристроями захисту інформації.

Криптографічний елемент системи захисту інформації призначений для захисту конфіденційної інформації методами криптографії. Елемент включає:

- регламентацію використання різних криптографічних методів в ЕОМ та локальних мережах;
- регламентацію використання засобів криптографічного перетворення переговорів по незахищених каналах телефонного та радіо зв'язку;
- регламентацію доступу до баз даних, файлів, електронних документів з персональними паролями, які ідентифікуються командами та іншими методами;
- регламентацію доступу персоналу у виділені приміщення за допомогою ідентифікуючих кодів, шифрів.

В залежності від поставлених завдань захисту інформації на конкретному об’єктові критичної інфраструктури окремі елементи системи захисту можуть бути реалізовані на практиці тільки як складові частини системи в цілому.

Кравчук А.І.
Житомирського військового інституту імені С.П. Корольова

ПРОБЛЕМА ПРОТИДІЇ ІНФОРМАЦІЙНИМ, ПСИХОЛОГІЧНИМ ВПЛИВАМ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ НА ОСОБОВИЙ СКЛАД ЗБРОЙНИХ ФОРМУВАНЬ СТРУКТУР СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

Україна вже другий рік стримує повномасштабну агресію Російської Федерації, що переросла із гібридної війни, розпочатої росіянами проти України в 2014 році. Поряд із веденням бойових дій Україна продовжує відчувати на собі потужні і численні інформаційні атаки, спрямовані на різні цільові аудиторії, що створюють реальні загрози інформаційній безпеці держави і потребують здійснення постійних заходів інформаційної протидії.

Водночас слід зауважити, що інформаційні операції – це надтонка сфера діяльності, де відбувається робота з психікою людини (цільової аудиторії), тому, з одного боку потребує надзвичайного професіоналізму і спеціальних знань у різноманітних (невійськових) галузях, починаючи від психології, релігієзнавства, соціології, політології, міжнародної історії, права тощо, з іншого ж, тут немає чітких маркерів ефективності діяльності саме тому, що робота спрямована на психологію великих груп, яка змінюється надто повільно і непомітно, особливо враховуючи потужний контрвплив з боку постійно діючої пропаганди країни ворога, країни агресора, у даному разі – Російської Федерації, де пропаганда історично є могутньою та впливовою базовою інституцією держави, яка проникла

у всі її сфери і працює не лише через ЗМІ, але й навіть через російську православну церкву [1].

Тож для проведення ефективних заходів протидії російським інформаційним впливам Україні потрібна дієва система протидії, утворена на державному рівні, що базується на всебічно обґрунтованій та практично вивіреній нормативно-правовій базі. Отже, **метою** даної роботи є виявлення та дослідження існуючих проблем протидії інформаційним, психологічним впливам рф на особовий склад збройних формувань структур сектору безпеки і оборони України.

Темою дослідження було взято один із тематичних напрямів роботи конференції – проблема протидії інформаційним, психологічним впливам рф на особовий склад збройних формувань структур сектору безпеки і оборони України у зв'язку з тим, що вже в самій назві міститься ряд питань, які слід розглянути. Зокрема, предметом дослідження є особовий склад збройних формувань структур сектору безпеки і оборони України.

Питання сектору безпеки і оборони України вже протягом багатьох років є предметом дискусій українських вчених. Особливої уваги дана тема набула після затвердження Указом Президента України від 12 лютого 2007 року "Стратегії національної безпеки України" [2]. Як стверджують науковці, саме вона стала першим документом, який офіційно в Україні ввів поняття "сектор безпеки і оборони України".

С. Поляков зауважив, що термін "сектор безпеки і оборони України" не є усталеним і не має чітких традицій його вживання [3].

Наразі поняття "**сектор безпеки і оборони**" визначено законодавцем у Законі України "Про національну безпеку України», так само як і поняття "**національні інтереси**" та "**національна безпека**". Натомість при більш ретельному дослідженні сектору безпеки і оборони як явища виходимо на його дві з чотирьох складових: **сили безпеки**, на які покладено функції із забезпечення **національної безпеки** України, і **сили оборони**, на які покладено функції із забезпечення **оборони** держави. І якщо з поняттям **національної безпеки** в даному Законі жодних запитань не виникає, через те що його визначення у Законі є, то що таке "**оборона держави"** законодавець не зазначає, через що вся, ніби то струнка конструкція такого фундаментального явища, як **сектор безпеки і оборони,** сиплеться через нерозуміння, а в чому все ж таки принципові відмінності між зазначеними складовими: силами безпеки та силами оборони [4]?

У Законі України "Про національну безпеку України" є лише одне згадування щодо **оборони України** в ч.1 ст.16, де сказано, що "Збройні Сили України є військовим формуванням, на яке відповідно до Конституції України покладаються **оборона** України, захист її суверенітету, територіальної цілісності та недоторканності", чим фактично скеровує з цього питання до Конституції України.

Водночас Конституція України так само має лише одне згадування щодо

поняття "**оборони**" в ст.17, де зазначено, що "оборона України, захист її суверенітету, територіальної цілісності і недоторканності покладаються на Збройні Сили України", тобто також не дає визначення що ж таке "**оборона України"** [5].

Так само і в Законі України "Про оборону України" в ст.2 зазначено, що "**оборона** України базується на готовності та здатності органів державної влади, **усіх складових сектору безпеки і оборони України**…", що лише ускладнює розуміння, що ж тоді належить до сил оборони [6]. Натомість, не розуміючи, що таке **оборона держави,** ми так і не зможемо чітко уявити, що є **сили оборони** і чим вони відрізняються від **сил безпеки.**

Цей поверхневий аналіз лише щодо одного визначення свідчить про те, що нормативно-правова база за цим напрямом потребує подальшого більш глибокого осмислення та вдосконалення, бо, не маючи розуміння таких фундаментальних понять, як складові **сектору безпеки і оборони, зокрема – сили оборони,** важко оперувати цими категоріями без знань про що насправді йдеться. Крім того, відсутність чітко сформульованого понятійного апарату значно ускладнює взаємодію між суб'єктами сектору безпеки і оборони та їх координацію, роблячи цей процес розмитим, малозрозумілим, а звідси й – неефективним.

Щодо існуючих проблем здійснення протидії інформаційним, психологічним впливам рф на особовий склад збройних формувань структур сектору безпеки і оборони України, то слід зазначити, що, виходячи із практики здійснення протидії інформаційним, психологічним впливам рф, таке широке поняття, як "особовий склад збройних формувань структур сектору безпеки і оборони" на практиці зводиться в основному до Збройних Сил України, на які припадає основне навантаження із **оборони України**.

Практика здійснення протидії інформаційним, психологічним впливам рф показала, що безпосередньо на особовий склад збройних формувань структур сектору безпеки і оборони України, а точніше, на особовий склад Збройних Сил України, ворог впливає вкрай рідко. За своєю суттю такі спроби були малопотужні, поодинокі, а, головне, малозначні та неефективні. Основні ж зусилля інформаційних, психологічних впливів рф під час здійснення повномасштабної агресії здебільшого спрямовані на населення окупованих територій. Водночас як впливи на особовий склад Збройних Сил (сектору безпеки і оборони), так і на населення окупованих територій мають одні і ті ж самі, спільні наративи, зокрема:

- навіть після викриття злочинів у Бучі та інших українських містах російська пропаганда в листівках постійно і наполегливо стверджує, що "російська армія не воює з українськими солдатами та не обстрілює мирне населення", війна відбувається з колективним Заходом заради ліквідації київського режиму (хунти), який давно і повністю продався Заходу;

- війна розпочалась через "західні плани" знищити російський та український

народи, тому її називають "операцією з ліквідації антинародного київського режиму";

- у російській агресії винними є самі українці та незаконно обрана ними влада неонацистів, отож: "горе, що спіткало вас – результат злочинної політики київського режиму";

- російська армія здійснює "захист Донбасу" і не має на меті знищення української державності та окупації усієї України.

- "не думайте, що це буде швидко та безболісно" – застерігають окупанти, готовлячи людей до довготривалих бойових дій, тим самим змушуючи більшість тікати з прифронтових територій, залишаючи їх для росіян, які так само активно їх заселяють переселенцями з російської глибинки, незаконно надаючи їм житло українців.

- українців активно закликають до колаборації з росіянами та попереджають про небезпеку для життя у разі наближення до російських військових.

Отже, якщо розглядати суто питання проблематики протидії інформаційним, психологічним впливам рф саме на особовий склад збройних формувань структур сектору безпеки і оборони України, то на сьогодні цих проблем небагато і вони є незначними, на що впливають два тісно взаємопов’язаних чинники:

1. Сам вплив є незначним, а головне, малоефективним.

2. Неефективність впливу зумовлена високою мотивацією до збройного протистояння особового складу збройних формувань структур сектору безпеки і оборони України, що фактично зводить нанівець усі потуги і намагання Російської Федерації щодо здійснення інформаційного, психологічного впливу.

Висновки. Зазначені неточності в формулюваннях фундаментальних понять, які належать до сектору безпеки і оборони, свідчать про існуючі прогалини в нормативно-правовому забезпеченні цього важливого для безпеки держави напряму та потребують більш ретельного вивчення, вдосконалення та виправлення нормативно-правового забезпечення. Щодо проблем інформаційних, психологічних впливів, то вони більше стосуються населення на окупованих територіях, а ніж особового складу збройних формувань структур сектору безпеки і оборони України, і потребують потужного дослідження саме в цій галузі за цим напрямом. Хоча б тому, що опосередковано вплив на населення віддзеркалюється впливом і на особовий склад збройних формувань структур сектору безпеки і оборони України, тому розділяти ці два явища не слід.

Література

1. Як працюють РПЦ і Гундяєв на інформаційному фронті проти України (ДОСЛІДЖЕННЯ). Сайт: TEXTY.ORG.UA URL: https://texty.org.ua/fragments/108345/yak-pracyuyut-rpc-i-gundyayev-na-informacijnomu-fronti-proty-ukrayiny-doslidzhennya/?src=read_next&from=103386

2. Про Стратегію національної безпеки України: Указу Президента України

від 12 лютого 2007 року № 105/2007 // Офіційний вісник України. – 2007. – № 11. – ст. 389.

3. Поляков С.Ю. Збройні Сили України у структурі Сектора безпеки і оборони / С.Ю. Поляков // Науковий вісник Інституту міжнародних відносин НАУ. – 2012. – № 1.

4. Закон України Про національну безпеку України. Сайт: Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/main/2469-19#Text (дата звернення: 15.03.23).

5. Конституція України. Сайт: Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення: 15.03.23).

6. Закон України Про оборону України. Сайт: Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/1932-12#Text (дата звернення: 15.03.23).

Кречетов М.Г.
Науковий співробітник науково-дослідного відділу
проблем інформаційної безпеки

ІНФОРМАЦІЙНА ВІЙНА КРАЇНИ-АГРЕСОРА: ВІД ТРАДИЦІЙНИХ МЕТОДІВ СПЕЦІАЛЬНОЇ ПРОПАГАНДИ ДО ПЕРЕБУДОВИ СТРУКТУРИ СПЕЦІАЛЬНИХ ЗАХОДІВ

На початку 2014 року наша держава зіштовхнулася з новими викликами і загрозами територіальній цілісності, суверенітету й демократичному ладу в країні. Анексія Кримського півострова в умовах відсутності збройного опору, військове вторгнення на Донбас й окупація в стислі строки значної території Донецької та Луганської областей, та з 2022 року широкомасштабна війна рф проти України, стали можливими завдяки багаторічним підготовчим діям росії з підриву авторитету та довіри місцевих мешканців до української влади і співгромадян з інших регіонів.

Довготривалі інформаційні кампанії, приховане втручання в економічні, енергетичні, гуманітарні сфери російської сторони сприяли створенню підґрунтя для реалізації більш потужних кроків і заходів агресивної політики росії у відносинах до незалежної України. На жаль, результативність російської інформаційної війни зумовлена неготовністю України до ведення протистояння в інформаційному просторі. Однією з причин швидкої окупації південно-східних територій стала дієвість пропагандистської машини рф з усіма її потужними інструментами, особливо в мережі Інтернет. Насичення ресурсів мережі Інтернет матеріалами з постійним насадження проросійських наративів, ускладнює процес

боротьби в інформаційному просторі.

Відповідно до положень Стратегії інформаційної безпеки України, затвердженої Указом Президента України від 28 грудня 2021 року № 685/2021 національними викликами та загрозами інформаційної безпеки є:

інформаційний вплив російської федерації як держави-агресора на населення України;

інформаційне домінування російської федерації як держави-агресора на тимчасово окупованих територіях України;

обмежені можливості реагувати на дезінформаційні кампанії;

несформованість системи стратегічних комунікацій;

недосконаліть регулювання відносин у сфері інформаційної діяльності та захисту професійної діяльності журналістів;

спроби маніпуляції свідомістю громадян України щодо європейської та євроатлантичної інтеграції України;

доступ до інформації на місцевому рівні;

недостатній рівень інформаційної культури та медіаграмотності в суспільстві для протидії маніпулятивним та інформаційним впливам.

Тривалий час спеціальні служби російської федерації проводять свої спеціальні інформаційні операції, більшість із яких спрямовані на підрив національної безпеки України, її національних інтересів, ліквідацію української державності та знищення української ідентичності, провокування проявів екстремізму, панічних настроїв у суспільстві, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації в Україні. Російською федерацією використовуються нові активні заходи, у тому числі міжнародного характеру, щодо легітимізації спроби анексії Автономної Республіки Крим та міста Севастополя, захоплення території інших областей України областей та посилення адвокаційної кампанії за зняття санкцій, запроваджених у зв'язку з порушенням російською федерацією суверенітету і територіальної цілісності України. Задіяння у цьому процесі російською федерацією всіх її спроможностей (політичних, інформаційних, економічних, розвідувальних та інших) залишається особливо небезпечним викликом для України.

У результаті тимчасової окупації у 2014 році та її розширення у 2022 році державою-агресором частини території України були захоплені розташовані на цій території об'єкти інформаційної інфраструктури, зокрема й об'єкти Концерну радіомовлення, радіозв'язку та телебачення.

Державою-агресором застосовуються методи тотального придушення свободи слова, контролю над редакційною політикою засобів масової інформації та інших інформаційних ресурсів, що функціонують на цих територіях.

На тимчасово окупованих територіях, у районах здійснення заходів із забезпечення національної безпеки і оборони, відсічі збройної агресії Російської федерації розгорнуто безпрецедентну інформаційну кампанію. Використовуючи

також регулярне постачання на тимчасово окуповані території потужного передавального обладнання та блокування українських інформаційних ресурсів, російська федерація намагається створити альтернативну викривлену інформаційну реальність, побудовану на наративах держави-агресора.

Придушення будь-яких спроб інакомислення посилюється регулярними репресіями стосовно незалежних журналістів, а також переслідуванням за перегляд українського контенту на тимчасово окупованій території.

Інформаційний тиск, що здійснюється державою-агресором, негативно відображається на дітях, які проживають на тимчасово окупованих територіях, адже через свій вік вони є особливо вразливими для впливу інформаційних кампаній.

Деструктивна пропаганда, поширення дезінформації як ззовні, так і всередині України застосовуються державою-агресором з метою підриву стійкості суспільства та інформаційної дестабілізації держави. Водночас ефективна система реагування на такі виклики в Україні досі не створена, не забезпечено функціонування розвиненої національної інформаційної інфраструктури, що обмежує можливість належним чином протидіяти інформаційній агресії з метою захисту національної безпеки та реалізації національних інтересів України.

Протягом року так званої “спеціальної військової операції (СВО)” на території України обома сторонами накопичено досвід використання різноманітних форм і методів інформаційного протиборства в реальних бойових умовах. Практика проведення рф “СВО” свідчить, що росія обмежено використовує інноваційні рішення та в більшості випадків повертається до традиційних методів спеціальної пропаганди.

Іншими словами, початок “СВО” призвів не до прогресу технологій інформаційної війни, а до їх регресу (1): класичні стратегічні інформаційні операції та оперативні ігри в інформаційному просторі з боку спецслужб та розвідок відійшли на другий план, поступившись місцем більш простим та масовим ідеологічним диверсіям, провокаціям, примітивним формам дезінформації та фейкам. Це пов’язано насамперед з браком часу для планування й реалізації оперативних комбінацій і відсутністю кадрів, здатних брати участь у таких оперативних іграх. Російська сторона, розпочавши “СВО”, розраховувала домогтися швидкого укладення мирного договору тільки з використанням військової сили. В рф робили ставку на раптовість та несподіваність нападу. В умовах швидкого просування вглиб території України силам інформаційних операцій росії потрібно було переважноно підтримувати бойовий дух своїх військовослужбовців, застосовуючи старі лозунги та патріотичну риторику, достатні для ідеологічної та інформаційної підтримки власного особового складу. Вважалося, що за таких умов для проведення справжніх інформаційних операцій (спеціальних розвідувальних операцій активного впливу в інформаційному просторі), підготовка до яких може потребуватиме від шести місяців до півтора

року, часу не залишиться.

Ситуація щодо “СВО” поступово змусила російське керівництво перебудовувати структуру спеціальних заходів та переформатувати її у чотири рівня (1) (згідно з російською класифікацією):

стратегічні інформаційні операції (притягнення до відповідальності військових злочинців);

спецпропаганда (деморалізація противника, дискредитація його лідерів, підрив політичної стабільності);

фейки (створення ажіотажу й паніки з метою відволікання сил та засобів противника на інші об’єкти);

оперативні ігри (наприклад, з певними елітами держави – об’єкта агресії).

Довідково:

Стратегічні інформаційні операції – оперативні комбінації, за допомогою яких можна досягти стратегічного ефекту в середньостроковій та довгостроковій перспективі. Мета таких операцій – висування звинувачень на адресу керівництва країни-противника у вчиненні військових чи інших злочинів (зазвичай, проти людяності, тероризмі, геноциді, застосуванні ЗМУ) та порушення кримінальних справ для розгляду в міжнародному трибуналі.

Спецпропаганда – заходи, спрямовані на деморалізацію противника, дискредитацію його лідерів, підрив політичної стабільності всередині воюючої держави. Ці заходи складають близько 80 % від усього обсягу розвідувально-диверсійної та підривної діяльності в інформаційному просторі в районі проведення “СВО” та за його межами. Єдина відмінність сучасної спецпропаганди від пропаганди радянських часів – канали зв’язку й доведення спрямованого впливу до цільової аудиторії, що дає змогу спецпропагандистам діяти точково, адресно, вибірково.

Фейки – специфічна форма дезінформації, яка масово застосовується для нагнітання страху, паніки, ажіотажу, поширення чуток, розпалювання ненависті і – вперше в ході “СВО” – для відволікання сил противника на інші об’єкти. У ході “СВО” виявилося ще одне призначення фейків – приховане (рефлексивне) управління противником, яке мотивує його на свідоме поширення фейків на власних каналах комунікації (у підконтрольних ЗМІ, у соціальних мережах, месенджерах). Використовуючи українські фейки російські пропагандисти мимоволі: створюють можливість тиражування та розповсюдження українських фейків шляхом їх відтворення на російському телебаченні та в електронних ЗМІ; створюють канали доведення дезінформації до широкої російської аудиторії (як результат – одіозний фейк, який побачила в мережі незначна кількість осіб, потрапляє на російське телебачення і стає доступним багатомільйонній російській аудиторії. При цьому це робиться без участі української сторони); створюють канал OSINT (отримання розвідувальної інформації з відкритих джерел шляхом зняття інформації від противника у вигляді відповідної реакції від т. зв.

прокремлівських спікерів, які входять в ідеологічний пул). Це повністю відповідає основному принципу спеціальних інформаційних розвідувальних операцій: противника необхідно простимулювати лише один раз, решту він має зробити власними руками.

Оперативні ігри – ігри, що проводяться з елітами (власниками великого бізнесу тощо), тобто з тими, чиї інтереси в основному за межами своєї країни і хто боїться втратити свої закордонні активи (2).

Література

1. Гузь Олександр. Особливості ведення інформаційної війни на території України в умовах проведення так званої спеціальної військової операції. Стратегічні комунікації у сфері забезпечення національної безпеки та оборони: проблеми, досвід, перспективи : ІІІ міжнар. наук.-практ. конф., 31 жовт. 2022 р.: тези доповідей / Міністерство оборони України, НУОУ імені Івана Черняховського. – К.: НУОУ, 2022. – 205 с.

2. Манойло А. Информационные диверсии в конфликте на Украине. URL: https://www.evestnik-mgou.ru/jour/article/view/1130/1129.

Кудінов В.А.
к.фіз.-мат.н., доцент
професор кафедри інформаційних технологій та кібербезпеки
Національної академії внутрішніх справ

ПРОБЛЕМИ КЛАСИФІКАЦІЇ РИЗИКІВ ІНФРАСТРУКТУРИ ІНФОРМАЦІЙНИХ СИСТЕМ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ МВС ТА НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

В Міністерстві внутрішніх справ (МВС) та Національній поліції України (НПУ) останніми роками здійснюється реформа їх інформаційних систем спеціального призначення (ССП). Так, зокрема, розроблені Положення щодо створення єдиної інформаційної системи МВС [1], інформаційно-комунікаційної системи «Інформаційний портал НПУ» [2]. Для ефективного функціонування цих та інших інформаційних ССП необхідно забезпечити створення належного рівня їх кіберзахищеності. Деякі шляхи його реалізації нами розглянуто у низці робіт [3-6]. Для подальшого удосконалення рівня кібербезпеки інформаційних систем спеціального призначення МВС та НПУ необхідно розглянути проблеми класифікації ризиків їх інфраструктури.

Методологія оцінки ризиків в інформаційних системах базується на дворівневому тлумаченні поняття ризику: коли передбачуваний ризик визначається ймовірністю виникнення небезпечної події (реальної загрози) та

рівнем серйозності його наслідків. Міра ризику – це своєрідна згортка двох змінних: «ймовірності реалізації загрози» та «вартості спричинених втрат».

Якщо загрози описуються кількісними змінними, то ризик виражається дійсним додатним числом відносною величиною в інтервалі [0;1] або грошовою сумою. Внаслідок того, що ні втрати, ні ймовірність здебільшого не можуть бути оцінені чисельно, значення ризику не може бути обчислене відповідно до визначення. Замість цього використовують методи оцінки ризиків, які ґрунтуються на якісних показниках [7].

Якісна шкала ризику встановлюється розбиттям області значень даного ризику на певні інтервали. Звичайно визначення ризиків у вигляді згортки якісних змінних здійснюється на основі спеціально розроблених двовимірних таблиць оцінки ризиків. Масштабування вихідних змінних і ризиків повинне здійснюватися на основі експертних оцінок. При цьому значення шкал повинні бути чітко визначеними та однаково розумітися всіма учасниками процедури експертної оцінки.

Найпростіші методи передбачають оцінювання рівня втрат та ймовірності реалізації ризику за якісною шкалою (малий / посередній / великий), а на їх основі – рівня ризику за табл. 1 [7].

Таблиця 1

Найпростіший метод оцінювання рівня ризику

Загальна серйозність ризику				
Втрати	ВИСОКІ	Посередня	Висока	Критична
	ПОСЕРЕДНІ	Низька	Посередня	Висока
	НИЗЬКІ	Відсутня	Низька	Посередня
		НИЗЬКА	ПОСЕРЕДНЯ	ВИСОКА
	Ймовірність			

Більш складні методи додатково враховують вплив взаємозв’язків інформаційних ресурсів, вже наявні заходи захисту, використовують певні бази вразливостей.

Результатом роботи усіх методів є відсортований за рейтингом перелік ризиків та, можливо, рекомендації з їх обробки.

Для оцінки ймовірності подій, які несуть загрози інфраструктурі інформаційних систем спеціального призначення Міністерства внутрішніх справ та Національної поліції України можна використовувати схему класифікації, яка приведена в табл. 2.

Тут ймовірність небезпечної події для кожного з п’яти класів описана як за

якісною, так і за кількісною шкалою.

Таблиця 2

Схема класифікації подій, що несуть загрози порушення інфраструктурі ССП, за ймовірністю настання подій

Ідентифікатор класу		***Клас подій за ймовірністю виникнення***	***Ймовірність***
	Дуже часта	Подія може відбутися один або кілька разів протягом терміну експлуатації ССП	$>10^{-4}$
	Часта	Подія може відбутися один раз протягом усього терміну експлуатації ССП	$10^{-5} \div 10^{-4}$
	Малоймовірна	Настання події малоймовірне протягом усього терміну експлуатації ССП, але подія може відбутися кілька разів, якщо розглядати сукупність систем того ж типу	$10^{-6} \div 10^{-5}$
	Вельми малоймовірна	Настання події малоймовірне, якщо розглядати декілька ССП того ж типу, але, разом з цим, виключати повністю таку можливість не можна	$10^{-8} \div 10^{-6}$
	Практично неможлива	Подія фактично не повинна відбутися за весь термін функціонування ССП	$<10^{-8}$

Для класифікації ризиків інфраструктури ССП пропонуються класи тяжкості наслідків подій, надані у табл. 3 [8].

Клас 1 (події найбільшої тяжкості): відсутнє незалежне джерело механізму відновлення, повна неспроможність забезпечити або підтримувати службу безпеки / захисту; повна втрата функціональних можливостей; майже постійне перебування у небезпеці.

Клас 2 (події великої тяжкості): серйозна неспроможність забезпечити або підтримувати службу безпеки / захисту; велике зменшення функціональних можливостей; небезпека продовжує існувати протягом доволі тривалого часу.

Клас 3 (події середньої тяжкості): часткова неспроможність забезпечити або підтримувати службу безпеки / захисту; значне зменшення функціональних можливостей; небезпека продовжує існувати протягом помірного періоду часу.

Клас 4 (події незначної тяжкості): зберігається здатність забезпечити або підтримувати службу безпеки / захисту; незначне зменшення функціональних можливостей; небезпека продовжує існувати протягом короткого періоду часу, такого, коли ще очікуються наслідки події.

Клас 5 (вплив події відсутній): відсутні умови виникнення небезпеки, тобто немає негайного прямого чи непрямого впливу на функціонування системи.

Таблиця 3

Класифікація тяжкості наслідків подій в інфраструктурі ССП

Рівень тяжкості / Аспекти наслідків		*1 Найбільша тяжкість*	*2 Велика тяжкість*	*3 Середня тяжкість*	*4 Незначна тяжкість*	*5 Вплив відсутній*
Вплив на систему		Катастрофічний вплив	Велике зменшення меж безпеки	Середнє зменшення меж безпеки	Незначне зменшення меж безпеки	Вплив відсутній
Вплив на ССП МВС, НПУ	*Зменшення спроможності виконувати зобов'язання*	Повна втрата спроможності	Серйозне погіршення спроможності	Значне погіршення спроможності	Незначне погіршення спроможності	Вплив відсутній
	Вплив на громадську репутацію	Постійна втрата довіри з боку громадськості	Часткова втрата довіри з боку громадськості	Завдано шкоди громадській репутації	Короткострокова шкода громадській репутації	Вплив відсутній
	Погіршення внутрішніх процесів	Цілковите порушення зв'язків	Значне погіршення	Середнє погіршення	Незначне погіршення	Вплив відсутній

Використання такої схеми класифікації ризиків і забезпечення участі у групових обговореннях експертів, що мають великий досвід діяльності у галузі інформаційної безпеки, дозволить своєчасно ухвалювати обґрунтовані та ефективні рішення у сфері кібербезпеки систем спеціального призначення Міністерства внутрішніх справ та Національної поліції України.

Література

1. Про затвердження Положення про єдину інформаційну систему Міністерства внутрішніх справ та переліку її пріоритетних інформаційних

ресурсів : Постанова Кабінету Міністрів України від 14 листоп. 2018 р. № 1024. URL: https://zakon.rada.gov.ua/laws/show/1024-2018-%D0%BF.

2. Про затвердження Положення про інформаційно-комунікаційну систему «Інформаційний портал Національної поліції України» : Наказ МВС України від 03 серп. 2017 р. № 676. URL: https://zakon.rada.gov.ua/laws/show/z1059-17#Text.

3. Кудінов В. А. Рекомендації щодо основних шляхів створення належного рівня захищеності єдиної інформаційної системи МВС України. *Кібербезпека в Україні: правові та організаційні питання*: матеріали міжнар. наук.-практ. конф. (Одеса, 22 листоп. 2019 р.). Одеса: Одеський держ. ун-т внутр. справ, 2019. С. 58–60.

4. Кудінов В. А. Проблема нормативно-правового визначення понять надійності, функціональної безпеки та живучості інформаційно-комунікаційних систем. *Протидія кіберзлочинності та торгівлі людьми*: матеріали міжнар. наук.-практ. конф. (Харків, 27 трав. 2020 р.). Харків: Харківський нац. ун-т внутр. справ. С. 151–153.

5. Кудінов В. А., Хорошко В. О. Математичне моделювання особливостей функціонування кіберзахищених інформаційних систем в залежності від кількості користувачів. *Інформатика та математичні методи в моделюванні.* 2021. Том 11, № 4. С. 374–387.

6. Khoroshko V. A., Kudinov V. A., Kapustian M. V. Evaluation of Quality Indicators of Functioning of Cyber Protection Management Systems of Information Systems. *Computer Systems and Information Technologies*. 2022. № 2. Pp. 47–56.

7. Ризик (інформаційна безпека). *Вікіпедія* : URL: https://uk.wikipedia.org/wiki/Ризик_(інформаційна_безпека).

8. Корченко А. Г., Архипов А. Е., Казмирчук С. В. Анализ и оценивание рисков информационной безопасности : монография. Київ, 2013. 275 с.

Литвиненко А.В.
науковий співробітник
Національного університету оборони України імені Івана Черняховського

ІНФОРМАЦІЙНА ДІЯЛЬНІСТЬ ПІД ЧАС ЗАХОДІВ ЦИВІЛЬНО-ВІЙСЬКОВОГО СПІВРОБІТНИЦТВА

Враховуючи зростаючу роль широкого спектру невоєнних чинників, які використовують протидіючі сторони в сучасних воєнних конфліктах (так звана “гібридна війна”), коли серед цілей та завдань держави-агресора, визначаються не фізичне знищення противника, а дестабілізація обстановки в країні, проти якої розпочато агресію, та нав’язування своєї ідеології населенню цієї країни, прийняття в 2014 році, рішення про створення у Збройних Силах України

структури цивільно-військового співробітництва, стало одним з адекватних кроків у відповідь на гібридні методи агресії російської федерації проти України.

В системі стратегічних комунікацій підрозділи цивільно-військового співробітництва на стратегічному, оперативному та тактичному рівнях значною мірою сприяють формуванню інформаційного середовища для розуміння, підтримки українським суспільством діяльності Збройних Сил України, створення сприятливих умов для виконання ними завдань за призначенням.

Зокрема, задля досягнення основної мети стратегічних комунікацій Збройних Сил України, відповідні підрозділи цивільно-військового співробітництва приймають участь у реалізації таких складових стратегічних комунікацій, як публічна дипломатія та зв'язки з громадськістю. Прикладами зазначеного, на стратегічному рівні, є:

за ініціативи Центрального управління цивільно-військового співробітництва Генерального штабу Збройних Сил України, з дозволу керівництва Міністерства оборони та Збройних Сил України, з початку квітня 2022 року, військовослужбовцями Центрального управління цивільно-військового співробітництва, у взаємодії з військовим телебаченням Міністерства оборони України та радником Міністра внутрішніх справ Антоном Геращенком, було організовано інформування українського суспільства та світової спільноти про дії Збройних Сил України щодо дотримання ними норм Міжнародного гуманітарного права в частині, що стосується збору та належного зберігання тіл загиблих окупантів, а також щодо ганебного відношення Російської Федерації до своїх загиблих військовослужбовців, які сотнями залишились на українській землі після відступу окупаційних військ на території Київської, Чернігівської та інших областей. До опрацювання відповідних матеріалів були залучені більше двох десятків інформаційних агенцій з усього світу. Станом на 8 червня 2022 року кількість переглядів окремих сюжетів в мережі Інтернет сягала: двох сюжетів вітчизняного військового телебачення – відповідно, майже 600 тис. та 1 млн. переглядів, "Al Jazeera" (Катар) – більше 400 тис. переглядів, "4 News" (Великобританія) – майже 1,5 млн. переглядів, "CNN" (США) – майже 3 млн. переглядів (1);

після оприлюдненої у соціальній мережі Facebook ветеранської ініціативи, відповідно до завдань, визначених Головнокомандувачем Збройних Сил України, Центральним управлінням цивільно-військового співробітництва Генерального штабу Збройних Сил України, з липня 2022 року, реалізується інформаційна кампанія "НА ЩИТІ", яка з перших днів отримала значну підтримку в українському суспільстві, зокрема у ветеранському середовищі. Серед основних завдань цієї інформаційної кампанії: героїзація та вшанування образу загиблих воїнів-оборонців України; зняття суспільної напруги довкола питання гибелі українських захисників; відхід від радянських військових традицій та запровадження нових традицій Збройних Сил України.

Таким чином, від початку російської агресії проти України в умовах повномасштабного військового вторгнення цивільно-військове співробітництво стало адекватною відповіддю на нові загрози. Насамперед це стосується взаємодії структур ЦВС ЗСУ із цивільним населенням та органами влади з проведення запобіжних заходів щодо недопущення перешкоджання діям військ. При цьому система цивільно-військового співробітництва функціонує у складі чотирьох основних взаємопов'язаних підсистем: цивільно-військової взаємодії, підтримки військ (сил), підтримки цивільного середовища, оцінювання цивільного середовища.

Також чинниками впливу на ситуацію щодо застосування військ (сил) є заходи цивільно-військової взаємодії, роботи з органами державної влади, міжнародними неурядовими організаціями та громадськими об'єднаннями, інформування населення, сприяння у наданні мешканцям гуманітарної допомоги, а також координації виконання робіт із відновлення інфраструктури й розмінування місцевості.

В урегулюванні криз беруть участь урядові установи. Це, насамперед, установи, до сфери повноважень яких відносяться питання тимчасово окупованих територій. Проте, наприклад, на тактичному рівні (незалежно від сценарію чи типу операції) група ЦВС бригади в основному взаємодіятиме з органами місцевого самоврядування до районного рівня (включно). При цьому потрібно брати до уваги практику представників цих структур в умовах кризової ситуації перекласти частину своїх проблем на війська.

Завдання органів державної влади в системі ЦВС формуються в процесі проведення відповідних організаційних заходів. Такі підходи дуже необхідні тому, що умови війни утворюють ситуацію «інформаційного вакууму». Люди не володіють значним обсягом інформації про події, які відбуваються в зоні бойових дій, та держави в цілому, про долю своїх близьких та рідних. Надається лише незначна частка інформації. Люди не бачать повної картини обставин, не розуміють, що буде далі, не можуть планувати свого життя. Їх життя змінюється на "пусте" існування з дня в день, без планів та перспектив, лише очікування. Життя наче зупиняється на цьому очікуванні й не йде далі. У найближчій перспективі підрозділи ЦВС спільно з міжнародними організаціями, які нарощують свою присутність в Україні, додадуть потужностей проектам з відновлення житлових приміщень та інфраструктури зруйнованих населених пунктів. Зокрема йдеться про забезпечення будівельними матеріалами для відновлення будинків та критичної інфраструктури, електрозабезпечення, водо- та газопостачання (2). Але, аналіз досвіду цивільно-військового співробітництва зі структурами ООН доводить, що вони розставляють інші акценти у своїй діяльності. Провідна роль належить саме інституціям цивільно-військового співробітництва, власне військовим інституціям відводиться вторинна роль. Такий підхід обґрунтовується тим, що останнім часом спостерігається стійка тенденція

збільшення кількості операцій соціально-гуманітарного характеру, а до виконання завдань цих операцій все більше залучаються військові ресурси (2). Таким чином можна зробити висновки, що впровадження цивільно-військового співробітництва сприяє значному підвищенню довіри цивільного населення до Збройних Сил України як інституту держави, дозволяє мінімізувати вплив наслідків бойових дій на цивільне населення, сприяє формуванню позитивної громадської думки щодо діяльності Збройних Сил України у районах дислокації та виконання завдань військових частин та підрозділів угруповань військ та розширило можливості щодо протидії негативному інформаційному впливу противника на населення держави.

Література

1. Актуальні питання цивільно-військового співробітництва в ході російсько-української війни (лютий-червень 2022 року). Збірник № 5 матеріалів вивчення бойового досвіду російсько-української війни 2022 року. ГУДП ГШ ЗС України. Київ, 2022. 189 с.
2. Калагін Ю. Феномен військово-цивільного співробітництва Збройних Сил України: концептуальні засади дослідження. Український соціологічний журнал. 2017. №1-2. С.64-68.

Мандрік О.Д.
Національна академія СБ України

СПЕЦІАЛЬНІ ІНФОРМАЦІЙНІ ОПЕРАЦІЇ ПРОТИ УКРАЇНИ В СУЧАСНИХ УМОВАХ

У міру розвитку країн їх зовнішньополітичні цілі неминуче перетинаються з цілями інших. Часом ці інтереси можуть призвести до напруженості, починаючи від економічного протекціонізму і закінчуючи територіальними суперечками, при цьому інформація відіграє вирішальну роль у формуванні думок. Розвиток глобальних інформаційних процесів і швидкий технологічний прогрес створили нові можливості для політиків використовувати цей простір, що призвело до дискусій і конференцій на тему інформаційної війни. Сьогодні зростає розуміння природи та цілей інформаційних війн, зокрема в контексті зовнішньополітичних дій, таких як агресія Російської Федерації проти України у 2022 році. Використання психологічних операцій і тактик дезінформації стало стандартною практикою для Кремля «гібридний» підхід до ведення війни на глобальній арені [1].

Сучасна ситуація в Україні є монументальним випробуванням державності країни. Ретельний аналіз положень сучасного міжнародного права малює похмуру

картину дій Російської Федерації щодо України без винятків. Крім того, Росія наполегливо використовує активні засоби психологічної маніпуляції та пропаганди для підриву стабільності України, намагаючись при цьому легітимізувати власну агресивну поведінку на світовій арені.

Аналізуючи інформаційні агентства Російської Федерації, видно, що вони численні і в основному діють на федеральному рівні. Багато з них були створені негласним указом президента Росії. На жаль, ці відомства часто поширюють неправдиві, брехливі та пропагандистські «новини» з антиукраїнським ухилом, іноді навіть спотворюють правду [2].

Протидіяти Україні російським інформаційним впливам можна на державному рівні, захищаючи інформаційний простір та забезпечуючи національну безпеку України [3]. Для цього необхідно: 1) забезпечити засоби масової інформації на інформаційну політику (як зовнішньої, так і внутрішньої) з доповненням законодавчої та нормативно-правової бази, яка відповідала б нормам міжнародного права; 2) здійснити захист національної інформаційної сфери; 3) просувати українську інформацію на територію агресора, використовуючи при цьому сучасні технології; 4) проводити люстрації серед власників українських медіа-ресурсів; 5) зменшити вплив олігархів на засоби масової інформації; 6) формувати та захищати сприятливий образ України за допомогою сучасних технологій; 7) створювати та підтримувати національний бренд, розвиток конкурентоспроможності на міжнародній арені; 8) проводити політику для збереження єдиної української політичної нації, на зближення політичних поглядів населення Сходу та Заходу України [4, с. 18-23]; 9) здійснювати обмеження російської інформації, що впливає на населення всієї України; 10) проводити постійний контроль іноземних засобів масової інформації; 11) сприяти розвитку вітчизняних інтернет ресурсів, що просувають іномовлення; 12) підвищувати якість та кількість українського продукту – до якої входять цікаві телепрограми, репортажі відомих людей, друкована продукція тощо; 13) здійснювати діяльність в інформаційному та віртуальному просторі у національних інтересах України, розповсюдження позитивної інформації про Україну; 14) брати участь у світових інформаційних процесах; 15) організовувати та проводити розвідувальну діяльність, пов’язану з проникненням в органи влади інших країн з метою просування наших національних інтересів; 16) введення контролю донесення правдивої інформації до споживача; 17) замінювати заклики «вироблено в Росії», «не купуй російське» тощо, доцільніше замінити на «купуй українське», адже воно рідне, якісне та перевірене; 18) блокувати інтернет-ресурси, які є загрозливими для інформаційної безпеки держави; 19) стимулювати наукові дослідження щодо державної інформаційної політики та безпеки; 20) вдосконалювати рівень підготовки фахівців у галузі інформаційної безпеки.

Аналіз інформаційної війни Росії проти України показав ефективність засобів масової інформації як інструменту для конструювання політичних планів і

налагодження важливих зв’язків із широкою громадськістю [5].

Література

1. Український медіаландшафт – 2015: аналітичний звіт / За ред. В. Іванова. Київ: ФКА, АУП, 2015. URL: https://www.aup.com.ua/upd/kas_43639-1522-13- 30.pdf (дата звернення: 23.03.2023).
2. Найбільш вражаючі приклади інформаційних війн 21 століття. URL: https://cutt.ly/LHwAatQ (дата звернення: 23.03.2023).
3. Христенко В. Є. Маніпулювання свідомістю в умовах гібридної війни: психологічний аспект. URL: http://repositsc.nuczu.edu.ua/bitstream/ 123456789/5929/1/ Khrystenko_monogr.pdf (дата звернення: 23.03.2023).
4. Сасин Г. В. Інформаційна війна: сутність, засоби реалізації, результати та можливості протидії (на прикладі російської експансії в український простір). Грані. 2015. № 3. С. 18-23. URL: http://nbuv.gov.ua/UJRN/Grani_2015_3_5. (дата звернення: 23.03.2023).
5. Максимович М. Медійні аспекти путінської" аудіовізуальної пропаганди. Теле- та радіожурналістика. 2015. Вип. 14. С. 195-202. URL: http://nbuv.gov.ua/UJRN/Tir_2015_14_28. (дата звернення: 23.03.2023).

Медведєв О.О.
Національний університет оборони України
імені Івана Черняховського
Сівоха І.М.
Національний університет оборони України
імені Івана Черняховського

ЗРИВ МОБІЛІЗАЦІЇ З МЕТОЮ ПІДРИВУ ОБОРОНОЗДАТНОСТІ ЯК НАРАТИВ РОСІЙСЬКИХ ТА ПСЕВДОУКРАЇНСЬКИХ ТЕЛЕГРАМ КАНАЛІВ

Кардинальні зміни, що відбуваються у сучасному інформаційному просторі, створили умови для їхнього використання в інтересах інформаційно-психологічного впливу, - зазначається в “Засадах реалізації стратегічних комунікацій у системі Міністерства оборони України”. Розгорнулася боротьба, що іноді за запеклістю протистояння не поступається класичній версії збройного протиборства. Така інформаційна війна, як відомо, передбачає “навмисне втручання у внутрішні справи країни з метою підриву довіри між державою та її громадянами; ...для просування інтересів іноземної держави через експлуатацію вразливостей у суспільстві з метою його поляризації та дестабілізації” [1].

“Тенденція використання соціальних мереж для здійснення інформаційного (психологічного) впливу на визначені цільові аудиторії на сьогодні стала

реальністю, а застосування соціальних мереж стало повсякденним процесом дестабілізації суспільно-політичної обстановки в країні-мішені" [2].

У 2022 році істотно прискорився процес змін в ієрархії каналів комунікації: відбулися подальше зниження частки телебачення як джерела новин, зростання ролі інтернету, соціальних мереж, особливо месенджерів, насамперед Telegram. Ще у липні 2022 року Київський міжнародний інститут соціології (КМІС) констатував, що телебачення остаточно поступилося інтернету першістю як найпопулярніше джерело отримання інформації. "Ми є свідками кардинальної трансформації медіаландшафту", – зазначають автори дослідження, – "де замість кількох потужних телевізійних каналів "виросли" сотні онлайн-джерел, кожне з яких не може похвалитися великою часткою "ринку" [3].

Якщо аналізувати сумарний час споживання новин у соціальних мережах, за даними КМІС, то 41% припадає на Telegram, 37% – на YouTube, у той час як Facebook, який після заборони в Україні "В Контакте" пережив пік популярності – 12%. На сьогодні Telegram став ключовою платформою для поширення російської пропаганди каналами, які формально позиціонують себе як українські, орієнтуються на українську аудиторію і подають українські новини в російській інтерпретації. У липні 2022 року СБУ, Міністерство оборони та інші українські відомства опублікували зведений список таких Telegram-каналів, підконтрольних Кремлю. Спецслужби встановили відповідний зв'язок у рамках відповідних кримінальних справ: "В умовах, коли Україна успішно протистоїть російському нападу, вкрай актуальним є питання інформаційної безпеки. Адже не маючи можливості перемогти на полі бою, ворог намагається посіяти „зраду" та розхитати українське суспільство".

Центр стратегічних комунікацій при Міністерстві культури та інформаційної політики з осені минулого року проводить глибинний моніторинг десятків прокремлівських каналів. При контент-аналізі цих досліджень, які лягли в основу даної роботи, чітко проглядаються і ключові теми, розраховані на підрив обороноздатності України, дискредитацію Збройних Сил України, зниження бойового духу наших військовослужбовців.

Особливості інформаційно-психологічного впливу на масову свідомість військовослужбовців добре відомі і досліджені. Серед них, як зазначає в своїй роботі Роман Саунін, "ініціювання сумнівів серед особового складу в доцільності ведення бойових дій; дезінформація військовослужбовців щодо реального стану справ на полі бою; створення паніки, масових психозів, настроїв поразки серед військовослужбовців; нагнітання страху бути вбитим або отримати тяжкі каліцтва" [4].

Протягом січня-березня однією з центральних тем російських телеграм-каналів стала тема начебто проблем з мобілізацією в Україні. Вона, очевидно, орієнтована як на цивільну аудиторію, так і на середовище військових. В цілому, абсолютно, очевидно, націлена на підрив обороноздатності України і

спроможностей ЗСУ. Фейками чи маніпуляціями ворог прагне генерувати недовіру українців до влади та знизити мотивацію долучення до армії. На загал – створити реальні проблеми для поповнення ЗСУ і таким чином - знизити обороноздатність країни. Російські пропагандисти відверто декларували у своїх каналах мету кампанії із дискредитації мобілізації: контрнаступ ЗСУ залежить від успіхів мобілізації. Зокрема, @legitimniy та @rezident_ua писали про те, що "Украине необходимо собрать десятки тысяч новых солдат и сформировать резервы в более чем 200 тысяч солдат".

Російські канали нагнітали загальну паніку про нібито насильницьку мобілізацію в лави ЗСУ. Наприклад, @Ze_Kartel опублікував цілу добірку епізодів, як військкомати вручають повістки у громадських місцях: від кафе до церков і бомбосховищ; на похороні у Львові та недільній службі у церкві; на гірськолижних курортах Карпат. Ці повідомлення - коктейль фейків, маніпуляцій і достовірної інформації, яка на задум розповсюджувачів має викликати довіру до усієї пропагандистської суміші.

В аналізованій кампанії ворог також наголошував на недотриманні принципу соціальної справедливості при мобілізації. Так, підозрюваний у державній зраді Шарій протиставляв простим чоловікам дітей та родичів можновладців, які виїхали за кордон Канал @legitimniy звинувачував працівників військкоматів у корупції та ухилянні від фронту: "Большинство этих ребят, которые раздают вам повестки, купили эти безопасные места, чтобы самим не ехать в бахмутовскую мясорубку или другие "проклятые места". Інші канали так само розігрували карту соціальної нерівності, поширюючи фейкове відео на кшталт "военкомы на шикарной машине угрожают охраннику жилого комплекса отправкой в армию за то, что он не открыл им шлагбаум".

Особливу увагу противник приділяє розпалюванню міжетнічної, міжрегіональної та мовної ворожнечі, протиставляли схід і захід України: мовляв, повістки роздають "особенно активно в восточной части страны, население русскоязычных ("пророссийских") регионов давно считают второсортным". Жителів сходу і півдня України у трактуванні російської пропаганди відправляють у найгарячіші точки, аби позбутися "проросійських російськомовних українців". Розігрувалася й угорська карта. Псевдо український канал @ZeRada1 розповідав про нібито масове вручення повісток у містах Берегове, Виноградів та селі Сюрте, де живе значна угорська діаспора і цитував угорську журналістку: Если так будет продолжаться, на Закарпатье не останется ни одного венгра".

Залякували тим, що мобілізованих направляють на фронт без підготовки "Вчера на Украине разразился скандал … свежемобилизованный гражданин из 57-й опбр уже через 2 дня после "добровольной мобилизации" оказался на фронте". @opersvodki публікував фото чоловіка без рук з погано перекладеним з російської підписом ("тварі вручили повестки"): "…на фронт попытались призвать украинца без рук. На очереди слепые и безногие".

Росіяни не обмежуються лише розповсюдженням дезінформації. Вони закликають українців до непокори та акцій протесту, рекламують українські онлайн сервіси, які інформують про місця видачі повісток чи юридичні послуги з уникнення мобілізації. У березні СБУ Кіберфахівці Служби безпеки України заблокували 26 Телеграм-каналів, які перешкоджали мобілізації українських громадян призовного віку. Інтернет-ресурси інформували про заходи, які проводять територіальні центри комплектування та соціальної підтримки з метою зниження їх ефективності. Насамперед вони, повідомляє УНІАН, надавали дані про актуальні місця вручення військовозобов'язаним повісток та закликали ховатися від представників військкоматів.

Такі захисні дії цілком виправдані, але протидія кампанії потребує зусиль із медіа-освіти українців, поширення правил елементарної медіа-гігієни. Одним із інструментів протидії є фахове використання прийомів і методів стратегічної комунікації: публічної дипломатії, зв'язків з громадськістю, військових зв'язків, інформаційних та психологічних операцій. Потрібні і новітні технологічні рішення. Так, фахівці Національного університету оборони України на чолі з Олександром Войтком та його співавтори запропонували метод прогнозування поширення інформаційних загроз у соціальних мережах, що містить у собі математичні моделі та методику їх застосування та розроблення програмних комплексів щодо обмеження доступності деструктивної інформації" [5].

Література

1. Зелена книга протидії дезінформації / Упоряд. і заг. ред. С. Балан. – ГО "Інститут інформаційної безпеки". – Київ, 2022. с.

2. Сідченко С., Залкін С., Хударковський К., Ревін О. Особливості підготовки і проведення інформаційної (психологічної) операції у соціальних мережах. Стратегічні комунікації у сфері забезпечення національної безпеки та оборони: проблеми, досвід, перспективи : тези доп. III Міжн. наук.-практ. конф. (м. Київ, 31 жовтня 2022р.). Київ : ННЦСК СЗНБО НУОУ, 2022. С. 48-51.

3. Київський міжнародний інститут соціології. Демократія, права і свободи громадян в умовах війни // 17.08.22 – Режим доступу ttps://www.kiis.com.ua/materials/pr/20220817.

4. Саунін Р. "Особливості інформаційно-психологічного впливу на масову свідомість військовослужбовців". Стратегічні пріоритети інформаційної безпеки держави у сфері оборони в умовах воєнного стану: тези доп. II міжв. наук.-практ. конф. (м. Київ, 29 листопада 2022р.) Київ. КЗІТтаІБ НУОУ, 2022, с. 121-124.

5. Войтко В., Солонніков В., Рахімов В. "Прогнозування розповсюдження деструктивного інформаційного впливу в соціальних мережах". Стратегічні комунікації у сфері забезпечення національної безпеки та оборони: проблеми, досвід, перспективи : тези доп. III Міжн. наук.-практ. конф. (м. Київ, 31 жовтня 2022р.). Київ : ННЦСК СЗНБО НУОУ, 2022. – 205 с.

Mikhieiev Y.I.
candidate of technical Sciences
Loboda V.V.
Korolyov Zhytomyr military institute

REQUIREMENTS TO AN AUTOMATED SYSTEM OF INFORMATION RETRIEVAL ON A SPECIFIC TOPIC ON THE INTERNET

The increase in volume of information on the Internet, which varies in type, form and content, makes the task of its thematic search more difficult. This issue becomes especially relevant when performing information warfare tasks.

Information retrieval systems are usually used in practice search for the necessary information about a particular object. The results of analysis existing information retrieval systems indicate that they are not able to fully provide with the consumer necessary information [1]. Therefore, the task is to develop a domestic automated information retrieval system (AIS) on a specific topic on the Internet.

During the creation of an AIS, it is necessary to develop algorithms and methods for rational search and further processing information on a particular topic. Such an AIS system should maintain an archive of queries, include a thesaurus, spell checking and parsing tools for language queries. A thesaurus can be used to increase the completeness of the search, in which case the words close to the query are added with words from the thesaurus. A future AIS should take into various Internet account services that attract attention of intelligence analysts, such as search engines, thematic resource directories, news sites, RSS messages and news agencies that broadcast news online. For this purpose, the first step in the creation of an AIS is to create a database of search resources available on the Internet, taking into account their specific features in providing information on a specific subject. Refinement a search is possible when using thematic classification of resources – vectors in the vocabulary space (indexing terms) system [2]. This task will be select the best possible features and formulate rules on the basis of which a decision will be made regarding the resource for a particular heading. Further work of AIS is related on processing material found. To resolve this task, a necessary stage in the creation of a future system is organising automatic abstracting of the information found.

For visualisation purposes of the found information with a view to its further analysis, it is advisable to use technology to build semantic networks. Comparing semantic networks in different texts allows to establish the degree at which they are semantically similar, which can be used for automatic classification of documents by specified headings, searching them by similarity with a given text, and dividing information set into classes containing similar documents. Model of promising AIS on a particular topic on the Internet may look like this (Fig. 1).

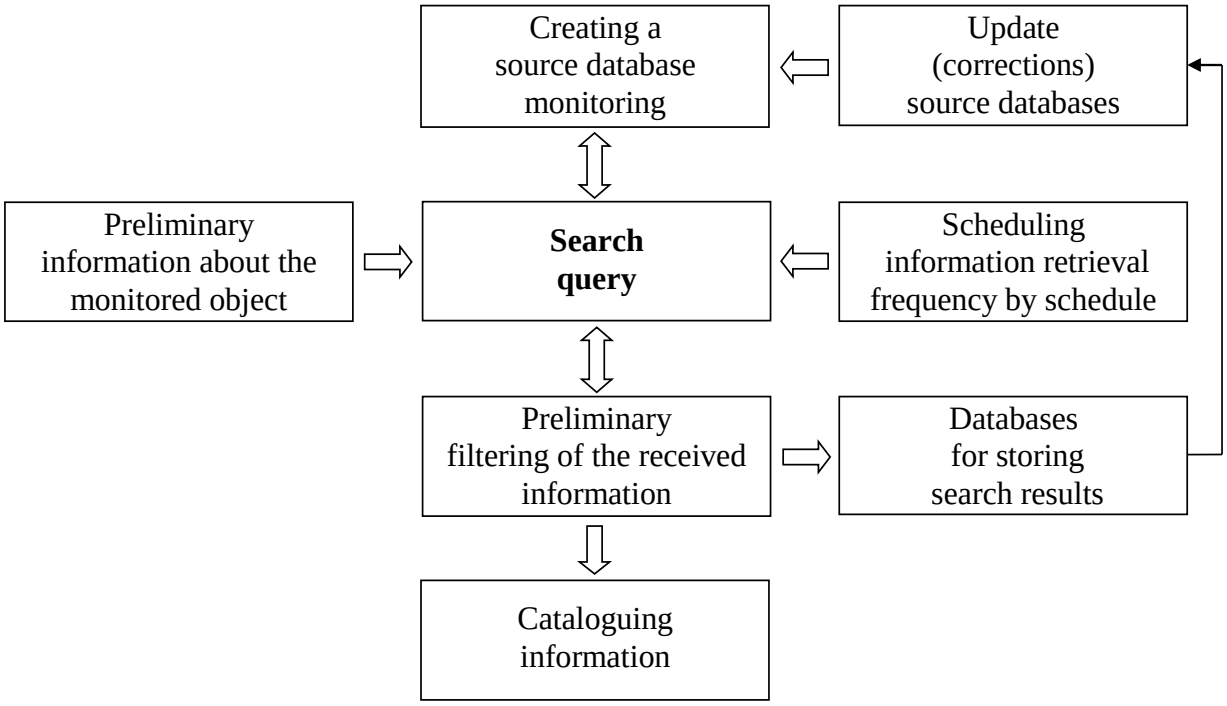


Figure 1 – Model of a prospective AIS on a specific topic on the Internet

It is expected that implementation of the proposed model AIS on a specific topic on the Internet into information and analytical activities of special units will provide: analyst operators with the means to quickly and efficiently search for heterogeneous information on the monitored objects; quick identification of implicit links between monitoring objects and related facts and events; capturing and visualising results of analytical research by generating digests articles, facts, formalised dossiers, semantic networks and other analytical reports.

Reference

1. Копина В.В., Шимчук Г.В. Пошукові системи та загальні принципи їх роботи// Зб.наук.пр. „Фундаментальні та прикладні проблеми сучасних технологій” до 100 річчя з дня заснування НАН України та на вшанування пам’яті Івана Пулюя (100 річчя з дня смерті). Тернопіль : 2018.С.203-204.

2. Сухий О. Л., Міленін В. М., Тарадайнік В. М. Алгоритми пошуку в інформаційних системах : методичні рекомендації. / Київ, 2015. 70 с.

Міхєєв Ю.І.
к.т.н.,
Павленко М.М.
Житомирський військовий інститут імені С. П. Корольова

СПОСІБ АВТОМАТИЗАЦІЇ РОЗПОВСЮДЖЕННЯ МАТЕРІАЛІВ ВПЛИВУ В СОЦІАЛЬНИХ МЕРЕЖАХ

Сьогодні країна-терорист продовжує чинити дії для досягнення переваги в інформаційній війні, використовуючи при цьому всі можливі інформаційні ресурси для розповсюдження матеріалів впливу на визначену цільову аудиторію. Результати моніторингу інформаційного простору свідчать про те, що розповсюдження матеріалів впливу переважно відбувається в соціальних мережах. Доцільність використання соціальних мереж для розповсюдження матеріалів впливу пояснюється тим, що в будь-який час, фактично в форматі онлайн можна приховано впливати на цільову аудиторію [1].

Досягнення бажаного психологічного ефекту від впливу передбачає вивчення потенційної цільової аудиторії, розроблення матеріалів впливу у вигляді спеціального контенту, відбір каналів розповсюдження та безпосереднє розповсюдження матеріалів впливу. Якість розповсюдження матеріалів впливу визначається ступенем охоплення ними цільової аудиторії. Значення ступеня охоплення цільової аудиторії матеріалами впливу в соціальних мережах залежить від:

кількості соціальних мереж у яких передбачається розповсюдження матеріалів впливу [2];

кількості груп в соціальних мережах, відібраних для розповсюдження матеріалів впливу;

інтенсивності розповсюдження матеріалів впливу у відповідних групах соціальних мереж.

Отже, для якісного виконання завдань з розповсюдження матеріалів впливу на визначену цільову аудиторію необхідне залучення відповідної кількості операторів. В умовах обмеженого людського ресурсу досягти бажаного ступеня охоплення цільової аудиторії матеріалами впливу в соціальних мережах можливо завдяки автоматизації процесу їх розповсюдження. Автоматизація процесу розповсюдження матеріалів впливу дозволяє перенести рутинні завдання щодо публікації матеріалів впливу в соціальних мережах та їх облік у сервіси або програмні додатки. У даному випадку як інструменти автоматизації можуть бути використані сучасні мови програмування, популярні бібліотеки (фреймворки), програмне забезпечення (конструктори) зі створення послідовності дій користувача (скрипту) в популярних веб-браузерах, таких як Google Chrome або Mozilla Firefox.

Скриптам, написаним у звичайний спосіб притаманний недолік використання незмінюваної послідовності дій під час реалізації певних алгоритмів. Наприклад, скрипту для розповсюдження матеріалів впливу на сторінці соціальної мережі необхідно виконати таку послідовність дій (натиснень на елементи сторінки за вказаними координатами): завантажити контент (розроблений матеріал впливу), обрати цільову аудиторію (окремі користувачі або групи користувачів), опублікувати матеріали впливу або виконати поширення (репост) опублікованих матеріалів [3]. Такий скрипт досить легко виявляється вбудованими аналізаторами дій, які використовують соціальні мережі для перевірки ботів. У подальшому акаунт з якого відбувається автоматизоване розповсюдження матеріалів впливу вважається фейковим та блокується. Тому більш доцільно використовувати розвинуті конструктори, які дозволяють до розробленого алгоритму додавати власні частини програмного коду, які більш точно реалізують імітацію дій користувача на сторінці соціальної мережі.

Для автоматизації розповсюдження матеріалів впливу в соціальних мережах пропонується використати конструктор BrowserAutomationStudio, який має широкий функціонал в базовому безкоштовному варіанті. Конструктор дозволяє у зручний спосіб створити модуль, що буде реалізовувати базовий функціонал взаємодії користувача з соціальною мережею через веб-браузер, а саме: завантаження початкової сторінки соціальної мережі, застосування профілю користувача веб-браузера, авторизація користувача в мережі.

У роботі запропоновано розширити базові можливості скрипту шляхом проведенням попереднього аналізу коду сторінки соціальної мережі для визначення структурних елементів: кнопок, списків. Для проведення аналізу елементів XML-документу було використано мову запитів XPath. В результаті аналізу було визначено необхідні для інтерактивної взаємодії елементи. Логіка роботи розширеного стрипту реалізована за допомогою конструкцій вибору IF-ELSE, циклів FOREACH, списків та регулярних виразів для аналізу строк, отриманих після попереднього аналізу. Для обходу алгоритмів виявлення ботів використано механізм випадкових часових затримок при вводі та імітації дій користувача в соціальних мережах за рахунок використання різних траєкторій переміщення курсору.

Для подальшого використання розробленого скрипту було використано можливості конструктора BrowserAutomationStudio, який дозволив створити програмний модуль автоматизованого розповсюдження матеріалів впливу в соціальній мережі “Фейсбук”. Розроблений програмний модуль дозволяє забезпечити необхідне значення ступеня охоплення цільової аудиторії матеріалами впливу в соціальних мережах за рахунок встановлення періодичності публікації у відповідних групах соціальних мереж та одночасного залучення максимально можливої кількості каналів розповсюдження.

Література

1. Євсеєв С. П., Кацалап В. О., Міхєєв Ю. І., Савчук В. С. та інш. Розробка методу визначення показників маніпуляції на основі морфологічного синтезу. Eastern-European Journal of Enterprise Technologies. Vol. 3, No. 9 (117), 2022. – pp. 22–35.

2. Найпопулярніші соціальні мережі у світі станом на січень 2022 URL: https://marketer.ua/ua/the-most-popular-social-networks-in-the-world-as-of-january-2022/.

3. Левченко О. В., Міхєєв Ю. І., Кравчук А.І ., Павленко М. М. Методичні рекомендації з розповсюдження інформаційних матеріалів у соціальній мережі "Фейсбук". – Житомир : ЖВІ, 2022. – 54 с.

Морозов О.М.
д.мед.н., професор,
почесний академік Національної
академії педагогічних наук України,
заслужений діяч науки і техніки України

З ІСТОРІЇ УСПІШНИХ МАСШТАБНИХ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ

Поняття «п'ята колона» вживається з часів першої половини XX сторіччя та носить виключно негативний зміст. Склалася традиція називати так великі групи людей схильних до зради інтересів власного народу та співпраці із ворожими силами. Воно вже давно перетворилося в негативний ярлик, якій навішують одне одному ворогуючи політичні, економічні, соціальні, етнічні угрупування, намагаючись дискредитувати одне одного. Це поняття широко застосовується в науковій і популярній літературі, перш за все під час дискусій щодо інформаційно-психологічної безпеки та боротьби в інформаційно-психологічному просторі (СІО, ІПСО). Спробуємо, спираючись на історичні факти, з'ясувати походження поняття «п'ята колона» та якій зміст насправді несе воно в собі – негативний чи позитивний.

У першій третині XX сторіччя імперська велич Іспанії, що у значній мірі забезпечувалася за рахунок заокеанських колоній, остаточно згасла. Не так давно одна з найбагатших і впливових країн Європи занурилася в бідність, а разом із бідністю в безліч соціальних проблем. Суспільство переживало етап «бродіння» думок і готовності до змін. Зрозуміло, що ослаблення країни з вигідним геостратегічним розташуванням і гарним кліматом викликало зацікавленість держав з імперськими амбіціями. Перш за все апетит запалав у вождів московської імперії, яка на той час називалася Союз Радянських Соціалістичних Республік.

Експансіоністські спрямування московії ніколи не були секретом для міжнародної спільноти. Маячня засновників комуністичної ідеї про світову революцію та світове панування комуністів співпало зі стародавнім прагненням московського улусу, нащадка Золотої орди, запанувати на євразійському просторі, у тому числі, шляхом контролю Гібралтарської протоки.

Враховуючи, що на початку тридцятих років XX сторіччя Іспанія була слабкою ланкою серед європейських країн, кремль розпочав несамовиту підготовку до її підкорення. Нестримний брехливий потік комуністичної пропаганди обрушився на голови населення Іспанії, збурював суспільство, роздмухував взаємну недовіру і ненависть, готував народ до війни. Пропаганда сполучалася зі стрімким зростанням воєнно-політичної присутності московії (СРСР) в Іспанії та просяканням іспанського суспільства представниками радянських спецслужб і партійних органів. Разом із завезенням, поки-що, легкої стрілецької зброї та радянських військових створювалися озброєні бойові групи з місцевих маргіналів. Усі заходи проводилися в умовах максимально можливої конспірації та абсолютного тупого заперечення всього, що ставало відомім світовій спільноті. На теренах Іспанії створився альянс, що складався з комуністичних пропагандистів, представників комуністичної партії Радянського Союзу, радянських спецслужб і збройних сил та місцевих прокомуністичних озброєних угрупувань. Усі представники московії мали підроблені документи громадян Іспанії, інколи – інших країн. Розпочалася прихована підготовка до створення маріонеткового прокомуністичного прокремлівського режиму в Іспанії.

У квітні 1931 року, ще до початку загарбницького процесу, в Іспанії пройшли муніципальні вибори, де впевнену перемогу отримали патріотичні сили. Дещо пізніше поволі почала набирати обертів комуністична пропаганда, а у 1935 році, вже набравши достатньої сили, відкрито активізувався так званий народний фронт тобто прокомуністичні сили. Така легалізація цього руху відбулася через те, що у Іспанії наближалися вибори кортесів, тобто членів іспанського парламенту. Паралельно активізувалися і пропаганда народного фронту і провокації радянських спецслужб, спрямовані на дискредитацію існуючої влади. Вбрані в форму представників різних державних установ та католицьких священиків співробітники радянських спецслужб здійснювали різні злочини, навіть отруєння дітей. Усе це дало результат. На неоднозначних виборах кортесів, що пройшли в лютому 1936 року, перемогли прокомуністичні сили. Після внутрішніх узгоджень позицій між ними в Іспанії склався так званий ліво-республіканський уряд, залежний від кремля.

Одразу після встановлення комуністичної промосковської влади в Іспанії почали відбуватися радикальні зміни, добре знайомі поневоленим москвою народам СРСР і далеко за його межами: всюди замайоріли червоні прапори, з’явилися портрети Енгельса, Маркса, Леніна та Сталіна, стрімко набирали обертів тоталітарний режим, залякування населення, репресії, затримання, ув’язнення та

зникнення людей, розстріли без слідства і суду, в тому числі масові, нестача продуктів харчування. З'явилися брехливі «полум'яні» пропагандистки, які оспівували режим і в середині країни і за її межами, виправдовували репресії інтересами трудового народу. За чотири місяці після зміни влади в країні склався пекельний червоний прокремлівський режим. Водночас у країні під проводом патріотичних сил почав формуватися народний опір червоному режиму. Тоді брехливі підступні інтернаціоналісти розгорнули фронт психологічної війни. З метою дискредитації називали патріотів на початку правими, далі – націоналістами, а пізніше – фашистами.

Кремлівські вожді розпочали відкриту окупацію Іспанії зрозумівши, що волелюбний іспанський народ не піде добровільно в московське рабство. На додаток до тих засобів війни і військових, які раніше були таємно завезені з московії до Іспанії, посунула армада танків, літаків, гармат, мінометів, різноманітної стрілецької зброї, тисячі військових, чекістів, інструкторів, радників і партійних чиновників. До радянських окупаційних сил, які почали стверджувати, що звільняють поневолених іспанців від фашистів, приєдналися так звані інтернаціональні бригади, тобто загони комуністичних бойовиків з 45 країн світу (фактичний початок Другої світової війни). Брали участь у війні і українці. На боці червоних окупантів воювала сформована радянськими військовими українська рота імені Т.Г. Шевченка, а на боці патріотів воював загін українських добровольців. Підтримала комуністичну навалу інфільтрована різноманітними лівацькими рухами Франція, а також і Мексика. Здавалося, що визвольний рух іспанського народу приречений на поразку. Однак не так сталося, як гадалося.

У літку 1936 року на батьківщину з Марокко повернувся Франсіску Франко – талановитий, енергійний, успішний, самий молодий у Європі генерал. Його поява організувала і пожвавила рух опору окупантам і зрадникам. Розгорнулася справжня війна за незалежність Іспанії, яка за загальноприйнятими термінами тривала з 17 липня 1936 року до 01 квітня 1939 року, тобто два роки та вісім з половиною місяців. За офіційними даними загинуло більше п'ятисот тисяч людей.

Що стосується інформації щодо цієї війни, то нічому без ретельної перевірки вірити не можна. Вся інформація, у формуванні якої брала участь московія, просякнута тотальною брехнею. У всі часи існування цієї імперії несамовита тотальна брехня є непохитним стилем її комунікації, СІО (ІПСО) не мають кінця. Джордж Орвелл добре знався на предметі своїх творів «1984» і «Скотний двір». Як свідок подій в Іспанії вивчив особливості радянського комунізму та його пропаганди, які і стали прототипами його книг.

Крок за кроком іспанці почали витискати з країни окупантів. 15 жовтня 1936 року розпочалася битва за звільнення окупованого Мадриду. Упевнений у швидкій перемозі командувач визвольних військ Еміліо Мола перед початком штурму сказав: «Сьомого листопада я вип'ю каву на Гран Віа. Чотири колони – зі мною, а п'ята – в Мадриді». Він мав на увазі, що під час розгортання операції

визволення столиці регулярні війська зайдуть в місто з чотирьох сторін чотирма колонами. Водночас, синхронно із наступом ззовні чотирьох колон, в середині міста виступлять загони патріотів-партизанів, яких Е. Мола назвав «п'ятою колоною». Тобто назвою «п'ята колона» було означено загони іспанських партизанів-патріотів.

Визволення Мадриду виявилося складним завданням. Е. Мола недооцінив сили окупантів. На той час Мадрид і увесь регіон був насичений окупаційними силами московії, інтернаціональними загонами та зрадниками Іспанії. Битва за Мадрид тривала аж до 28 березня 1939 року. Через три дні після визволення Мадрида війна в Іспанії скінчилася. Комуністи, в тому числі і «полум'яні», розбіглися по світах, залишивши після себе руїну та розбрат, який і досі дається взнаки. У Іспанії комуністичні пропагандисти досі мають багато прихильних вух.

01 квітня 1939 року закінчилася фізична війна, але пропагандистська війна кремля проти Іспанії тривала. Імперія брехні ніколи не мовчить. Ф. Франко вони назвали диктатором, його правління – тоталітарним, Іспанію – франкістскою, патріотів – фашистами, зрадників – героями, кровавих катів – людьми честі, окупантів – визволителями, окупацію Іспанії – свободою, визвольну війну іспанського народу – путчем, усіх, хто допомагав іспанцям – імперіалістами, «п'яту колону» партизанів-патріотів – зрадниками. Саме так створився та почав жити своїм життям брехливий негативний ярлик «п'ята колона». Його щодня тисячі разів бездумно повторюють пересічні люди, політики, аналітики, військові, журналісти в приватних розмовах, ток-шоу, виступах у ЗМІ та дискусіях.

Висновок. Сполучення несамовитої брехливої пропаганди (СІО, ІПСО) одних та відсутність здорового глузду інших призводить до неправильного розуміння правильних термінів, а за умови масованої підміни понять – до викривленого світогляду, помилкових висновків та дій (Б. Окуджава: «На дурака не нужен нож: / Ему с три короба наврешь / И делай с ним что хошь»). За подібним сценарієм діє московія сьогодні в Україні.

Ничитайло І.М.
к.ю.н., доцент, завідувач КІБД
Національної академії СБ України
Прокопчук Ю.Ю.
студент Національної академії СБ України

РОЗВІНЧУВАННЯ МІФУ, ЩО «АЗОВ» - НЕОНАЦИСТСЬКИЙ ПОЛК

Теза про те, що Азов - неонацисти, є однією з найбільш обговорюваних тем в українському та світовому просторі. Російський міф про Азов як неонацистську організацію базується на фальсифікаціях, маніпуляціях та спотворенні фактів, які

часто використовуються для політичних цілей.

Полк «Азов» є добровільним українським військовим формуванням, що бере участь у захисті територіальної цілісності України від російської агресії. Вони складаються з різних людей, які об'єднуються заради цієї спільної мети. Ідеологія Азова ґрунтується на принципах українського націоналізму та патріотизму, що орієнтована на захист інтересів України та її народу.

Потрібно розуміти, що те, що російські ЗМІ та політики називають "неонацистами", є лише частиною їхньої інформаційної війни проти України. Це зроблено з метою дискредитації української армії та держави в цілому.

Основні контраргументи щодо міфу про те, що полк «Азов» не є неонацистською організацією, ґрунтується на декількох ключових аспектах:

- по-перше, слід зазначити, що ідеологія полку «Азов» базується на принципах українського націоналізму, а не на неонацизмі. Український націоналізм - це ідеологія, яка прагне до захисту інтересів українського народу та його держави, але відрізняється від неонацизму своїми цінностями та принципами;
- по-друге, історія створення та розвитку полку «Азов» свідчить про те, що ця організація не має відношення до неонацизму: полк був створений в 2014 році відразу після російської агресії на сході України. Засновниками були українські волонтери, які приєдналися до нього з метою боротьби проти розпочатої ворогом агресії. З часом полк « Азов» став частиною Національної гвардії України, яка є офіційною військовою структурою держави;
- по-третє, ідеологія та практика полку «Азов» не містять у собі таких елементів, як расизм, антисемітизм, ксенофобія та інші прояви неонацизму. Більшість бійців цього полку - це прості українці, які захищають свою країну від ворога;
- по-четверте, не можна ігнорувати той факт, що полк "Азов" активно співпрацює зі спеціальними службами України та має значний внесок у боротьбі проти тероризму та організованої злочинності. Зокрема, полк "Азов" брав участь у важливих операціях зі звільнення заручників та злочинців, що свідчить про його професіоналізм та відданість;
- по-п’яте, полк «Азов» пройшов офіційну реєстрацію в українському Міністерстві юстиції. Це означає, що організація пройшла перевірку та відповідає вимогам українського законодавства. Звідси випливає, що українська влада визнала легітимність полку "Азов" та підтримує його діяльність.

Загалом, можна стверджувати, що полк «Азов» не є неонацистами, а характеризується українським націоналізмом та патріотизмом. Російський міф про «Азов» як неонацистську організацію базується на фальсифікаціях та перекрученні фактах, і не відображає реального стану речей. Важливо зрозуміти, що український націоналізм та патріотизм - це не є те саме, що неонацизм, і їх не слід ототожнювати. Український націоналізм є нормальною ідеологією для

держави, яка прагне до збереження своєї незалежності та відстоювання своїх інтересів.

Україна, як держава, знаходиться в складних умовах зовнішньої та внутрішньої політики, і полк «Азов» разом з іншими військовими формуваннями виконують важливу функцію в оборони країни. Важливо розуміти, що вони не є злочинними організаціями, а складаються з звичайних громадян, які віддають своє життя за свою країну.

Нарешті, варто зазначити, що незважаючи на те, що полк "Азов" може мати своїх критиків, він заслуговує на повагу за свою відданість Україні та її народу, адже його бійці відважно борються проти російської агресії та охороняють територію України від терористичних та злочинних елементів, прикладом чого є оборонна м. Маріуполь.

Отже, можна стверджувати, що російський міф про полк «Азов», як неонацистську організацію є неправдивим та має на меті лише дискредитувати Україну та її військові формування. Варто звернути увагу на реальний стан речей та наголосити на тому, що Азов є важливою складовою частиною національної оборони України, яка бореться за свою незалежність та територіальну цілісність.

У підсумку слід зазначити, що важливо розрізняти військові формування, які захищають свою країну, від неонацистських груп, які прагнуть до насильства та шовінізму.

Література

1. Про відзначення Дня партизанської слави : Розпорядж. Президента України від 18.06.2002 р. № 216/2002-рп. URL: https://zakon.rada.gov.ua/laws/show/216/2002-рп#Text (дата звернення: 03.03.2023).

2. Про План реалізації Стратегії кібербезпеки України : Рішення Ради нац. безпеки і оборони України від 30.12.2021 р. : станом на 3 лют. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/n0087525-21#Text (дата звернення: 06.03.2023).

Оніщук В.С.
Національний університет оборони України імені Івана Черняховського

ХАРАКТЕРИСТИКА ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ рф

Аналіз ведення інформаційних операцій рф [1] проти Естонії, Грузії та України дозволяє з упевненістю сказати, що росія використовує всі напрямки ведення інформаційної операції проти своїх противників, однак успішні дії їй вдаються не всюди. Там, де завданням є впровадження у свідомість особи чи групи людей певної ідеї, модифікації їх поведінки, результати, досягнуті російськими підрозділами інформаційної операції, не завжди прийнятні для них, а

іноді їх можна назвати провальними. Зокрема, загальні підсумки інформаційної війни навколо грузинсько-російського збройного конфлікту за більшістю складових є поразкою Росії. Це не означає, що в певних напрямках дії російських підрозділів інформаційних операцій не можна визнати винятково успішними. Насамперед, це технічні напрямки впливу, покликані зруйнувати або придушити ворожі засоби розповсюдження інформації. Однак там, де йдеться про модифікацію поведінки чи то естонців, чи грузин, чи навіть окремих державних діячів у цих країнах, російські зусилля зазнали фіаско. В Грузії дії росіян навпаки призвели до консолідації політиків навколо президента, усунення якого так прагнула Росія.

У Російській Федерації за інформаційну діяльність відповідає безпосередньо Адміністрація президента, на яку підпорядковуються підрозділи Федеральна служба безпеки та Медіа Холдінг, завданням яких є інформаційна діяльність на території колишніх республік Радянського Союзу, зокрема й України. Для впливу на соціальні мережі через Інтернет створено два інформаційних центри: Ольгіно та Сколково. Загальна мета зазначених інформаційних центрів полягає у створенні в Україні плацдарму для впливу на українську політику шляхом просування відповідних політиків.

Аналізуючи перелік засобів, використаних сторонами в інформаційній операції, можна зробити висновок про перевагу Росії в інформаційних засобах в українському інформаційному просторі. Таке співвідношення у силах і засобах дає гарантовану перемогу сильнішій стороні. Причиною того, що росіяни програли у 2014 році виборчу кампанію на посаду Президента України, та й не змогли досягнути моральної капітуляції українців у "газовій" війні, пояснюється дією в інформаційному протиборстві інших чинників. Інформаційна операція росіян в українському інформаційному полі не була пристосована до українського середовища. Тому ефективність використання російських інформаційних розробок була низькою, а дії українських інформаційних партизанів – зокрема в полі СМС, наліпок а також настінних гасел, – надзвичайно ефективною.

Слід зазначити, що вплив на широкі маси населення, про який йдеться у цій праці, не є єдиним завданням учасників інформаційної боротьби. В ході інформаційних операцій плануються і здійснюються операції проти окремих осіб і цілих відомств, зокрема Збройних Сил України. Як відомо, Росія теж працює в цьому напрямку: “Малоефективне використання федеральними силами методів спеціальних інформаційних операцій в Україні”, як результат, частковий виграш в інформаційному плані, змусили Росію врахувати негативний досвід, зробити якісні корективи в питаннях інформаційно-психологічної діяльності. Зараз вона координується на державному рівні помічником президента рф. У збройних силах ці функції покладено на першого заступника начальника Генерального штабу ЗС російської федерації.

Останнім часом стали актуальними операції, спрямовані проти осіб, що

ухвалюють рішення. На думку керівництва, роль політичного лідера, державного діяча вважається надзвичайно важливою, відтак потребує детального вивчення з метою впливу на його свідомість. Тому зараз у Росії на базі Інституту світової економіки і міжнародних відносин РАН відновлено діяльність центру створення психологічних портретів політичних лідерів. Для цього аналізується інформація за такими напрямами: концепція лідерства, мотиваційна сфера, система політичних переконань, стиль ухвалення політичних рішень, стиль міжособистісних стосунків, стійкість об'єкту вивчення до стресу. Відповідно до цього відпрацьовується алгоритм прийняття та реалізації рішення щодо конкретної особи.

Не викликає сумнівів, що в сьогоднішньому конфлікті з Україною російські підрозділи інформаційних операцій намагатимуться створити в Україні вигідне для себе бачення, наприклад, світової громадської думки, для зміни громадської думки в потрібному для себе напрямку та впливу на рішення українських політиків. Частину цієї роботи виконують бездумні редактори і журналісти, які просто й безкритично копіюють сервіс російських інформагентств.

Сьогодні об'єктом інформаційної атаки з боку Росії є Східні регіони України. Росія, творчо осмисливши перебіг подій в Косові та Абхазії й Осетії, намагається побудувати схему інформаційної операції за зразками подій, які відбувалися. В усіх згаданих випадках процес відторгнення території починався зі скасування автономії. Проблема сьогоднішніх подій на Сході України в тому, що росіяни мають схему розвитку подій, знають, які чинники в яких вузлах цієї схеми дають потрібний їм результат, і коригують свої дії відповідно до обставин, а українська сторона навіть не аналізує того, що відбувається. Хоч варто було б провести свій порівняльний аналіз розвитку подій у згаданих регіонах та в Криму і зробити власні висновки щодо українського способу вирішення згаданих проблем.

Отже, наведена характеристика інформаційних операцій рф дозволяє дійти висновку такому, що інформаційний простір постійно змінюється і це дозволяє противника створювати нові інформаційні загрози для всіх країн світу.

Література

1. Дузь-Крятченко О. П. Проблеми забезпечення воєнної безпеки України і деякі шляхи їх розв'язання. Державне реагування на загрози національним інтересам: матеріали круглого столу / О. П. Дузь-Крятченко, В. О. Косевцов. – К. : НАДУ, 2014. – С. 34–41.

2. Телелим В. М. Планування сил для виконання бойових завдань у "гібридній війні" / В. М. Телелим, Д. П. Музиченко, Ю. В. Пунда // Наука і оборона. – 2014. – № 3. – С. 30–35.

Орищук І.О.
Безай І.В.
Житомирський військовий інститут імені С.П.Корольова

СПОСІБ ПРОТИДІЇ ПРОПАГАНДІ росії ЧЕРЕЗ ЗАСОБИ РАДІОМОВЛЕННЯ

Найбільш розповсюдженим, доступним та впливовим на цільову аудиторію засобом інформаційного і психологічного впливу (ПсВ) який здійснюється противником на даний час залишається радіомовлення. Це підтверджує аналіз дій російських структур ПсО з початку агресії в Україні у 2014 році по теперішній час. Так, першочерговими заходами російських окупаційних військ були заходи щодо отримання контролю в інформаційному просторі у районах дестабілізації обстановки і безпосередньо на окупованих територіях, а саме захоплення або знищення передаючих радіотелевізійних центрів (веж).

З початком повномасштабного вторгнення та при окупації територій України Росія продовжує здійснювати повну ізоляцію захоплених територій від інформаційного простору України та заповнення інформаційного вакууму власним контентом а саме:

блокування українського телебачення та налаштування захопленої апаратури ТРЦ та веж на трансляцію російських каналів телебачення;

при неможливості використання зазначеної апаратури (виведенні з ладу, зруйновані) трансляція каналів російського телебачення на екранах пересувних комплексів у місцях масового збору населення (торгівельні центри, місця видачі гуманітарної допомоги тощо);

блокування станцій українського радіомовлення та налаштування захопленої апаратури ТРЦ та веж на трансляцію проросійських радіостанцій та трансляція власного контенту;

використання персоналу (обслуговуючого ТРЦ, журналістів, кореспондентів, ведучих програм) з числа колаборантів для формування власного контенту, його трансляції через місцеві канали та надання до центральних російських агентств;

блокування українських операторів мобільного зв’язку, переналаштування захопленої апаратури та впровадження російських операторів з заміною телефонних номерів користувачів;

ліквідація українських та впровадження підконтрольних провайдерів з надання послуг щодо кабельного телебачення та доступу до мережі інтернет з блокуванням ресурсів з українським доменним ім’ям;

застосування мобільних засобів звукомовлення, радіомовлення та пересувних телевізійних комплексів (мобільні екрани для трансляції телебачення);

знищення зразків української преси та впровадження проросійських періодичних видань тощо.

Нажаль, з початком агресії та по теперішній час ряд технічних та організаційних причин не дозволяють своєчасно та повністю відновити присутність українських інформаційних джерел в інформаційному просторі прифронтових та захоплених ворогом територій, що значно знижує ефективність заходів з інформаційних в цих регіонах. Це дозволяє ворогу знизити морально-психологічний стан населення, втратити надію на звільнення їх територій від ворога, зламати волю до спротиву.

Особливо активно окупаційні війська здійснюють вплив на населення України та особовий склад збройних формувань сектору безпеки та оборони України поблизу лінії зіткнення шляхом трансляції передач власних FM-радіостанцій. Використання активних засобів (РЕБ) для придушення радіостанцій ворога неможливо у зв'язку з можливим вогневим ураженням та недоцільно так як потребує їх цілодобового або тривалого використання їх протягом доби. Одним з шляхів протидії такій пропаганді може бути застосування невеликих мобільних комплексів радіомовлення, мовлення яких здійснювати на частотах радіостанцій противника.

В доповіді розглядається досвід експлуатації зразка комплексу радіомовлення та пропозиції щодо його застосування. Невисока потужність таких трансляторів обмежує можливості щодо придушення ворожих станцій на велику відстань але може забезпечити впевнений прийом сигналу власної радіостанції в районі її розташування (селище, місто), унеможливити прийом сигналів ворожої радіостанції на обраній частоті. Невелика вартість обладнання, можливість автономного функціонування без постійної присутності обслуговуючого персоналу (ретрансляції програм радіостанцій України) зменшує ризики їх використання і може суттєво знизити вплив російської пропаганди на населення України та особовий склад збройних формувань сектору безпеки та оборони України у прифронтовій зоні.

Паливода В.О.
головний консультант відділу нових викликів
центру зовнішньополітичних досліджень
Національного інституту стратегічних досліджень

РОСІЙСЬКА ДЕЗІНФОРМАЦІЯ ПРОТИ УКРАЇНИ ТА ПОЛЬЩІ

Україна та Польща належать до країн, які особливо вразливі до дезінформаційної діяльності Кремля. У такий спосіб Росія намагається дискредитувати обидві країни на міжнародній арені та послабити українсько-польські відносини. Російські пропагандисти використовують різні методи та прийоми введення в оману. Російська дезінформація охоплює багато тем і часто

базується на емоціях. Це – загроза як для України, так і для Польщі.

Дезінформація роками використовувалася рф як зовнішньополітичний інструмент для досягнення політичних цілей, посилення впливу та послаблення противників. Її коріння сягають пропаганди Радянського Союзу, хоча нинішня дезінформаційна діяльність здійснюється іншим шляхом, і завдяки використанню Інтернету та соціальних мереж вона може бути набагато ефективнішою. За останні роки російська дезінформаційна діяльність еволюціонувала від 4D-стратегій (Dismiss, Distort, Distract, Dismay) до тактик, заснованих на нових технологіях [1].

Зараз російська пропаганда значною мірою базується на використанні соціальних мереж і фейкових акаунтів. Також важливу роль відіграють тролі та боти, які поширюють в Інтернеті маніпулятивні повідомлення. У рф є навіть спеціальні так звані фабрики тролів, де працюють люди, метою яких є публікація певного вмісту в мережі. Найбільша така фабрика працює в Санкт-Петербурзі [2]. Крім того, Росія вкладає значні кошти в діяльність порталу «Sputnik», багатомовного телебачення «Russia Today» та російського агентства преси ТАСС. Неправдива інформація також поширюється на різних менших новинних порталах. Часто та сама інформація з'являється на багатьох порталах, щоб підвищити її довіру та охоплення. Ці портали працюють у різних країнах, і контент публікується там місцевими мовами. Після початку війни в Україні діяльність такого типу проросійських порталів в європейських країнах була обмежена, а деякі з них заблоковані. Неправдиву інформацію поширюють і російські політики у своїх ЗМІ.

Цілі російської дезінформації відрізняються залежно від держави та інституцій, проти яких вона спрямована. Однак є загальні цілі, такі як відновлення домінування Росії в пострадянській сфері впливу, знищення впливу західних демократичних цінностей, інститутів і систем з метою створення поліцентричної моделі світу, посилення політичного, економічного і військового впливу Москви в усьому світі. Важливість дезінформації у зовнішній політиці Росії підкреслив, зокрема, теоретик інформаційної війни, професор Дипломатичної академії МЗС рф Ігор Панарін, який заявив, що успіх геополітичних планів давно асоціюється з перемогою в інформаційній війні [3].

Російська дезінформація націлена на різні групи та має різні цілі для кожної з них. З точки зору дезінформації проти України та Польщі, найважливішими цільовими групами є російське суспільство, українське суспільство, польське суспільство та західне суспільство.

Російські пропагандисти використовують різні методи введення в оману. Основний – це багатовекторні наративи на окремі теми, які регулярно повторюються [4]. Важливою особливістю російської дезінформації є безперервність дії, тобто певний дезінформаційний наратив регулярно передається в різних формах, щоб він запам'ятався реципієнту. Короткі повідомлення часто містять емоційно насичену інформацію, зазвичай без згадки джерела. Мета цих

повідомлень – викликати певну реакцію та спотворити сприйняття подій у адресатів. Інший спосіб – неправдиві або маніпулятивні назви статей, які не відповідають тексту. Цей метод передбачає, що більшість одержувачів не прочитають його повністю, а отримають інформацію лише з помітного, оманливого заголовка. Хорошим полем для маніпуляцій за допомогою цього методу є соціальні мережі, де користувачі через надлишок інформації не встигають прочитати статтю цілком і часто звертають увагу лише на назву поширеного тексту. Інший метод полягає у тому, щоб використовувати старі твердження як нову інформацію, і таким чином цитувати слова в невідповідному контексті у пропагандистських цілях. Подібним способом є цитування фальшивих цитат, тобто приписування комусь слів, яких він ніколи не говорив. Ще один спосіб, який використовує Росія, є поширення теорій змови. Характерним прийомом маніпуляції є приховування невигідних Москві фактів. Після початку війни в Україні у лютому 2022 року Росія приховувала від громадськості, що в рамках «спеціальної військової операції» також були атаковані цивільні об'єкти. На пізніх етапах війни усі невдачі російської армії на полі бою намагалися приховати. Яскравим прикладом використання цього методу в минулому було багаторічне заперечення СРСР розстрілу польських офіцерів у Катині. Інший спосіб – публікація фейкових інтерв'ю з вигаданими людьми. Потім розмова поширюється у письмовій формі, а цю «особу» представляють як експерта або жителя області, що надає цінну інформацію. Насправді ж цих людей не існує.

Література

1. A. Pellegatta, Disinformation from Russia: Kremlin info-ops in Europe. Italian Institute for International Political Studies, 01.07.2020. URL: https://www.ispionline.it/en/pubblicazione/disinformation-russia-kremlin-info-ops-europe-26796 (дата звернення 24.03.2023).

2. X. Kurowska, A. Reshetnikov. Russia's trolling complex at home and abroad. Paris: European Union Institute for Security Studies, 2018, p. 27.

3. O. Wasiuta, S. Wasiuta, Kremlowska dezinformacja w Internecie i reakcja społeczeństw zachodnich. Kraków: Przegląd Geopolityczny, 2020, nr 34. URL: cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-fa9f1fc7-ca37-4e98-b76f-d7d08d86d7cb/c/XXXIV-07-Wasiuta2.pdf (дата звернення 24.03.2023).

4. Wojna informacyjna w Internecie. Przeciwdziałanie prokremlowskiej dezinformacji w państwach Europy Środkowej i Wschodniej. Centrum Stosunków Międzynarodowych, 2017. URL: http://old.csm.org.pl/pl/raporty?download=855: raport-csm-wojna-informacyjna-w-internecie (дата звернення 24.03.2023).

Паливода О.О.
к.психол.н.
Національна академія СБУ

ПРОАКТИВНІСТЬ ЯК ОСНОВНИЙ ПРИНЦИП ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ПРОТИБОРСТВА

Особливості функціонування інформаційного простору в умовах повномасштабного збройного протистояння, коли всі прорахунки в комунікації з населенням активно використовуються ворогом, коли «психологічна зброя» (насамперед, пропаганда, дезінформація, фейки, маніпуляції) стає невід'ємною складовою агресії в арсеналі противника, доповнюють вже звичні для сучасної людини значні обсяги циркулюючої інформації, наявний інформаційний шум (надлишок «зайвої» інформації, серед якої цілеспрямовано чи стихійно «губиться» актуальне повідомлення), а також неможливість задовольнити потребу більшості реципієнтів в оперативному отриманні достовірних повідомлень, у тому числі й вітального характеру.

Усе це не тільки ускладнює функціонування окремих безпекових структур, діяльність яких безпосередньо пов'язана із захистом інформаційної сфери держави, їх контактування із стейкхолдерами, але й впливає на психологічне благополуччя їх представників, які самі стають об'єктами деструктивного психологічного впливу. Отже, виникають додаткові «людські втрати» (організаційні, фізичні, моральні тощо) через зниження продуктивності виконання поставлених завдань, відволікання на усунення напружень, непорозумінь та панічних реакцій на окремі інформаційні вкиди.

Зазначене вимагає сутнісної трансформації організації інформаційно-психологічного протиборства в аспекті запровадження системного підходу щодо мінімізації можливостей противника вчиняти інформаційно-психологічні впливи на окремі цільові аудиторії та населення України в цілому. І ці перетворення мають посилювати наші спроможності діяти на упередження, не дозволяючи ворогові отримати перевагу навіть на незначний час.

Йдеться про проактивність як визначний принцип організації інформаційно-психологічного протистояння. Спробуємо сформулювати основні тези щодо наповнення цього принципу в аспекті боротьби за «розум і серця» нашого народу. Зрозуміло, що проактивність (дія на упередження) базується передусім на прогнозованості дій супротивника і сформованості власної потенціалу та спроможностей, що дозволяє вирішувати поточні завдання із мінімальною ймовірністю настання ускладнень й негативних наслідків. Відтак, проактивність має включати:

- аналіз пропагандистських наративів противника – підхід «йти від наративів, а не від джерела» дозволяє більш ефективно моніторити інформаційний простір і

вчасно знаходити всі можливі канали поширення деструктивних ворожих впливів);

- аналіз активностей ворога в інформаційно-психологічному протистоянні – основні цільові аудиторії, цілі / мішені, канали поширення «психологічної зброї»), що, передусім, дозволяє краще розуміти наші уразливості;

- визначення трендів у просуванні ворогом інформації – для цього необхідно вивчити та «зрозуміти» основні постулати його пропагандистської концепції, прагнення та плани у конфлікті, як вони «вписуються» у базові наративи та порівняти отримане бачення із способами та каналами поширення інформації. Можливість виокремлення таких трендів обумовлюється суто психологічними закономірностями функціонування психіки людини і соціальних спільнот, а важливість їх формулювання – у тому, що завдяки ним з'являється час на продумане активне протистояння, а також можливість в подальшому перевіряти наші припущення щодо наступних кроків супротивника;

- інформування – будь-яка потреба в інформації (особливо, якщо вона стосується життєво важливих аспектів існування) задовольняється людиною у вигляді споживання повідомлень різного ступеня достовірності – тобто якщо немає можливості отримати її з достовірних джерел, людина буде послуговуватись чутками, «сумнівними новинами», «експертними думками». При цьому, в ситуації війни «порожнє місце» завжди буде використане ворогом задля просування вигідних йому ідей. Тож, максимальна доступність інформації – це більше про убезпечення та захист, про формування системи поглядів, які виступатимуть фільтром для сприйняття подальших меседжів;

- формування резилієнтності співробітників як внутрішньої здатності протистояти негативним інформаційно-психологічним впливам – резилієнс значною мірою залежить від досвіду, отримання певних знань, умінь та навичок, і тоді можна говорити про медіаграмотність як базову компетентність сучасної людини. Але психологічна стійкість – це й особисті характеристики, як-то: стресостійкість, мотивація, Я-концепція, копінг-стратегії, цінності, й наявність ресурсне середовище, насамперед, підтримка в підрозділі, довіра до побратимів і керівництва тощо.

Безмовно, запропоновані складові принципу проактивності інформаційно-психологічного протиборства не є вичерпними, проте вони визначають пріоритетні вектори протидії деструктивним ворожим інформаційно-психологічним впливам. Варто також зазначити, що лише комплексна реалізація всіх цих заходів робить таке протистояння дієвим.

Таким чином, інформаційно-психологічні впливи противника як один із інструментів сучасного збройного протистояння рф використовують, насамперед, вразливості українського суспільства й спрямовуються на створення недовіри як між громадянами, так і між громадянами і державою. А відтак реалізація інформаційно-психологічного протиборства має орієнтуватися передусім на

результат, абстрагуючись від інституційного середовища та дійових осіб, і передбачати обрання оптимального набору інструментів в боротьбі за «розум і серця» людей. Саме системна різновекторна діяльність, зорієнтована на запобігання можливим впливам та формування базової психологічної стійкості усіх верств населення до «бомбардування шкідливою інформацією», є більш дієвою у порівнянні із алгоритмізованим протистоянням із ворогом за традиційною схемою «виявлення-нейтралізація».

Перегуда С.П.
Національний університет оборони України імені Івана Черняховського

АНАЛІЗ ЕЛЕМЕНТІВ СИСТЕМИ ПРОТИДІЇ ПСИХОЛОГІЧНОМУ ВПЛИВУ ПРОТИВНИКА НА СИЛИ ОБОРОНИ УКРАЇНИ

Аналіз джерел показав [1-3], що зміст психологічного впливу полягає в досягненні успіху в збройній боротьбі не через інформаційне домінування в кількості залучених медіа ресурсу, а завдяки їх перевазі в інформаційних можливостях та організаційній побудові за мережевою структурою. Суцільна інформатизація та інтелектуалізація систем управління військами і зброєю якісно змінили зміст операцій. Вони дістали назву “медійних” або спеціальних операцій, що проводяться складом “мережевих ботів”, які навмисно заманюють “соціальних зівак”, та керуються з єдиного стратегічного центру й одночасно діють як окремі ключові елементи системи стратегічних комунікацій державного й військового рівнів.

Метою тез доповіді є аналіз елементів системи протидії психологічному впливу противника на Сили оборони України.

Під випереджувальними інформаційними заходами будемо розуміти цілеспрямовану дію однієї сторони (джерело впливу) на іншу (об’єкт впливу) за допомогою певної інформації (інформаційного процесу) для досягнення бажаного результату [3]. Головною метою здійснення випереджувальних інформаційних заходів на об’єкти інформаційної інфраструктури є досягнення переваги в інформаційному протиборстві, дестабілізація або виведення із ладу системи державного (у тому числі військового) управління, деморалізація населення, особового складу Сил оборони, керівництва держави та осіб, що приймають рішення на всіх рівнях державної влади та місцевого самоврядування за рахунок проведення “медійних” операцій.

Особливістю “медійних” операцій є застосування побудованих на нових принципах методів розвідки, управління й забезпечення, які дають можливість застосовувати сили й засоби не в одній лінії, а відразу на всій сферах національної безпеки відповідно до своїх спроможностей. Спільне застосування контенту на всі

можливі цільові аудиторії підвищує результативність стратегічних комунікацій [2].

Протистояння меседжів (провокація) – це зіткнення як достовірних тематик повідомлень, так і упередженої інформації, яка класифікує події та не визнає норми і правил змістовного наповнення. Упереджені та неупереджені меседжі можуть бути симетричними й асиметричними. Асиметричні меседжі розповсюджуються інсайдерськими повідомленнями за участю суб'єктів, що якісно відрізняються стосовно інформаційного потенціалу й принципів організації та управління.

Навіть без переходу до інформаційної операції асиметричні меседжі мають ряд специфічних ознак, які є наслідком обмеженого арсеналу засобів для слабших за можливостями учасників. В асиметричних відносинах сильний партнер зазвичай не потребує застосування додаткових інформаційних заходів для нав'язування власної поведінки. Тому зміст інформації часто відображається в латентному вигляді, лише епізодично переходячи в інтенсивну фазу у формі жорстоких і на перший погляд ірраціональних закликів, зокрема "зрада", "все втрачено". Такі дії є тим засобом з обмеженого арсеналу, за допомогою якого асиметричні меседжі мають сильніший психологічний вплив (і потенційно перемагають) над симетричними меседжами [3].

Виходячи із зазначеного виникає протиріччя з одного боку є комунікативні системи в сферах національної безпеки з іншого такі ж системи в силах безпеки. Тому виникає необхідність розмежування функцій між цими системами з виявлення психологічного впливу на цільові аудиторії.

Під час хаотичного використання інформаційного простору важко визначити противника, тим паче важко вести мову про правові, етичні та моральні норми поведінки. Без них організоване насильство веде до деградації локальних спільнот, їх варваризації.

М. Требін одним з перших українських дослідників визначає використання комунікативних можливостей з впливу на конкретні цільові аудиторії, як певну форму гібридної війни [6]. Використання такої форми дозволяє державам зняти з себе відповідальність за військове втручання, порушення норм міжнародного права і підтримку нерегулярних військових формувань. В схожих термінологічних рамках дане явище аналізують експерти українського Центру суспільних відносин, коли визначають, це як сукупність підготовлених і оперативно реалізованих державою дій військового, дипломатичного, інформаційного, економічного характеру, спрямованих на досягнення стратегічних цілей. Тому, все частіше досягнення перемоги відбувається не на полі бою, а в когнітивному та економічному просторі.

Використання переваг когнітивного інформаційного простору в системі стратегічних комунікацій дозволяє державам уникати відповідальності за розв'язання збройного конфлікту, військові злочини, порушення міжнародного

права або знаходити інформаційні приводи для виправдання власної агресії.

Важливою частиною такої форми політичного насилля є використання цивільної інфраструктури та інформаційних каналів комунікації для маніпулювання суспільною думкою і забезпечення підтримки місцевого населення. Фактично, це реалізується у формі психологічного впливу, який включає отримання розвідувальної інформації, психологічний тиск і дезінформацію, кібератаки, руйнування інформаційної інфраструктури противника. Саме тому, український політолог Є. Магда висловив думку, що в умовах сучасного інформаційного суспільства головним засобом ефективної реалізації гібридної війни є контроль над інформаційним простором. Як ми можемо побачити, комунікативна гібридна війна характеризується органічним поєднанням методів прямої і непрямої агресії, із залученням нерегулярних військових формувань, невдоволеного цивільного населення та інфраструктури.

Для оцінювання рівня деструктивного інформаційного впливу на об'єкти інформаційної інфраструктури необхідно мати певну систему показників, а для визначення його критичного (допустимого) значення – відповідні критерії.

У [3] стверджується, що формалізація та оцінювання інформаційного впливу за допомогою точних математичних моделей і методів суттєво обмежені через:

різнорідність, розподіленість, багатозв'язність і динамічність джерел і об'єктів інформаційних загроз, що його породжують;

надто велику кількість параметрів, що відображають суспільні інформаційні відносини і характеризують відповідні інформаційні загрози;

відсутність необхідних статистичних даних внаслідок неповноти, неоперативності і недостовірності практично доступної інформації.

Виходячи із наведених аргументів, одним із підходів до отримання оцінок інформаційного впливу може бути застосування методів експертного оцінювання на основі використання досвіду фахівців інформаційної сфери [2] за показниками, які характеризують такий вплив на об'єкти інформаційної інфраструктури. Саме професійний досвід та інтелектуальні можливості фахівців інформаційної сфери дають можливість відносно адекватно "вимірювати" інформаційні процеси, які проявляються безпосередньо в певному інформаційному просторі. Це може стати основою становлення вищезазначеної системи моніторингу загроз.

Комунікативна гібридна війна завжди є брудною за своїм змістом, бо, вона характеризується такими методами, як: підкуп, залякування, злочинність, викрадення людей, мародерство, насилля проти цивільних, захоплення державних установ, організація і проведення терористичних актів (підтвердженням цього стали численні теракти в Одесі та Харкові) [3].

Викладені основні підходи до формування комунікативних основ системи стратегічних комунікацій Сил оборони дозволять:

забезпечити єдність, збалансованість та координованість інформаційних заходів щодо створення, розвитку та захисту єдиного інформаційного простору

Міністерства оборони України та Збройних Сил України;

підтримувати достатній рівень інформаційної безпеки Міністерства оборони України та Збройних Сил України і створити належні умови для реалізації функцій управління усіма суб'єктами Сектору безпеки і оборони держави з метою вирішення завдань військового будівництва у мирний час, а також досягнення інформаційної переваги над противником та здійснення управління ним силовими і несиловими методами на свою користь у ході можливого воєнного конфлікту.

Отже, наведений аналіз елементів системи протидії психологічному впливу противника на Сили оборони України дозволить сформувати можливі сценарії розвитку інформаційних загроз та започаткувати нові показники для їх оцінювання.

Література

1. ВСТ 01.004.004 – 2014 (01). Інформаційна безпека держави у воєнній сфері. Терміни та визначення;

2. Bonk K., Griggs H., Tynes E. Strategic communications for nonprofits – CCMC, 1999. – 214 с.;

3. US. Governmental information operations and strategic communications: a discredited tool or user failure. Implications future conflict / Steve Tatham, 2013. – 98 с.

Петренко С.В.
науковий співробітник НЛ 4,
НОЦ Національної академії СБ України
Дубінець Д.І.
студент Національної академії СБ України

ДОСТУП ДО ПУБЛІЧНОЇ ІНФОРМАЦІЇ В УМОВАХ ВОЄННОГО СТАНУ

Повномасштабна війна кардинально змінила наше життя в усіх його сферах. У зв'язку з військовою агресією рф Президентом України було підписано Указ № 64/2022 про введення в Україні воєнного стану з 05 години 30 хвилин 24 лютого 2022 року. Частина друга статті 64 Конституції України передбачає, що в умовах воєнного стану можуть бути обмежені деякі конституційні права і свободи громадян, зокрема право на вільне збирання, зберігання, використання і поширення інформації в будь-який спосіб [1]. Право на доступ до інформації в умовах воєнного стану може підлягати обмеженням, насамперед для захисту інтересів національної безпеки та територіальної цілісності держави. Однак право громадян на звернення до суб'єктів владних повноважень з метою отримання публічної інформації у жодному разі не може бути обмеженим навіть в умовах воєнного стану.

Отримання громадянами публічної інформації здійснюється різними способами. Наприклад, шляхом оприлюднення інформації в масмедіа, створення різноманітних публікацій на офіційних вебсторінках державних органів влади, наповнення єдиного державного вебпорталу відкритих даних тощо. Проте, найпоширенішим інструментом доступу до публічної інформації залишається звернення особи із запитом до розпорядника інформації. Не можна не зазначити, що публічна інформація - це відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, що була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, або яка знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації [4]. Розпорядники інформації наділені повноваженнями відмовляти в наданні інформації, якщо такі відомості мають обмежений доступ та в сукупності відповідають кільком вимогам. По-перше, обмеження доступу до інформації здійснюється в інтересах національної безпеки, територіальної цілісності або громадського порядку, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету й неупередженості правосуддя. По-друге, розголошення інформації може заподіяти істотної шкоди цим інтересам. По-третє, шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні. Доречно підмітити, що обмеженню доступу підлягає саме інформація, а не документ. У випадку, якщо документ містить інформацію з обмеженим доступом, для ознайомлення надається інформація, доступ до якої необмежений.

Можна зробити висновок, що попри правовий режим воєнного стану, фізичні, юридичні особи та об'єднання громадян без статусу юридичної особи не позбавлені права на доступ до публічної інформації. Обмеження доступу до такої інформації можливе виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку із чітким обгрунтуванням відповідно до вимог, які законодавець прописав у статті 6 Закону «Про доступ до публічної інформації». Строки розгляду запитів залишилися без змін.

Література

1. Конституція України: Закон України від 28.06.1996р. № 254к/96-ВР. URL:https://zakon.rada.gov.ua/laws/show/254 (дата звернення 4.03.2023).

2. Кримінальний кодекс України : Закон України від 05.04.2001 р. № 2341-III. URL:https://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення 4.03.2023).

3. Про правовий режим воєнного стану: Закон України від 12 травня 2015 р. № 389-VIII. URL: https://zakon.rada.gov.ua/laws/show/389-19#Text (дата звернення 4.03.2023).

4. Про доступ до публічної інформації: Закон України від 13 січня 2011 р. № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення

4.03.2023).

5. Про національну безпеку України: Закон України від 21 червня 2018 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення 4.03.2023).

Погорілий М.І.
студент НА СБ України
Стрельбицька Л.М.
д.ю.н., проф., заслужений працівник освіти України

СПЕЦІАЛЬНИЙ ПСИХОЛОГІЧНИЙ ВПЛИВ ІНФОРМАЦІЙНИХ РЕСУРСІВ рф НА ГРОМАДЯН УКРАЇНИ – ЯК ЗАГРОЗА НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ

Протягом більш ніж тридцяти років існування відновленої незалежності української держави, паралельно зі становленням сектору безпеки та стрімким розвитком технологій у зв'язку з науково-технічним прогресом, активно нарощувалася політична, інформаційна, кібернетична, та пряма воєнна інтервенція терористичної держави російської федерації (далі за тестом – рф) проти України.

Одним з головних елементів вищевказаної конфронтації було і залишається інформаційне протиборство у засобах масової інформації (далі за текстом – ЗМІ) та кібернетичному просторі в цілому.

Отже ще до початку прямої воєнної агресії, рф вела проти України інформаційну війну, впроваджуючи засоби пропаганди через підконтрольні ЗМІ, політичні сили та навіть релігійні організації (у т.ч. нетрадиційні), з метою впливу на думки, психологічний стан, погляди та поведінку жертви. Такий вплив було направлено як на суб'єкти владних повноважень, так і на населення України – цивільних, військових, виборців та спостерігачів.

Службами спеціального призначення рф широко застосовується так звана інформаційна зброя, шляхом донесення інформації (дезінформації) у такий спосіб, щоб викликати переосмислення жертвою політичної та воєнної обстановки, що в результаті повинно спричинити втрату мотивів протистояння ворогові.

Застосовується інформаційна зброя спецслужбами рф не тільки у ЗМІ (в загальноприйнятому розумінні), але й в соціальних мережах. У дослідженні проблематики теми виділяється російський веб-сайт chatroulette.com. Цей сервіс передбачає спілкування з випадково вибраними користувачами у відео-форматі в режимі Online. Використання даного веб-сайту заборонено на території України Указами Президента України від 15 травня 2017 року №133/2017 [1] та від 14 травня 2020 року №184/2020 [2]. Однак з початком повномасштабної війни, розв'язаної рф проти України, кількість українських користувачів chatroulette.com

зросла, люди намагалися вплинути на російське суспільство з метою повалення пануючого в рф владного режиму та подальшого припинення російської воєнної агресії.

Відомо, що веб-сайт chatroulette.com та його користувачі відповідно контролюються федеральною службою безпеки рф (далі за текстом – фсб рф). Так, фсб рф використовує даний веб-сайт як платформу для здійснення спеціальних інформаційних операцій (далі за текстом – СІО) проти громадян та, зокрема, представників підрозділів Сил безпеки і оборони України.

Спеціальна інформаційна операція – це інтегроване застосування ключових можливостей електромагнітних засобів, комп'ютерних мереж, психологічних операцій, військового мистецтва та безпекових операцій разом із спеціальною підтримкою та відповідними можливостями з метою впливу, руйнування, завдання шкоди, захоплення процесу ухвалення рішень (людиною чи технічними засобами) [3].

Таким чином на різноманітних інформаційних ресурсах та в соціальних мережах зокрема працюють спеціально підготовлені групи фахівців фсб рф, які комунікуючи з громадянами України впроваджують СІО.

Комунікація таких спеціалістів російських спецслужб з українцями призводить не лише до негативного впливу на емоційно-психологічний стан та базові погляди останніх, але й до збору їх персональних даних та з'ясування місць дислокації частин та підрозділів Сил безпеки і оборони України. Особливо небезпечною є така комунікація з українськими військовослужбовцями. Так, у разі підключення до російського веб-сайту через незахищену мережу, ворог може отримати IP-адресу користувача та відслідкувати його місцезнаходження. Також, шляхом застосування методики OSINT розвідки, за зображенням обличчя співрозмовника, встановлюється детальна інформація про особу, що посилює психологічний вплив в результаті її використання під час діалогу.

OSINT – термін, який розшифровується як open-source intelligence, – це одна з форм процесу організації та управління збором розвідувальних даних (Intelligence Collection Management), що включає їх пошук і відбір із публічних загальнодоступних джерел, добування та аналіз інформації, формування розвідувального документу для прийняття відповідного рішення [4].

Найбільшою загрозою національній безпеці України є випадки підключення до подібних сервісів військовослужбовців Сил безпеки і оборони України, в момент перебування на бойових позиціях.

Таким чином ворогом збирається таємна інформація про місця розташування частин та підрозділів Сил безпеки і оборони України, з метою подальшого ураження наших позицій.

Отже, особливої уваги з боку суспільства та правоохоронних органів, заслуговує застосування українцями російських інформаційних каналів та, зокрема, соціальних мереж, що має не лише деструктивний вплив на їх емоційно-

психологічний стан, але й прямо загрожує національній безпеці України, через можливе «злиття» (свідоме/несвідоме повідомлення) ворогові надважливої таємної інформації.

Література

1. Указ Президента України №133/2017 «Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)».

2. Указ Президента України №184/2020 «Про рішення Ради національної безпеки і оборони України від 14 травня 2020 року «Про застосування, скасування і внесення змін до персональних спеціальних економічних та інших обмежувальних заходів (санкцій)».

3. Joint publication: 3-13. Information operation, 2006 [Електронний ресурс]. – Режим доступу : http://www.acqnotes.com/Attachments/Joint%20Publication%203-13%20Information%20Operations%2013%20Feb%2006.pdf.

4. Ланде Д. В. Правові питання конкурентної розвідки // Інформація і право. 2020. № 2(33) [Електронний ресурс]. – Режим доступу : http://ippi.org.ua/lande-dv-pravovi-pitannya-konkurentnoirozvidki-st-51-68 (дата звернення: 21.05.2022).

5. Указ Президента України №56/2022 «Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки».

6. Указ Президента України №447/2021 «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України».

Полевий В.І.
к.ю.н., с.н.с
Онофрійчук О.Ю.
Національний університет оборони України

АКТУАЛЬНІСТЬ РОЗМЕЖУВАННЯ ФОРМУВАННЯ КОМУНКАЦІЙНОЇ ПОЛІТИКИ ВІД ЇЇ РЕАЛІЗАЦІЇ В УМОВАХ ВІЙНИ

Комунікація є ресурсом влади і складовою самою сутності влади як можливості здійснювати вплив. Вона формує зв’язки між суб‘єктами і поєднує мету, силу та інших людей, які необхідні для реалізації задуму суб’єкта влади. Іншим подібним елементом є, наприклад, сила.

Стратегічні комунікації «прив‘язані» безпосередньо до суб‘єкта влади і здійснюються в його інтересах. Комунікації також є необхідною функцією влади:

вони забезпечують реалізацію державних політик. Виконавці політик мають мати спільне бачення мети і цілей цих політик, тобто володіти відповідним наративом; громадськість, в інтересах якої здійснюється влада, має розуміти що і з якою метою робить влада. Якщо стратком не працює – зв‘язок влади і суспільства втрачається і у демократичному суспільстві, яким є Україна, така влада не отримає підтримки на виборах.

Оскільки стратком є функцією, яку реалізовують органи і структури в інтересах держави (влади) – то центром тяжіння цієї функції є структура, найближча до центру влади. Це важливо, наприклад, для координації та розмежування комунікацій між міністерством оборони і Генштабом ЗСУ, або СБУ та Офісом Президента.

Влада делегується, в тому числі для виконання функцій, наприклад, оборони чи контррозвідки. Тому комунікація - це і елемент і інструмент політики держави (її керівників) в цілому, так і окремих політик держави (оборони чи контррозвідки як складової оборони). Повторюся, що на стратегічному рівні державного управління говоримо про стратегічні комунікації.

Я сфокусую вашу увагу на оперативному та, частково, тактичному рівні комунікацій органів влади. Щоб реалізовувати ВЛАДУ у сфері оборони та національної безпеки потрібно зберегти комунікацію, як елемент цієї влади.

Сьогодні офіс Президента України формує політичний порядок денний, а отже визначає наративи стратегічної комунікації. Далі має включатися принцип розмежування функції визначення, встановлення політик від їх реалізацій. Політичне рішення прийняте:

1) Україна звільняє усі окуповані території;

2) Україна звільняється від усіх корупційних та агентурних зв’язків з агресором.

Далі, на рівні державних структур – ЦОВВ має здійснюватися реалізація цього стратегічного наративу через призму функцій, які виконує даний орган. Міністерство оборони реалізує цю політику шляхом збройної відсічі агресії, ЗСУ виконує свою роботу як інструмент цієї політики. СБУ ловить ворожих агентів і протидіє усім корозійним та корупційним економічним впливам росії.

Важливо, що ані СБУ, ані ЗСУ не визначають свій власний наратив, оскільки вони не є політичними, виборними органами влади держави. Вони розвивають власні піднаративи в межах, які визначені їх функціями. У стратегічних комунікаціях існує і не повинна порушуватися жорстка вертикаль влади. Прийняття політичних рішень і відповідальність за них – це робота політиків. Президент України, який є гарантом державного суверенітету, територіальної цілісності України (див. ст. 102 Конституції України) та «забезпечує державну незалежність, національну безпеку» (п.1 ст.106 Конституції України), його апарат визначає засади, на яких буде досягнутий мир. Саме цей виборний державний орган несе відповідальність за те, щоб через підзвітні і підконтрольні йому

міністерства закордонних справ, економіки, оборони тощо створити умови для озброєння, постачання армії, нашої міжнародної підтримки, ізоляції агресора. ЗСУ є ключовим, але не єдиним інструментом створення умов для настання миру. Це є частиною цивільного контролю над сектором безпеки і має бути відображено в комунікаціях.

Чому я так багато увагу приділяю питанням розмежування політичної влади та її реалізації? Тому що сили оборони (ЗСУ і СБУ, в тому числі) функціонально наділені величезним обсягом іншої складової влади: силою. В умовах війни сила цих владним інструментів непомірно зростає. Історія знає чимало прикладів, коли ця сила потім і проголошувала себе владою. Ставала авторитарною, тобто не обраною демократично. Ворог чітко усвідомлює цю притаманну демократіям слабину і намагається експлуатувати наративи, які вбивають клин між владою та силами оборони. Наприклад, що влада позбавляє Головнокомандувача, Голову СБУ (потрібне - підкреслити), повноважень, не визнає заслуг, ревнує доуспіху тощо.

Щоб перемогти, Україна має пам‘ятати хто наш ворог і який головний наратив цієї боротьби: свобода і демократія бореться з авторитаризмом та безправ‘ям.

Присяжнюк М.М.
к.т.н., с.н.с.,
доцент кафедри СКПЛ ЦСК ННІ ІБ СК НА СБ України,
Сергієнко О.П.
аспірант НА СБ України

ІНФОРМАЦІЙНА ВІЙНА ПРОТИ УКРАЇНИ ЯК СКЛАДОВА ГІБРИДНОЇ АГРЕСІЇ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ

Сучасний розвиток подій в інформаційному просторі України як навколо операції Об’єднаних сил так і держави в цілому свідчить, що інформаційна складова набуває дедалі більшої значущості і стає одним із найважливіших елементів забезпечення національної безпеки. Інформаційний простір через інформаційні ресурси та супутні технології великою мірою впливають на рівень і темпи соціально-економічного, наукового та культурного розвитку [1].

Інформаційні війни – це один з основних інструментів досягнення домінування в тому чи іншому регіоні та є основою для ведення гібридної війни. Інформаційна кампанія (війна) проти України, яку розгорнула рф, є багаторівневою та довготривалою агресією, що посилюється від початку АТО, згодом ООС, до повномасштабного вторгнення на територію України.

Під час підготовки до воєнної агресії проти України сили інформаційної

боротьби рф особливу увагу приділяють саме організації ведення деструктивного маніпулятивного інформаційно-психологічного впливу (ІПсВ), спрямованого на формування викривлених уявлень про події в Україні. У цей час в активний ужиток як представників українських засобів масової інформацій, так і державного апарату силових структур сектора безпеки та оборони України увійшли такі поняття як інформаційна війна, інформаційне протиборство, спеціальні інформаційні та інформаційно-психологічні операції, що спрямовуються рф проти України в рамках гібридної війни.

Вплив інформаційно-психологічного контенту в гібридній війні рф проти України направлений на такі основні цільові аудиторії: населення рф; населення та правлячу еліту країн, що підтримують рф; населення та керівництво інших країн світу; населення тимчасово окупованих територій України; населення та керівництво України, особовий склад її Збройних Сил та інших військових формувань.

В основі інформаційної війни лежить намагання рф змінити поведінку цільових аудиторій на бажану для агресора, здійснення ІПсВ, спрямованого на ураження свідомості населення, руйнування способів і форм ідентифікації особистості, що веде до зміни форм самовизначення, деперсоналізації, знищення людської здатності до вільної ідентифікації, знищення системи переконань в рамках культурно-історичних традицій.

Сучасні технології дають можливість перенести традиційні воєнні дії з безпосереднього місця бою в глобальний комунікаційний простір, що не має жодних кордонів та інформаційних обмежень, а інструментом ведення інформаційної війни є медіа ресурси та соціальні мережі. Контент медіа ресурсів та соціальних мереж, їх аудіовізуальна інформація – найбільш приваблива і така, що легко сприймається широким колом інтернет-користувачів, а відсутність цензури та неконтрольований потік деструктивної інформації сприяють досягненню цілей країни агресора у гібридній війні проти України.

Висновок. У рамках інформаційної війни, що є невід’ємною складовою гібридної агресії, рф докладає чималих зусиль для підриву та спотворення міжнародного позитивного іміджу України, посилення ІПсВ на її громадян, особовий склад ЗС України та інших військових формувань, населення тимчасово окупованих територій Донецької, Луганської областей та АР Крим.

Зважаючи на зазначене, формування стратегії виявлення загроз національній безпеці в інформаційній сфері, вчасна ідентифікація, локалізація та нейтралізація її осередків, а також зменшення негативного ІПсВ на населення України має бути пріоритетним напрямком роботи відповідних силових структур сектору безпеки і оборони держави.

Література

1. Горбулін В. У пошуках асиметричних відповідей: кіберпростір у

гібридній війні. ZN,UA. [Електронний ресурс]. – Режим доступу: https://zn.ua/ukr/internal/u-poshukah-asimetrichnih-vidpovidey-kiberprostir-u-gibridniy-viyni-_.html.

Прокопенко О.С.
д.філос. (комп'ютерні науки)
Національний університет оборони України імені Івана Черняховського
Федорієнко В.А.
к.т.н.,
Національний університет оборони України імені Івана Черняховського

ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ВИЯВЛЕННЯ І АНАЛІЗУ НЕГАТИВНОГО ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ

Стрімкий розвиток науково-технічного прогресу останніми десятиліттями, сприяє інтенсивному розвитку і використанню інформаційних технологій. Поряд з корисними і необхідними кроками цифровізації, призначеної, перш за все, для підвищення рівня інформаційної обізнаності суспільства, існують виклики і загрози застосування негативного інформаційно-психологічного впливу у відкритих джерелах інформації, що значно ускладнює процеси реалізації комунікативних заходів для досягнення стратегічних цілей держави. Особливої актуальності порушене питання набуває під час широкомасштабної збройної агресії російської федерації проти України. Негативний інформаційний вплив, заснований на використанні змісту ворожих пропагандистських наративів, активно розповсюджуються у глобальному інформаційному просторі, що негативно впливає на соціальну свідомість і суспільну думку, нав'язуючи на свою користь надуманий світогляд, твердження, факти, аргументи, чутки, тощо [1, 2]. Зазначене, вкрай негативно впливає на різні соціальні верстви населення тимчасово окупованих і прифронтових територій України, а також рівень мотивації особового складу частин і підрозділів Сил оборони України, які ведуть активні бойові дії.

На сьогодні, гостро постає питання використання сучасних інформаційних технологій моніторингу, збирання і обробки інформації з відкритих джерел у інформаційних системах військового призначення. Це пояснюється необхідністю вироблення необхідних заходів інформаційного протиборства проти розгорнутих інформаційно-психологічних спеціальних операцій противника, які можуть відбуватися комплексно з активізацією, підвищеною динамічністю і напруженістю ведення бойових дій на окремих напрямах фронту. За кількістю, інтенсивністю і масштабністю вкидань інформаційної пропаганди ворога, на основі використання

відомих математичних методів аналізу і прогнозування, можливо визначати етапи інформаційно-психологічної спеціальної операції, що надає додаткові можливості для своєчасних адекватних дій з інформаційної протидії.

Питання моніторингу інформаційного простору найбільшої ефективності набуло у програмних продуктах зарубіжних і вітчизняних розробників. До них відносяться як повнофункціональні продукти, де забезпечуються процеси обробки даних: збір даних, аналіз даних, візуалізація і інтерпретація даних, так і окремі сервіси і бібліотеки, за допомогою яких спрощуються процеси розробки програмного забезпечення на високорівневих мовах програмування: Python, C#, C++, PhP, Java та інші.

До першої категорії програмних продуктів належать: Semantrum, InfoStream, Wisdom Well, Web-Observer, Semantic Force, Multigo, Google Trends, Brandwatch, UAport, GreyLog. Усі зазначені продукти працюють в мережі Інтернет та реалізовані на веб платформах. Доступ здійснюється через веб браузер, за необхідністю для здійснення інтеграції між компонентами систем надається API-конектор [3]. Здебільшого, зазначені програмні продукти, розроблені у вигляді агрегаторів новин, де за допомогою відповідних фільтрів відслідковується необхідна інформація з обраних відкритих джерел. Обробка текстових даних веб-сторінок і соціальних мереж здійснюється на основі Web-скрапінгу і парсингу даних, а технології Machine Learning – вирішують задачі класифікації і кластеризації при розпізнаванні характеристик досліджуваного контенту інформації. Зрештою, оброблені дані візуалізують за допомогою спеціалізованих засобів у вигляді графіків, діаграм та інших графічних представлень, що дозволяє легше сприймати великі об’єми даних, швидко отримати візуальне уявлення про те, як дані пов’язані між собою і як вони можуть бути використані для вирішення конкретних проблем.

Проте, використання наведених вище програмних продуктів в інформаційно-аналітичному забезпеченні військового призначення супроводжується низкою невирішених питань, пов’язаних не лише з специфікою ліцензійних політик компаній-розробників, порядку обробки і зберігання даних, але й пристосованістю лише до цивільної сфери діяльності. Технологічні аспекти інформаційно-аналітичного забезпечення моніторингу інформаційного простору, крім вирішення наведених вище задач, в своєму арсеналі повинні включати:

Можливості з приймання-передавання, обробки текстових повідомлень про розташування і дії ворога, від населення тимчасово окупованих територій;

Технологію пошуку ворожих наративів в інформаційних повідомленнях відкритих джерел інформації, їх взаємозв’язок і прогнозовані ступені ризику на певні складові сектору безпеки і оборони України;

Систему підтримки прийняття рішень для оперативного вироблення, прийняття і реалізації необхідних заходів протидії деструктивного інформаційно-психологічного впливу противника.

Існуючі у практиці використання інформаційно-аналітичного забезпечення невідповідності, створюють передумови для розроблення інформаційної технології виявлення і аналізу негативного інформаційно-психологічного впливу. В сучасних реаліях, зазначене можливо досягти за рахунок низки різноманітних сервісів і спеціалізованих додатків обробки текстових масивів даних, можливості яких дозволяють виявляти та аналізувати інформаційні загрози. До таких відносяться:

Сервіси для аналізу тональності тексту – для визначення позитивного, негативного або нейтрального відтінку тексту: Такі сервіси, як TextRazor [4] та Aylien, можуть бути використані для аналізу соціальних мереж, новин та інших джерел інформації. Зазначене здійснюється на основі глибокого аналізу текстових даних для вилучення зв'язків, типізованих залежностей між словами та синонімами, уможливлюючи потужні контекстно-семантичні конструкції.

Сервіси для аналізу семантики та структури тексту, наприклад Gensim, FastText та SpaCy – дозволяють відшукувати спільні слова та теми у текстах. Вони можуть бути використані для аналізу новин, блогів, відгуків користувачів та інших джерел інформації. На прикладі бібліотеки машинного навчання для обробки текстів Gensim [5], можливо виокремити такі специфічні функції, як: аналіз семантики та структури тексту, тематичне моделювання, векторне представлення слів. Функції тематичного моделювання Gensim, на основі байєсівської моделі тематичного моделювання (Hierarchical Dirichlet Process), здійснює автоматизоване розпізнавання тематики текстового контенту. А на основі ймовірнісної моделі тематичного моделювання (Latent Dirichlet Allocation) – визначити кількість тематик та їх ключові слова.

Інструментарій для збору та аналізу даних з соціальних мереж, які дозволяють відслідковувати обговорення певної теми в соціальних мережах. Такі інструменти, як: Social Mention, Netvibes та Hootsuite, можуть використовуватися для моніторингу репутації, виявлення інформаційних загроз та аналізу тенденцій у громадській думці.

Наведені вище бібліотеки побудовані на базі платформи з відкритим кодом NLTK (Natural Language Toolkit) [6] для роботи з природними мовами. Вона надає доступ до корпусів текстів та лексичних ресурсів, а також має набір інструментів для обробки текстів, що допомагає вирішувати завдання, пов'язані з обробкою природних мов.

Сукупність наведених вище положень, дозволяє стверджувати про доволі обширні можливості сучасного інформаційного забезпечення, що дозволяє створювати нові інформаційні технології моніторингу інформаційного простору для певної специфіки діяльності, в тому числі удосконалення існуючого інформаційно-аналітичного забезпечення Збройних Сил України. Можливості з обробки тексту, побудованих на основі технологій штучного інтелекту, дозволяють виявляти у джерелах інформації не лише маніпулятивний зміст і

ворожі наративи, а також здійснювати:

Аналіз ключових слів у повідомленнях, які пов’язані з конкретною темою, та визначити, які саме аспекти повідомлень є ворожими;

Дослідження джерел (соціальних мережі, тематичні блоги), які поширюють інформацію до інших джерел;

Аналіз якості контенту інформації, за критеріями граматичної та стилістичної правильності, логіки, послідовності, та відповідності мовленнєвому етикету;

Оцінку рівня страху у повідомленнях, на основі аналізу лексики, тону та стилю повідомлень;

Оцінку рівня конфліктності, на основі аналізу кількості та ступеню емоційної напруги в повідомленнях, а також за кількістю звернень до агресивних слів та висловлювань.

Література

1. Почепцов Г. Сучасні інформаційні війни. Видання третє, доповнене та перероблене. Київ : Видавничий дім “Києво-Могилянська академія”, 2016. 504 с.

2. Курбан О. В. Сучасні інформаційні війни у мережевому он-лайн просторі. Навчальний посібник. Київ : ВІКНУ, 2016. 286 с.

3. Коротко про API та його тестування. – URL : https://qagroup.com.ua/publications/korotko-pro-ari-ta-jogo-testuvannia/ (дата звернення: 18.03.2023).

4. TextRazor. – URL : https://sourceforge.net/software/product/TextRazor/ (дата звернення: 18.03.2022).

5. D'Agostino A. How to Train a Word2Vec Model from Scratch with Gensim. – URL : https://towardsdatascience.com/how-to-train-a-word2vec-model-from-scratch-with-gensim-c457d587e031 (дата звернення: 13.03.2022).

6. Documentation. Natural Language Toolkit. – URL : https://www.nltk.org/ (дата звернення: 14.03.2023).

Рибальченко О.М.
аспірант кафедри психології та педагогіки,
Національного технічного університету України
«КПІ імені Ігоря Сікорського»

ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ОСОБИСТОСТІ

Минулі цивілізації і теперішній світ, навколишнє природнє середовище і соціальні явища в суспільстві, питання благополуччя, забезпечення безпеки, а саме захист життя і збереження здоров’я людини в будь якій державі не спроможні існувати без такого поняття як – інформація.

Термін «інформація» походить від латинського слова «informatio», що означає відомості, роз'яснення, виклад. Інформація – це все те, що безпосередньо впливає на людину, все те що людина бачить, відчуває, сприймає, отримує і передає, використовує і т. п. у своєму повсякденному житті. Інформація для людини в першу чергу – це джерело існування у суспільстві, а по друге – безцінний накопичений скарб для виживання при загрозливих обставинах або важких умовах.

Сьогодні в державі інформація перетворилась на важливий воєнний, економічний, політичний та соціальний ресурс. Сучасна свідомість, задовольняючи потреби українців в отриманні та переробці інформації, сприяє їхній орієнтації в швидкозмінюваних політичних, соціально-економічних умовах в період бойових дій, наполягає бути пильними і гнучкими у сприйнятті відомостей, а також бути активними учасниками в тих чи інших суспільно-політичних, громадських, військових подіях.

З одного боку наявність скривленої та брехливої інформації характеризує небезпеку і як наслідок нестійкий психологічний стан особистості, тому що дезінформація дестабілізує особистісну поведінку, спотворює взаємозв’язки і колективну діяльність людини у суспільстві.

А з іншого боку, за своєю природою викликає у людини потребу в безпеці, прагненні особистості до щирості і відвертості, гідності і справедливості, а також відчуттю захисту від зовні негативного впливу, готовності до супротиву і боротьбі з вигадками, плітками і фейками.

Поняття безпеки є багатозначним та багатофункціональним. Сучасні науковці надають велику кількість його тлумачень залежно від її різновидів.

Серед основних змістовних понять «безпека» можна виділити наступні: безпека як внутрішнє самовідчуття людини, безпека як необхідна умова індивідуальної свободи; безпека як умова розвитку соціуму і безпека як стан держави або міжнародного співтовариства держав. З аналізу літературу, стає зрозумілим, що головним чинником, навколо кого з'являється поняття про захист – це особистість. Наявність безліч різновидів «безпек» породжує і безліч понять «безпека особистості».

У загальному розумінні безпека особистості – це стан відсутності небезпеки при взаємодії з об'єктами зовнішнього середовища, процес забезпечення захищеності життєво важливих інтересів, а також здатність зберегтися при руйнівних впливах.

Серед різноманітних видів безпек, таких як військова, економічна, техногенна, політична, правова, соціальна, психологічна тощо, в залежності від функціональної спрямованості виділяють – інформаційну безпеку.

Інформаційна безпека особистості – це особливий стан специфічної захищеності і гарант непохитної стійкості людини до руйнівних сил та засобів в інформаційному просторі (середовищі).

Розглядаючи інформаційну безпеку особистості (у вузькому розумінні) – можна зауважити, що це стан захищеності психіки людини від негативного впливу, який здійснюється шляхом упровадження деструктивної інформації у свідомість і (або) упідсвідомість людини, що призводить до неадекватного сприйняття нею дійсності.

А розглядаючи інформаційну безпеку особистості (в широкому розумінні) – потрібно розуміти, що це:

- належний рівень теоретичної і практичної підготовки особистості, при якому досягається захищеність і реалізація її життєво важливих інтересів і гармонійний розвиток незалежно від інформаційних загроз;
- здатність держави створити можливості для гармонійного розвитку і задоволення потреб особистості в інформації, незалежно від інформаційних загроз;
- гарантування, розвиток і використання інформаційного середовища в інтересах особистості;
- захищеність від різного роду інформаційних небезпек.

Окремо потрібно зауважити, що на стан інформаційної безпеки особистості впливають багато різноманітних чинників але серед них в першу чергу визначають загрози та ризики.

Загрози інформаційній безпеці можна трактувати як сукупність внутрішніх та зовнішніх умов, які можуть нанести шкоду інтересам особистості та суспільства через небажані інформаційні атаки на відповідні об’єкти інформаційної інфраструктури держави. А вдале, вміле і ефективне управління небезпеками і пов’язані з ними загрозами сприяє їх успішному усуненню.

Так, на думку Г. Сащук [1], «враховуючи той факт, що під впливом інформаційних атак може цілеспрямовано змінюватися світогляд та мораль як окремих осіб, так і суспільства в цілому, нав’язуються чужі інтереси, мотиви, спосіб життя, на перший план випливає аналіз сутності та форм проявів сучасних методів прихованого агресивного впливу, вияву дій, що мають цілеспрямований агресивний характер і які протирічать інтересам національної безпеки, та вироблення механізмів протидії їм у всіх напрямах».

З досліджень Горбатюка О.М., Гуцалюка М., Ліпкана В.А. та ін. стало відомо, що в загальному, виділили наступні види загроз інформаційній безпеці, а саме: загрози впливу неякісної інформації (недостовірної, фальшивої, дезінформації) на особистість, суспільство, державу; загрози несанкціонованого і неправомірного впливу сторонніх осіб на інформацію і інформаційні ресурси (на виробництво інформації, інформаційні ресурси, на системи їхнього формування і використання); збої в роботі обладнання (може виникнути при блокуванні доступу до одного або декількох ресурсів інформаційної системи); загрози інформаційним правам і свободам особистості (праву на виробництво, розповсюдження, пошук, одержання, передавання і використання інформації; праву на інтелектуальну

власність на інформацію і речову власність на документовану інформацію; праву на особисту таємницю; праву на захист честі і достоїнства і т. ін.) [2; 3].

Аналіз наукових робіт також свідчить і про джерела загроз інформаційній безпеці які розподілили на три групи, де було визначено що:

- (перша група), це джерела загроз інформаційній безпеці особистості (тобто забезпеченню конституційних прав і свобод людини і громадянина на доступ до відкритої інформації, на використання інформації в інтересах здійснення незабороненої законом діяльності, а також у захисту інформації, що забезпечує особисту безпеку, духовний та інтелектуальний розвиток.

- (друга група), це джерела загроз інформаційній безпеці суспільства (безперервне ускладнення інформаційних систем і мереж зв'язку кри тично важливих інфраструктур забезпечення життя суспільства.

- (третя група), це джерела інформаційній безпеці держави (отримання протиправного доступу до відомостей, що складають державну таємницю, до іншої конфіденційної інформації, розкриття якої може нанести збитки державі; спроби реалізації концепції ведення інформаційних війн; неконтрольоване розповсюдження інформаційної зброї.

Важливо відзначити, що несприятливі ситуації чи події для людини – це лише показники наявності небезпеки. Поки ці показники не трансформувалися в критерії загроз, існує лише ризик заподіяння шкоди чи збитку особистості [4].

Загрози інформаційній безпеці особистості тісно сплітаються, пов’язані і суттєво впливають на психологічний стан особистості.

Рівень психологічної загрози значно залежить від кількості і сили дії небезпечних факторів на свідомість людини. Що більше таких факторів, то швидше небезпека переростає у психологічну загрозу, унаслідок чого виникає деструктивна поведінка особистості.

Тому, загроза – це суб’єктивна ознака, яка викликає в особистості необхідність захищатися від несприятливих подій [4].

За наявності таких психологічних небезпек особистості, як порушення ідентичності, неадекватність самооцінки, втрата самоконтролю, зміна рольової поведінки, втрата моральних орієнтирів, соціальна дезорганізація, виникають умови, за яких можуть виявлятися психологічні загрози особистості, а саме: трансформація спрямованості; деформація цінностей; порушення мотивації; спотворення цілей; деструкція сенсів – які здатні дестабілізовано і дисбалансовано впливати на інформаційну безпеку особистості.

Висновки: Загрози інформаційній безпеці особистості впливають на: людський фактор, де враховуються психічні та фізичні можливості суб’єкта; фактор середовища, а саме стан життєдіяльності людини (місце проживання, погодні умови, наявність небезпек природнього і техногенного характеру, тощо); соціальний фактор, який поділяється на макро- та мікро- соціальні чинники, які в свою чергу зумовлюють стабільність суспільства і де особистість набуває

безпосередній досвід соціального розвитку, отримує реальні навички адаптації до постійно мінливих умов діяльності; засоби захисту – які формують у особистості індивідуальне відчуття безпеки, як на фізичному (одяг, взуття, зброя) так і психологічному рівнях (механізми психологічного захисту і співволодіння зі стресовими ситуаціями).

Література

1. Сащук Г.М. Роль і місце національної спецслужби в історії українського державотворення. Київ: ВПЦ «Київський Університет», 2017. 183с.
2. Світлична В. Ю. Інформаційна безпека: сутність та порядок реалізації / Молодий вчений. 2014. № 11(14). С. 97-100. Режим доступу: http://nbuv.gov.ua/UJRN/molv_2014_11(14)__26.
3. Остроухов В., Петрик В. До проблеми забезпечення інформаційної безпеки України / Політичний менеджмент. 2008. № 4. С. 135-141. Режим доступу: http://nbuv.gov.ua/UJRN/PoMe_2008_4_16.
4. Рибальченко О.М. «Психологічні загрози – компонент безпеки особистості». Науковий журнал з соціології та психології «Габітус». Випуск 32/2021, С. 104 – 109.

Романчук М.П.
к.т.н.,
Наумчак О.М.
Наумчак Л.М.
Житомирський військовий інститут імені С.П. Корольова

ВИКОРИСТАННЯ ГРАФОВИХ НЕЙРОННИХ МЕРЕЖ ДЛЯ ВИЯВЛЕННЯ ПОШИРЮВАНОЇ ПРОТИВНИКОМ ПРОПАГАНДИ

Інформація стала одним із найбільш перспективних видів зброї. Протиборства в інформаційній сфері розширюють свої можливості стрімкими темпами. Відсутність фізичних кордонів дозволяє «проникати» в інформаційне середовище іншої країни та здійснювати агресію проти її громадян, державних інститутів, сфери бізнесу тощо. Мова йде про прихований вплив не лише на критичну інформаційну інфраструктуру, а й на населення країни, що безпосередньо впливає на стан національної безпеки держави.

Інформаційні конфлікти можуть бути спрямовані на різноманітні цілі, такі як вплив на політичні процеси, військову сферу, економіку, соціальні проблеми та культурні аспекти.

Один з основних методів протиборства в інформаційній сфері – це пропаганда, що може включати розповсюдження дезінформації, маніпулювання

фактами, поширення фейкових новин тощо. Це може призвести до створення спотвореного уявлення про реальну ситуацію в державі, що може спричинити різні наслідки, зокрема мати значний вплив на стан безпеки держави. Наприклад активно поширювана пропаганда може призвести до зниження довіри громадян до влади, збудити напруження в суспільстві, порушити демократичні процеси, спричинити економічні труднощі та інші проблеми.

рф має значний потенціал для ведення інформаційної боротьби. Війна, що триває, ґрунтується на багаторічній експансії інформаційного простору та насиченні його пропагандою з метою витіснення української ідентифікації. За таких умов особливо небезпечний негативний інформаційний вплив на військовослужбовців сил безпеки та оборони.

Організація захисту військовослужбовців від негативного інформаційного впливу передбачає наявність 3 складових: моніторингу інформаційного простору; аналізу та прогнозування інформаційних загроз, вироблення стратегій щодо забезпечення захисту особового складу сил оборони; нейтралізації таких впливів та здійснення адекватних контр- та превентивних заходів [1].

Зважаючи на викладене вище, питання вдосконалення системи протидії агресивним діям в інформаційному просторі лишається достатньо актуальним аспектом системи національної безпеки. Для протиборства в інформаційній сфері потрібно розвивати механізми виявлення пропаганди та вчасно реагувати на неї, відповідно до законодавства. Також важливо забезпечувати належний рівень кібербезпеки та інформаційної безпеки, щоб запобігти хакерським атакам та витокам даних, які можуть створювати підґрунтя для поширення дезінформації фейкових новин тощо.

Враховуючи те, що фейкові новини є засобом поширення пропаганди, механізми виявлення та реагування на неї можуть включати наступне:

моніторинг медіа: відстеження засобів масових комунікацій, соціальних мереж, інших інтернет-ресурсів з метою виявлення поширення фейкових новин;

аналіз даних: застосування методів аналізу даних, таких як машинне навчання та аналіз текстів, для виявлення та аналізу фейкових новин;

розвиток стратегічних комунікацій: використання комунікативних можливостей держави (зокрема співпраця з різними спільнотами, дослідниками, журналістами, громадськими активістами та іншими) для виявлення та протидії (спростування) фейкових новин, спільного реагування та надання об'єктивної та достовірної інформації громадськості;

правові механізми: використання правових механізмів для протидії поширення пропаганди – притягнення до відповідальності тих, хто поширює неправдиву інформацію;

технічні рішення: використання фільтрів, антивірусних програм, для зменшення ризику вірусних атак та розповсюдження спаму.

Моніторинг медіа – це процес відстеження новин та інформації, яка

публікується в різних джерелах масової комунікації, включаючи традиційні ЗМІ, соціальні мережі, блоги та інтернет-форуми. Він може проводитися вручну, спеціалістами, які відстежують джерела новин та аналізують їх зміст. Однак краще використовувати автоматизовані інструменти.

Автоматизовані засоби моніторингу медіа зазвичай базуються на алгоритмах машинного навчання та обробці природної мови. Основна їх перевага полягає у швидкості, адже вони дозволяють відстежувати новини в режимі реального часу та одночасно аналізувати тисячі джерел медіа.

Серед автоматизованих засобів моніторингу медіа можна виділити такі:

1. Платформи моніторингу соціальних медіа – ці інструменти дозволяють відстежувати активність користувачів у соціальних мережах, аналізувати настрої громадськості та виявляти тренди.

2. Аналітичні інструменти – ці інструменти дозволяють відстежувати джерела новин, проводити аналіз текстів, розрізняти позитивні та негативні новини, визначати тональність тексту та інші параметри.

Однією із задач системи протидії впливам ворога в інформаційному просторі є моніторинг та виявлення ознак деструктивного психологічного впливу, поширюваного в інформаційних повідомленнях, які можуть виступати у вигляді текстових, візуальних, аудіо- та аудіовізуальних матеріалів. Для моніторингу кожного окремого виду розповсюджуваних матеріалів використовуватимуться різні методи та підходи.

Зазвичай системи моніторингу складаються із 3 основних складових: спостереження, оцінювання та прогнозування. Розглянуто елемент системи моніторингу, що відповідає за збір та аналіз текстових даних з мережі Інтернет з метою виявлення деструктивних впливів. У [2] було розглянуто підхід до вияву фейкових новин, заснований на графових нейронних мережах.

Графові нейронні мережі (Graph Neural Networks, GNNs) є потужним інструментом для аналізу складних взаємодій між об'єктами у графах, що може бути корисним при виявленні фейкових новин. Головною перевагою використання графів є їх здатність представляти інформацію про вузли (вершини) та про їх зв’язки. Графи, відповідно до їх структури, дозволяють вирішувати одночасно задачі трьох рівнів: на рівні вершин; на рівні ребер; на рівні графу.

Завдання на рівні вершин: класифікація та регресія. Їх мета: передбачити мітку, тип, категорію або атрибут вершини.

Завдання рівня ребер: прогноз посилань. Мета: відновити зв’язки між вершинами у заданому неповному наборі.

Завдання на рівні графів: класифікація графів, регресія та кластеризація. Мета: виконувати завдання класифікації, регресії або кластеризації на усьому графі (або підграфі).

GNNs можуть бути корисними для моніторингу інформаційного простору на рівні вершин графа для виконання наступних завдань:

1. Виявлення фейкових новин або дезінформації. Наприклад, мережа може аналізувати поширення інформації і виявляти відхилення від типових шаблонів.

2. Виявлення впливових користувачів або ботів. Наприклад, мережа може аналізувати граф взаємодій користувачів в соціальній мережі та виявляти впливових користувачів або ботів, що можуть використовуватись для розповсюдження пропаганди.

3. Виявлення класів користувачів. Наприклад, мережа може аналізувати взаємодії користувачів в соціальній мережі та виявляти групи користувачів зі схожими інтересами, що можуть використовуватись для поширення пропаганди.

4. Виявлення відгуків та реакцій. Наприклад, мережа може аналізувати реакції користувачів на новини або інші події та виявляти шаблони поведінки або настроїв, що можуть бути корисними для аналізу громадської думки.

5. Виявлення популярних тем. Наприклад, мережа може аналізувати теми, виявляти популярні серед користувачів.

Одна з ключових складностей виявлення фейкових новин полягає у визначенні взаємодій між суб'єктами та об'єктами у тексті новин. Застосування GNNs може допомогти в цьому завданні, адже вони дозволяють моделювати взаємодії між об'єктами у вигляді графа.

Отже, для виявлення фейкових новин за допомогою GNNs необхідно побудувати граф, де кожен вузол представляє один елемент новини, наприклад, слово або фразу, а ребра позначають взаємодії між ними. На основі цього графа можна створити модель GNN, яка аналізуватиме структуру графа та взаємодії між його вузлами, щоб визначити, чи є новина фейком.

Окрім того, GNNs можуть бути використані для аналізу відносин між джерелами новин. Наприклад, можна побудувати граф, де кожен вузол представляє одне джерело новин, а ребра показують, які джерела мають схожу тематику та як вони пов'язані між собою. Це може допомогти визначити, чи є джерело надійним, або чи є його новини фейками.

Загалом, GNNs є потужним інструментом для аналізу складних взаємодій у графах, що може бути корисним для виявлення фейкових новин та підвищення якості розпізнавання та аналізу текстів. Використання програмних засобів, які виявляють пропаганду та дезінформацію, має свої обмеження, і вони повинні використовуватися в поєднанні з людською експертизою та аналізом. Важливо пам'ятати, що критичне мислення та аналітичні навички є ключовими для розуміння та інтерпретації інформації, а також для виявлення пропаганди.

Література

1. Манько О., Наумчак О. Підхід до організації захисту військовослужбовців від негативного інформаційного впливу. Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем. 2019. № 17. С. 110–120. doi: 10.46972/2076-1546.2019.17.10.

2. Fake News Detection in the Framework of Decision-Making System through Graph Neural Network / I. Pilkevych та ін. 2021 IEEE 4th International Conference on Advanced Information and Communication Technologies (AICT), м. Львів, 2021 р. С. 153–157. doi : 10.1109/AICT52120.2021.9628907.

Самойленко О.О.
д.пед.н, доцент
ННІ ІБСК НА СБ України
Войтович А.О.
курсант НА СБ України

ФАКТЧЕКІНГ ЯК ІНСТРУМЕНТ БОРОТЬБИ З РОСІЙСЬКОЮ ПРОПАГАНДОЮ

Фактчекінг - це процес перевірки фактів, який використовується з метою підтвердження або спростування неправдивої інформації. Цей процес включає перевірку джерел інформації, їх авторитетності, перевірку статистичних даних, дат та іншої інформації, що міститься в тексті [2].

Мета фактчекінгу - забезпечити точність та достовірність інформації, що надається читачам або глядачам, та запобігти поширенню неправдивої інформації. У даний час фактчекінг є важливою складовою журналістики та інших засобів масової інформації, а також широко використовується у соціальних мережах для боротьби з дезінформацією [2].

Фактчекінг має високу актуальність в контексті сучасної політичної ситуації в світі, а особливо в Україні та країнах, які перебувають в зоні впливу російської пропаганди. Пропаганда рф має довгу історію та активно використовується для досягнення політичних цілей, в тому числі втручання в виборчі процеси, підриву стабільності країн, зміни світогляду та збільшення впливу на суспільство. З використанням спеціалізованих інтернет-ресурсів, які займаються перевіркою фактів, громадяни мають доступ до найбільш достовірної та об'єктивної інформації, яка допомагає їм робити більш обґрунтовані та зважені рішення.

Розглянемо декілька спеціалізованих інтернет-ресурсів:

1. PolitiFact - ресурс, який займається перевіркою тверджень, що стосуються політики та громадського життя в США. Ресурс використовує шкалу оцінювання від "правда" до "брехня".
2. FactCheck.org - ресурс, що перевіряє твердження, що стосуються політики та громадського життя в США. Ресурс відносить твердження до категорій "правда", "частково правда", "частково неправда", "неправда" та "заплутано".
3. Snopes - ресурс, який перевіряє твердження з різних сфер життя,

включаючи політику, громадське життя та інші. Ресурс відносить твердження до категорій "правда", "частково правда", "частково неправда", "неправда" та "заплутано".

4. TruthOrFiction.com - ресурс, що займається перевіркою тверджень та ланцюжків електронних листів, які часто містять неперевірену інформацію. Ресурс відносить твердження до категорій "правда", "фейк" та "заплутано".

5. Fact-Checking Ukraine - перший в Україні ресурс, який займається перевіркою тверджень, що стосуються політики та суспільства в Україні. Ресурс працює відтінком оцінювання від "правда" до "брехня".

6. Full Fact - ресурс з Великої Британії, який займається перевіркою тверджень, що стосуються політики та громадського життя. Ресурс використовує систему оцінювання від "правда" до "неправда"[3].

Ці ресурси забезпечують громадянам доступну та достовірну інформацію, що допомагає розуміти, наскільки достовірні та точні твердження, які вони отримують із ЗМІ або на теренах мережі Інтернет. Вони також допомагають зменшити поширення неправдивої інформації, що може бути шкідливою для суспільства та демократії. При цьому важливо зазначити, що ні один із наведених ресурсів не є абсолютно точним та повністю об'єктивним. Кожен ресурс має свої власні процедури та стандарти для оцінки тверджень, і, хоча вони прагнуть бути об'єктивними та надійними, іноді можуть зробити помилку або пропустити важливу деталь.

Застосування методу перевірки фактів забезпечує зменшення впливу російської пропаганди на суспільство та підвищує рівень довіри до засобів масової інформації та політичних діячів. Також цей інструмент є важливим для збереження свободи слова та інформаційної безпеки в країнах, які перебувають під впливом російської пропаганди. Крім того, фактчекінг допомагає розвивати критичне мислення та навички аналізу інформації серед населення, що є особливо важливим в епоху інформаційних технологій, коли доступ до інформації став легким і безкоштовним.

Проте, слід зазначити, що фактчекінг не є універсальним інструментом для боротьби з російською пропагандою. Пропаганда має складну структуру та різноманітні методи впливу на суспільство, тому потрібно використовувати комплексний підхід до боротьби з нею. До таких підходів можуть належати підвищення рівня медіаграмотності серед населення, створення відкритих джерел інформації, залучення міжнародних експертів та організацій для аналізу інформації та боротьби з пропагандою, а також розвиток внутрішніх інститутів демократії, які забезпечують свободу слова та інформаційну безпеку.

Отже, фактчекінг є важливим інструментом боротьби з російською пропагандою, що допомагає забезпечити правдиву та об'єктивну інформацію, а також розвивати критичне мислення в суспільстві. Проте, для ефективної боротьби з пропагандою необхідний комплексний підхід та залучення

різноманітних інструментів.

Література

1. Панчук Д.М. Фактчекінг // Велика українська енциклопедія. URL: https://vue.gov.ua/Фактчекінг (дата звернення: 10.03.2023).

2. Fact-checking. URL: https://en.m.wikipedia.org/wiki/Fact-checking (дата звернення: 10.03.2023)

3. Stencel M., Luther J. Fact-checking Census Shows Slower Growth // Duke Reporters' Lab. 2021. URL: https://reporterslab.org/fact-checking-census-shows-slower-growth/ (дата звернення: 11.03.2023)

Самойленко О.О.
д.пед.н., доцент, доцент КІБД
Національної академії СБ України
Шульга А.В.
студент Національної академії СБ України

РОЗВІНЧАННЯ МІФУ ПРО ТЕ, ЩО УКРАЇНА НЕ ДОТРИМУЄТЬСЯ ЖЕНЕВСЬКОЇ КОНВЕНЦІЇ ПРО ПОВОДЖЕННЯ З ВІЙСЬКОВОПОЛОНЕНИМИ

Актуальність розвінчування міфу про те що Україна не дотримується женевської конвенції є значущою, оскільки розвіювання саме цього міфу допоможе вплинути не тільки на російських військових, які можуть бути впевнені у людському поводженні в разі здачі в полон, а й на західних партнерів, що в свою чергу дозволить збільшити постачання матеріального забезпечення та підніме авторитет України як європейської держави. Теоретична вагомість дослідження дасть можливість зрозуміти підхід рф до написання фейків. В свою чергу, практичним значенням є застосування спеціальних методів для ефективного і швидкого виявлення та розвінчування фейків.

Женевська конвенція про поводження з військовополоненими є міжнародним документом, прийнятим у 1949 році, що встановлює правила поведінки сторін конфлікту відносно військовополонених. Цей документ зобов'язує сторони конфлікту поважати права та гуманітарні принципи, пов'язані з поводженням з полоненими. Україна підписала цю конвенцію в 1958 році чим зобов'язалася дотримуватися її положень.

Україна дотримується своїх міжнародних зобов'язань, включаючи Женевські конвенції. Вона має законодавство, яке регулює поводження з військовополоненими та іншими особами, що перебувають під її владою. У разі порушення прав людини та міжнародних стандартів Україна проводить відповідні

розслідування та притягує до відповідальності за порушення.

Немає жодних обґрунтованих доказів того, що Україна не дотримується женевської конвенції про поводження з військовополоненими.

Водночас, теза про те, що Україна не дотримується женевської конвенції про поводження з військовополоненими завжди була актуальна для російських та сепаратистських ЗМІ. Ще починаючи з 2014 року, росія активно поширювала інформацію, про нелюдське поводження з бойовиками так званих ДНР та ЛНР. На спростування цієї інформації є декілька аргументів:

- по-перше, бойовики так званих ДНР та ЛНР, не підпадають під класифікацію військовополонених, зазначених в Конвенції про поводження з військовополоненими. Отже вони класифікуються, як особи, які скоїли злочини на території України, і вважаюся підозрюваними чи обвинуваченими, залежно від стадії кримінального провадження. Відповідно їхні права та обов'язки передбачені в Кримінальному процесуальному кодексі, а не у вищезазначеній Конвенції;

- по-друге, згідно зі звітом Міжнародного Комітету Червоного Хреста, який був надісланий до України у вересні 2014 року, стверджується, що Україна дотримується міжнародних стандартів відносно поводження з бойовиками ДНР та ЛНР. Зокрема, звіт був опублікований після відвідин в'язниць та інших місць тримання бойовиків.

Отже можна зробити висновок, що незважаючи на невідповідний статус бойовиків так званих ДНР та ЛНР, Україна неухильно дотримується усіх правил та обов'язків пов'язаних з перебуванням цих осіб під вартою. Це підтверджується звітами та офіційними заявами міжнародних організацій, таких, як Міжнародний Комітет Червоного Хреста.

Ситуація з російськими військовополоненими є іншою, оскільки вони вже підпадають під дію Конвенції про поводження з військовополоненими. На цьому підґрунті росія також маніпулює та робить заяви, що Україна начебто порушує права російських військовополонених. Зокрема:

- по-перше, Управління Верховного комісара ООН з прав людини випустило доповідь про те, як під час війни росії проти України сторони конфлікту поводяться з військовополоненими. В цій доповіді зазначається, що Україна дотримується усіх передбачених Женевською конвенцією про поводження з військовополоненими прав та надає доступ до полонених спеціальним комісіям;

- по-друге, у Міністерстві юстиції України неодноразово повідомляли, як утримують російських військовополонених (на їх утримання щомісячно витрачається біля 10-11 тис. грн, полонених годують тричі на день, виводять на прогулянку, що найменше, на годину тощо).

Підсумовуючи, можна впевнено сказати, що Україна дотримується своїх зобов'язань передбачених Женевською конвенцією про поводження з військовополоненими. Це підтверджується заявами авторитетних міжнародних організацій, зокрема, таких як Управління Верховного комісара ООН з прав

людини.

Отже можемо зробити висновок, що Україна має відповідальне ставлення до поводження з військовополоненими та відповідно до цього забезпечує їм повагу та захист. Військові, які потрапили в полон, отримують належне лікування та гуманне поводження від українських військових та цивільних організацій. Україна також забезпечує міжнародний доступ до військовополонених, відповідно до зобов'язань, встановлених у Женевській конвенції. Україна регулярно співпрацює з Міжнародним комітетом Червоного Хреста та іншими міжнародними організаціями для забезпечення відповідного поводження з військовополоненими.

Таким чином, можна стверджувати, що міф про те, що Україна не дотримується Женевської конвенції про поводження з військовополоненими, не має під собою жодних підстав.

Література

1. Женевська конвенція про поводження з військовополоненими: Конвенція від 12.08.1949. URL: https://zakon.rada.gov.ua/laws/show/995_153#Text (дата звернення: 10.03.2023).

2. В Мін'юсті розповіли, скільки витрачають в місяць на утримання одного полоненого окупанта. ZN.UA. URL: https://zn.ua/ukr/war/v-minjusti-rozpovili-skilki-vitrchajut-v-misjats-na-utrimannja-odnoho-polonenoho-okupanta.html (дата звернення: 10.03.2023).

3. Олена Висоцька: Російські військовополонені скаржаться на «катування історіями про гетьманів та державним гімном України. Minjust.gov.ua. URL: https://minjust.gov.ua/news/ministry/olena-visotska-rosiyski-viyskovopoloneni-skarjatsya-na-katuvannya-istoriyami-pro-getmaniv-ta-derjavnim-gimnom-ukraini (дата звернення: 10.03.2023).

4. Як російська пропаганда впливає на суспільну думку в Україні. Media Sapiens. 2017. 13 лютого. URL: http://osvita.mediasapiens.ua/mediaprosvita/research/yak_rosiyska_propaganda_vplvae_na_suspilnu_dumku_v_ukraini_doslidzhennya (дата звернення: 10.03.2023).

Саричев Ю.О.
к.т.н., с.н.с.,
Уварова Т.В.
к.т.н.,
Зубков В.П.
Піщанський Ю.А.
Національний університет оборони України імені Івана Черняховського

ПРОБЛЕМНІ ПИТАННЯ РЕАЛІЗАЦІЇ ЗАВДАНЬ КІБЕРОБОРОНИ ЯК СКЛАДОВОЇ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

Забезпечення інформаційної безпеки держави у воєнній сфері в сучасних умовах залежить від наявності багатьох чинників, що цілком справедливо і для забезпечення кібербезпеки України. Зокрема, завдання кібероборони в системі Міністерстві оборони (МО) України ставиться до виконання в умовах недосконалої теорії забезпечення інформаційної безпеки держави, починаючи з питання термінології в наслідок плутанини у відповідних законодавчих актах. Такий негативний стан потребує удосконалення теоретичної та нормативно-правової бази усього інформаційного законодавства України.

З позицій системного підходу до розгляду питань забезпечення інформаційної безпеки у воєнній сфері можна стверджувати, що в Україні фактично маємо дві стратегії інформаційного спрямування, одна з яких стосується питань кібербезпеки держави. В цих умовах для розуміння можливих шляхів удосконалення існуючої системи забезпечення інформаційної безпеки у воєнній сфері необхідно уточнити законодавчі положення стосовно завдань щодо кібербезпеки у цій сфері.

Відповідно до чинного законодавства з питань кібербезпеки стосовно воєнної сфери діють наступні положення. Зокрема, [1] встановлює наступне.

МО України, Генеральний штаб (ГШ) ЗС України відповідно до компетенції:

здійснюють заходи з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони);

здійснюють військову співпрацю з НАТО та іншими суб’єктами оборонної сфери щодо забезпечення безпеки кіберпростору та спільного захисту від загроз;

впроваджують заходи із забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного стану.

З огляду на те, що Головне розвідувальне управління (ГУР) є структурним підрозділом МО України, то до зазначених пунктів слід долучити і таке (четверте) положення із цього Закону:

розвідувальні органи України здійснюють розвідувальну діяльність щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки.

Це положення відноситься до усього розвідувального співтовариства України. Судячи зі змісту статті 9 Закону України [2], розвідувальний орган МО України (тобто ГУР) здійснює розвідувальну діяльність у воєнній сфері, сферах оборони, військового будівництва, військово-технічній та кібербезпеки.

Іншим розвідувальним органам в системі МО України, зокрема у складі ЗС України, завдань розвідувальної діяльності щодо загроз у кіберпросторі цим законом України [2] не ставиться.

До усіх вищезазначених положень Закону України [1] також є ряд принципових запитань, щоб зрозуміти їх предметну сутність, аби не натикатися у практиці на потребу вольових суб'єктивних рішень та дій.

Перше запитання термінологічного характеру. Зокрема, як з позиції положень цього Закону розуміти поняття "кібероборона" та що означають словосполучення "воєнна агресія у кіберпросторі", "відбиття воєнної агресії у кіберпросторі"?

Друге запитання щодо логіки вимог у цих законодавчих положеннях:

чому для умов воєнного стану цей закон вимагає лише "забезпечення кіберзахисту критичної інформаційної інфраструктури", а не відбиття воєнної агресії у кіберпросторі, тобто кібероборони у повному обсязі?;

чому розвідувальний орган МО України здійснює розвідувальну діяльність за усім спектром питань кібербезпеки, а не лише щодо питання кібероборони як головного питання для МО України у сфері кібербезпеки?

По-третє, чому всупереч Закону України [3] МО України, ГШ ЗС України мають впроваджувати заходи із забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного стану?

Спробуємо і на ці запитання, по можливості, з'ясувати відповідь.

По першому запитанню щодо поняття терміну "кібероборона". Виходячи із контексту вищенаведеного законодавчого положення, зазначено, що кібероборона – відбиття воєнної агресії у кіберпросторі.

Але, спочатку, в Законі України [1] визначається, що кібероборона – сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії.

Крім зазначеного, в Законі України [4] міститься:

кібероборона – активний кіберзахист (для захисту суверенітету держави та забезпечення її обороноздатності, запобігання збройному конфлікту та відсічі збройній агресії).

З іншого боку, в [4] (стаття 4 "Відсіч збройній агресії проти України") також міститься положення, що у разі збройної агресії проти України на підставі відповідного рішення Президента України ЗС України розпочинають воєнні дії, у тому числі проведення спеціальних операцій (розвідувальних, інформаційно-

психологічних тощо) у кіберпросторі. Тобто, за цим положенням "відсіч (отже відбиття) збройній агресії проти України у кіберпросторі", що збігається з одним із щойно вищенаведених понять терміну "кібероборона", означає "проведення спеціальних операцій (розвідувальних, інформаційно-психологічних тощо) у кіберпросторі".

Розглядаючи одночасно усі ці визначення, що містяться в законодавстві України, суть кібероборони держави зрозуміти неможливо, оскільки усі описані сутності принципово різні, а до цього ж (у прямому визначені) неможливо також уявити шляхи реалізації у кіберпросторі більшості перелічених заходів. Отже, поняття "кібероборона" в законодавстві України виписане недосконало, а тому потребує коректного та однозначного законодавчого визначення.

Щодо незрозумілих термінів з першого запитання зазначимо наступне. Поняття "воєнна агресія у кіберпросторі" визначене в редакції [5]:

воєнна агресія в кіберпросторі – здійснення системних та масштабних дій проти України в кіберпросторі іноземними державами (групами держав), зокрема із залученням кіберпідрозділів військових формувань, розвідувальних та спеціальних служб, включаючи використання кіберозброєння та інших спеціальних засобів впливу в кіберпросторі (зокрема, шляхом приховування джерел їх походження).

Але, таке визначення викликає принципові питання: по-перше, щодо сумнівної можливості за цим формулюванням ідентифікувати агресора з метою надання йому адресної відсічі без порушення міжнародного права, по-друге, не усі масштабні дії проти України в кіберпросторі іноземними державами (групами держав) можуть вважатися воєнною агресією, а по-третє, невизначеним, отже незрозумілим, є вжитий термін "кіберозброєння". Тому це визначення потребує уточнення.

Інше поняття "відбиття воєнної агресії у кіберпросторі" в законодавстві України не визначене. Не зустрічається його тлумачення і в доступних фахових наукових виданнях. У цій ситуації, на перший погляд, можна посилатися на вищезазначену статтю 4 Закону України [4], де міститься положення, що у разі збройної агресії ЗС України розпочинають воєнні дії, у тому числі проведення спеціальних операцій (розвідувальних, інформаційно-психологічних тощо) у кіберпросторі.

Тоді термін "відбиття воєнної агресії у кіберпросторі" (як варіант, це сутність кібероборони) означає проведення спеціальних операцій (розвідувальних, інформаційно-психологічних тощо) у кіберпросторі. За цією логікою відбиття воєнної агресії у кіберпросторі (кібероборону) мають здійснювати Сили спеціальних операцій (ССО) ЗС України, оскільки, відповідно до Законів України [2, 4, 6], лише вони проводять спеціальні операції, включно із спеціальною розвідкою та інформаційно-психологічними діями. У зв'язку із цим виникає питання щодо доцільності створення (відповідно до Указів Президента України [7,

8]) в системі МО України кібервійськ, що суперечить положенням цих Законів. Тут необхідно або змінювати статтю 4 Закону України [4], або кібероборону держави зосередити в межах завдань ССО ЗС України. На наш погляд, простіше внести зміни до Закону.

Перша частина другого запитання полягає в тому, що за сукупністю усіх завдань для МО України та ГШ ЗС України не акцентовано завдання відбиття (відсічі) воєнної агресії у кіберпросторі. Це видно із того, що поставлено завдання з підготовки держави до кібероборони, розвідувальної діяльності у кіберпросторі, військової співпраці щодо спільного захисту від кіберзагроз та забезпечення кіберзахисту інформаційної інфраструктури в умовах надзвичайного і воєнного стану. Якщо завдання щодо підготовки держави до кібероборони (до речі, включає і розвідувальну діяльність, і військову співпрацю), зрозуміти ще можливо, то наступне: розвідувальна діяльність, військова співпраця та кіберзахист інформаційної інфраструктури не забезпечують виконання у повному обсязі завдання відсічі воєнної агресії у кіберпросторі. Отже, завдання щодо відсічі воєнної агресії у кіберпросторі в цьому Законі необхідно конкретизувати.

Друга частина другого запитання полягає в суперечливості того, що відповідно до [2] ГУР МО України як його структурний орган має здійснювати розвідувальну діяльність за усім спектром питань кібербезпеки, в той час як МО України (отже і його структурним підрозділам) [1] таке завдання не ставиться, а лише в частині цього спектру, що стосується питання кібероборони. Звідси виникає необхідність усунення суперечності шляхом уточнення статті 9 Закону України [2].

Наведені неоднозначності мають бути усунені шляхом уточнення цього положення в [1] та інших законодавчих актах. А до усього вищезазначеного стосовно вже проведених в системі МО України організаційних заходів з кібероборони, як важливої складової забезпечення кібербезпеки держави, виникає питання щодо місця та ролі у цьому процесі розвідувального органу МО України – сьогодні цей орган, відповідно до чинної нормативно-правової бази, залишився поза системою кібероборони, оскільки, відповідно до змісту Доктрини [9], здійснення кіберрозвідки, кібердорозвідки та оцінки обстановки в кіберпросторі, всупереч положенням [2], покладено на Війська зв’язку та кібербезпеки ЗС України.

Література

1. Закон України “Про основні засади забезпечення кібербезпеки України” від 5 жовтня 2017 року № 2163-VIII // [Електронний ресурс]. – Режим доступу: http: // zakon2.rada.gov.ua.

2. Закон України “Про розвідку” від 17 вересня 2020 року № 912-IX // [Електронний ресурс]. – Режим доступу: http: // zakon.rada.gov.ua.

3. Закон України “Про правовий режим надзвичайного стану” від 16

березня 2000 року № 550-III // [Електронний ресурс]. – Режим доступу: http: // zakon.rada.gov.ua.

4. Закон України “Про оборону України” від 6 грудня 1991 року № 1933-XII (зі змінами) // [Електронний ресурс]. – Режим доступу: http: // zakon.rada.gov.ua.

5. Стратегічний оборонний бюлетень України: Указ Президента України від 17 вересня 2021 року № 473/2021 Про рішення РНБО України від 20 травня 2021 року “Про Стратегічний оборонний бюлетень України” // [Електронний ресурс]. – Режим доступу: http: // president.gov.ua.

6. Закон України “Про Збройні Сили України” від 6 грудня 1991 року № 1934-XII (зі змінами) // [Електронний ресурс]. – Режим доступу: http: // zakon.rada.gov.ua.

7. Стратегія кібербезпеки України: Указ Президента України від 26 серпня 2021 року № 447/2021 Про рішення РНБО України від 14 травня 2021 року “Про Стратегію кібербезпеки України” // [Електронний ресурс]. – Режим доступу: http: // president.gov.ua.

8. Указ Президента України від 26 серпня 2021 року № 446/2021 Про рішення РНБО України від 14 травня 2021 року “Про невідкладні заходи з кібероборони держави” // [Електронний ресурс]. – Режим доступу: http: // president.gov.ua.

9. ВКП 6-00(01).01. Доктрина Військ зв’язку та кібербезпеки Збройних Сил України. – К.: ГШ ЗСУ, 2021. – 52 с.

Сичов О.Л.
Національний університет оборони України імені Івана Черняховського

АНАЛІЗ УМОВ, ЯКІ ФОРМУЮТЬ ПСИХОЛОГІЧНИЙ СТАН ЦІЛЬОВОЇ АУДИТОРІЇ

Аналіз більшості наукових праць, у яких досліджуються проблеми психологічного стану цільової аудиторії, свідчить про відсутність єдиних підходів до базових категорій. Так, В.Алещенко вважає, що взаємопов’язаними сторонами морального духу є морально-психологічний потенціал і морально-психологічний стан [1]; у методиці розрахунку морально-психологічного стану військового підрозділу на основі експертних оцінок П.Криворучка, О.Хміляра, Р.Шпака, С.Василенка стверджується, що моральний дух є фактором морально-психологічного стану; В.Кліменко у структурі морально-психологічного стану вбачає тісний взаємозв’язок трьох складників: моралі, духу та енергопотенціалу, які у сукупності є критеріями психічного здоров’я особистості; за підходами Ю.Московчука, морально-психологічний стан є узагальненою формою вияву

політичної і духовної свідомості військовослужбовців, їх морально-психологічної стійкості; М.Варій вважає, що морально-психологічний стан – це цілісне, визначальне морально-психологічне явище, яке є похідним від інтегрованої єдності і взаємодії духовних, моральних, морально-психологічних, політичних, національних, соціальних, економічних, військово-службових, навчально-бойових (у воєнний час бойових), інших соціально-психологічних і психологічних чинників, які інтеграційно відображаються в їх соціальній психіці у вигляді певних морально-психологічних стереотипів, що спрямовують його діяльність і поведінку; Г. Давидов доводить необхідність дослідження політико-морального стану та морально-психологічного стану особового складу.

Сукупною сутністю цих розбіжностей є показник взаємовідношення змісту та логічного обсягу категорій “моральний дух” і “морально-психологічний стан”. Виходячи із наведеного сутність проблеми можна виразити через три твердження:

перше – морально-психологічний стан є складником морального духу, тобто зміст категорії “морально-психологічний стан” є частиною змісту “морального духу”, а логічний обсяг першої категорії повністю входить у логічний обсяг другої категорії [1];

друге – моральний дух є складником морально-психологічного стану, тобто зміст категорії “моральний дух” є частиною змісту категорії “морально-психологічний стан”, а логічний обсяг першої категорії повністю входить до логічного обсягу другої категорії;

третє – “моральний дух” і “морально-психологічний стан” є категоріями супідрядними;

будучи однаково загальними, вони підпорядковані більш спільній родовій категорії – “людському фактору”. Супідрядні категорії “моральний дух” і “морально-психологічний стан” – це види однієї родової категорії “людський фактор”, у них спільні родові ознаки, але видові ознаки різні [2].

Другий закон логіки не припускає логічного протиріччя у будь-якому правильному мисленні.

Закон протиріччя формулює це так: не можуть бути одночасно правдивими два несумісні висловлювання – два протилежні твердження і заперечення – про один і той же самий предмет у одному й тому ж відношенні; одне із них буде обов’язково неправдивим [3], а ми маємо протилежних тверджень три.

Логічний аналіз, наукові дослідження та практичний досвід найбільше свідчать про правильність третього твердження.

Методологічною основою для класифікації морального духу і морально-психологічного стану як складників людського фактора є філософське положення про взаємозв’язані раціональний і чуттєвий рівні психіки людини.

На користь висновку про правильність третього твердження свідчить дослідження філософсько-етимологічної сутності поняття “дух”, яке є ключовим у словосполученні моральний дух, і поняття “психіка” у словосполученні

“морально-психологічний стан”.

У словнику С. Ожегова поняття “дух” визначається як психічні здібності (свідомість, мислення), те, що спонукає до дій, до діяльності, начало, яке визначає поведінку, дію, а поняття “психіка” – там само тлумачиться як сукупність душевних переживань, як відображення у свідомості об’єктивної дійсності, душевний склад, властивий кому-небудь.

Свідомість – це вища, властива лише людині форма відображення об’єктивної дійсності. Отже, свідомість людини – це форма відображення об’єктивної дійсності; моральний дух є вираженням раціонального рівня свідомості людини; морально-психологічний стан є вираженням чуттєвого рівня свідомості людини.

Моральний дух разом з морально-психологічним станом виступають як видові категорії у відношенні до родової категорії – “людський фактор”.

Правильність третього твердження доводить практичний досвід. У другій половині 80-х років відомий військовий психолог Г. А. Давидов у процесі оцінювання людського фактора військових формувань використовував категорії “політико-моральний стан” і “морально-психологічний стан”. Він висловлював думку, що політико-моральний стан армії і флоту – це сукупність політичних і моральних ідей, почуттів, якими сповнені військовослужбовці, що визначають їх ставлення до інтересів Батьківщини, народу, соціально-політичного ладу, а під час війни виражають ставлення до її цілей.

До компонентів політико-морального стану він відносив: ідейно-політичну єдність особового складу військ; рівень організованості у військових частинах і підрозділах, рівень керівництва ними; військово-бойову підготовку особового складу; соціально-політичну освіченість керівного складу.

На побутовому рівні під категорію “політико-моральний стан” усі розуміли категорію “моральний дух”, але у науковій та методичній літературі ця категорія не вживалась. У ті часи на підставі ідеологічних міркувань сутність поняття “дух” визначалася лише на основі релігійно-містичних уявлень – безтілесна, надприродна істота, і наукові роботи не могли мати положень, що навіть опосередковано суперечили б офіційним атеїстичним підходам.

Після перемоги демократичних засад (на початку 90-х років) було оголошено нову тезу – військові формування поза політикою, який за сутністю означає, що силові структури мають бути поза впливом політичних партій, а військовослужбовці не можуть бути членами політичних партій. Закономірно, категорія “політико-моральний стан”, у складі якої є поняття політика, набула “невизнавального” статусу. Про категорію забули, але явища, які вона узагальнювала, залишилися. Змістовні фактори категорії “політико-моральний стан” перенесли до змісту категорії “морально-психологічний стан”, а згодом конкретні їх ознаки, що характеризували ідейні переконання, політичну свідомість.

Таким чином, системний підхід до проведеного дослідження та закони

формальної логіки дають право зробити висновок, що моральний дух і психологічний стан є складовими запланованої поведінки цільової аудиторії і вимагають самостійних підходів до визначення сутності, змісту та оцінювання.

Література

1. Московчук Ю.А. Методика оцінки морально-психологічного стану частин і підрозділів Збройних сил України / Ю. А. Московчук. – Вінниця: ВПСУ, 1997. – 23 с.
2. Ожегов С. И. Словарь русского языка / С. И. Ожегов. – [изд. 8-е]. – М. : Сов. энцикл., 1970. – 900 с.
3. Пелещишин А. М. Процеси управління інтерактивними соціальними комунікаціями в умовах розвитку інформаційного суспільства : монографія / Ю.О. Сєров, О.Л. Березко, О.П. Пелещишин, О.Ю. Тимовчак-Максимець, О.В. Марковець; за заг. ред. А.М. Пелещишина. – Львів : Видавництво Львівської політехніки, 2012. – 368 с.

Сіманський Д.А.
НУОУ ім. І. Черняховського

НЕОБХІДНІСТЬ ІНТЕНСИФІКАЦІЇ КОМУНІКАЦІЙНИХ ВПЛИВІВ НА НАСЕЛЕННЯ ТИМЧАСОВО ОКУПОВАНИХ ТЕРИТОРІЙ ПІД ЧАС МАСШТАБНИХ БОЙОВИХ ДІЙ У ХОДІ ДЕОКУПАЦІЇ

Сьогодні, напередодні широкомасштабного контрнаступу Збройних Сил України, ще більш актуальною стає проблема підсилення комунікаційних впливів держави на населення тимчасово окупованих територій (надалі – ТОТ) у процесі їх деокупації та подальшої реінтеграції.

Адже нині наявний цілий комплекс проблем: 1. Тривала відірваність населення ТОТ від джерел об’єктивної проукраїнської інформації. 2. Обмеження доступу до мережі Інтернет та соціальних мереж (Фейсбуку зокрема). 3. Пропагандистські впливи російської комунікації, у першу чергу – засобів масової інформації країни-агресора. 4. Репресії окупаційної влади проти усього населення і, особливо, проти проукраїнської його частини. 5. Погіршення рівня життя населення ТОТ. 6 Інтенсифікація бойових дій та наближення лінії фронту до дедалі більшої кількості населення тимчасово окупованих територій і значно посилений психологічний тиск на людей.

З абсолютною впевненістю можна стверджувати, що країна-агресор веде проти України на тимчасово окупованих територіях консцієнтальну війну – війну на ураження свідомості та зміну самоідентифікації людей. Яскраве підтвердження злочинних впливів такої діяльності окупантів – ордер на арешт російського

президента путіна за звинуваченням саме у викраденні дітей з метою подальшої їх «індоктринації». Особливо потужні прояви ми спостерігаємо в тимчасово окупованому 9 років Криму – коли населенню нашого півострову систематично нав'язують російські наративи і одночасно збільшується масштаб політичних репресій проти незгодних за, часто вигаданими, кримінальними справами.

Наближення часу деокупації та реінтеграції тимчасово окупованих територій нашої країни також ставить перед інститутами комунікації серйозні виклики – починаючи від суттєвих коректив у Стратегії деокупації Криму [1] і до відсутності стратегії деокупації Донбасу. У сучасні інформаційній війні перемагає той, хто швидше наповнює необхідним контентом інформаційний простір, у якому перебуває визначена цільова аудиторія. Для України ефективна комунікація з населенням деокупованих територій - це питання остаточної перемоги у війні та подальшого виживання як країни. Ключові рішення, які треба використати в стратегічній комунікації: а) поєднання новітніх інструментів комунікації (як от наприклад інформування в Дії) з надзвичайно традиційними (друковані газети та листівки наприклад); б) ефективна взаємодія, командна співпраця усіх інститутів влади, місцевих громад, правоохоронних органів, організацій громадянського суспільства, міжнародних організацій; в) лідерство Збройних Сил України в ефективній комунікації у час активних бойових дій та деокупації [2]; г) захист військовослужбовців Сил оборони України від інформаційно-психологічних впливів противника в часі активних бойових дій та деокупації й реінтеграції нашої країни.

Як зазначено в Наказі Головнокомандувача ЗСУ №70 від 18.03.2023 року: «Організація стратегічних комунікацій Збройних Сил України здійснюється шляхом формалізації завдань, оцінювання цільових авдиторій, визначення форм та способів реалізації стратегічних комунікацій, необхідних сил та засобів, порядку їх використання, організації управління, взаємодії та забезпечення (п.8)» [3]. Очевидно, що Збройні Сили України будуть ключовою комунікаційною інституцією в процесі деокупації та подальшої реінтеграції ТОТ.

Окремо варто виділити швидкість (вчасність) комунікації та охоплення цільової авдиторії, масштаб комунікації. Існують дві серйозні проблеми, які стоять на перешкоді побудові ефективної комунікації на деокупованих територіях: атомізація суспільства в умовах війни та окупації й руйнація традиційних для ЦА каналів комунікації (перше що робили окупанти на захоплених територіях – руйнували ретрансляційні вежі та мобільний зв'язок) .

Відтак комунікаційні впливи України на населення тимчасово окупованих територій і, в подальшому, деокупованих територій мають бути вчасними, швидкими, всеохоплюючими та скоординованими. Для цього потрібне планування , взаємодія та делегування завдань на підставі спроможностей . Цьому сприятиме стратегічний підхід до комунікації , розробка наративів та меседжів комунікаційними групами вищого порядку, синхронізація та уніфікація (принцип

«ван войс» [4].) інформаційних впливів на центральному рівні та їх інтерпретація (збагачення різноманіттям)на місцевих рівнях відповідно до запитів цільових авдиторій.

Такий спосіб здійснення комунікації, стратегічний за своє суттю, зможе значно наблизити деокупацію тимчасово окупованих територій України та пришвидшити їх реінтеграцію в майбутньому.

Література

1. Президент затвердив Стратегію деокупації та реінтеграції тимчасово окупованого Криму — Офіційне інтернет-представництво Президента України (president.gov.ua). УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №117/2021 — Офіційне інтернет-представництво Президента України (president.gov.ua)

2. Віллінк Дж., Бебін Л. Абсолютна відповідальність. Уроки лідерства від «морських котиків». – Київ, 2020. – С. 229, 268.

3. Наказ Головнокомандувача Збройних Сил України № 70 від 18.03.2023 року «Про затвердження Порядку здійснення стратегічних комунікацій Збройних Сил України»

4. Інтерньюз-Україна. «Курс стратегічних комунікацій» Лекція 4. Основні елементи стратегічної комунікації (culturepartnership.eu) Київ, 2020. –лекція 4.

Скіцько О.І.
к.т.н., с.н.с.,
Національна академія України

КРИПТОРЕГУЛЯЦІЯ ТА ЇЇ СТАН В УКРАЇНІ

Стрімкий розвиток інформаційних систем та технологій як у світі так і в України засвідчує їх широке застосування в різних сферах діяльності суспільства. Обсяг електронних інформаційних ресурсів збільшується, а технології їх обробки постійно еволюціонують. Служба безпеки України має враховувати перспективи розвитку сучасних технологій при побудові системи контррозвідувального захисту електронних інформаційних ресурсів [1].

В останні роки значно популяризується блокчейн, що підштовхнуло уряди по всьому світу до прийняття чи розгляду нормативної бази для контролю крипто валют.

В даний час правила регулювання криптовалют варіюються від країни до країни. В одних державах криптовалюти заборонені повністю, в інших – дозволені, але діють обмеження. У більшості країн криптовалюти підпадають під вимоги щодо боротьби з відмиванням грошей (anti money laundering - AML).

Регулювання криптовалют у світі:

- регіони ОАЕ - активно працюють над залученням криптовалютних компаній і вже завоювали репутацію центру криптовалют та блокчейн-технологій у регіоні Перської затоки. Один із кроків, зроблених Еміратами, навіть включав запуск стратегії Dubai Metaverse Strategy. Крім сприятливих умов, запропонованих компаніям, Дубай сприяє загальному поширенню криптовалюти. У криптобіржі, такій як Sell Bitcoin in Dubai (SBID), будь-який бажаючий може купити та продати BTC, ETH, USDT та інші криптовалюти за готівку. Також є можливість оплачувати нерухомість у криптовалюті. Крім того, у вільних зонах Емірату діє нульовий відсоток податку на доходи фізичних осіб і це звільнення також поширюється на криптовалюту та будь-які операції з нею, такі як торгівля, ставки, фармінг та інше.

- серед країн Латинської Америки Сальвадор виділяється тим, що першим у світі запровадив BTC як законний платіжний засіб ще в 2021 році, а також звільнив іноземних інвесторів від сплати податків і випустив публічний додаток цифрового гаманця.

- США, криптовалюта регулюється державними органами на федеральному рівні - "Мережею боротьби з фінансовими злочинами (FinCEN)", "Комісією з цінних паперів і бірж США (SEC)" і "Комісією з торгівлі товарними ф'ючерсами (CFTC)", а також місцевими регуляторами на рівні штатів, де розбіжності стосуються переважно питань ліцензування. Податки залежать від суми зароблені криптовалюти та можуть досягати 37% на короткостроковий приріст капіталу.

- що стосується Європейського союзу, то загалом криптовалюти оподатковуються на прибуток, але ставка варіюється від країни до країни. Біржі мають бути зареєстровані лише в деяких країнах-членах ЄС, але зазвичай застосовується законодавство ЄС щодо боротьби з відмиванням грошей. Щоб вирішити проблеми скамів у 2024 році “Європейська рада” має намір запровадити закон про ринки криптоактивів (MiCA) як частину ширшого закону про цифрову операційну стійкість (DORA). Як і в Дубаї, майбутнє регулювання спрямоване на боротьбу з анонімним обігом монет. MiCA вимагає, щоб торгові платформи працювали лише з тими активами, чиї власники та історія транзакцій можуть бути перевірені.

У 2022 році Україна опинилась у трійці світових лідерів з використання криптовалюти. Міністерством цифрової трансформації України був розроблений профільний закон "Про віртуальні активи" та він не набрав чинності. Цей закон мав регулювати правовідносини, що виникають у зв’язку з оборотом віртуальних активів в Україні, визначати права та обов’язки учасників ринку віртуальних активів, засади державної політики у сфері обороту віртуальних активів [2].

Висновок: питання регулювання криптовалюти а також технології, пов'язані з криптовалютами уряди деяких країн намагаються впровадити у фінансові послуги та скористатися перевагами зростаючого сектора, відкриваючи консультації для

отримання коментарів щодо пропозицій щодо регулювання. Хоча деякі пропозиції ще перебувають на розгляді, вже було зроблено кроки, спрямовані на покращення захисту роздрібних інвесторів чи просто запровадження додаткових обмежень. Одним з основних напрямків залишається те, як біржі керують своїми активами, щоб уникнути їхнього змішування з активами клієнтів. Однак, у нових законах та проектах особлива увага приділяється також стейблкоїнам, ставкам та кредитуванню.

Література

1. Куліковський А.В. Технологія Blockchain як складова інформаційної безпеки/ А. Куліковський // Кібербезпека: освіта, наука, техніка. 2019, № 4. С. 85-89.

2. Про віртуальні активи: Закон України від 17.02.2022 р. № 2074-IX : URL: https://zakon.rada.gov.ua/laws/show/2074-20#Text (дата звернення: 19.03.2023).

Скрипнюк О.В.
д.ю.н.,
академік НАПрН України, заслужений юрист України
директор Інституту держави і права
імені В.М. Корецького НАН України,

ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ В УМОВАХ ВІЙНИ: ВИКЛИКИ І ЗАВДАННЯ

Використання сучасних засобів і технологій, інформаційно-комунікаційних систем спричинюють разом з тим передумови витоку інформації, потенційні можливості несанкціонованого доступу до персональних даних, до різноманітних інформаційних ресурсів чи будь-якої стратегічної інформаційно-технічної інфраструктури, поширення недостовірних відомостей, цілеспрямований деструктивний інформаційно-психологічний вплив на окрему особу чи групу населення з метою формування певної громадської думки, маніпулювання нею тощо, зумовлюють вразливість загальної системи безпеки.

Складні реалії існуючих перед Україною на нинішньому етапі державотворення новітніх викликів та загроз, пов’язаних, зокрема зі збереженням єдності і цілісності держави, недоторканності кордонів та її територіальної цілісності, зміцненням державного суверенітету, спричинених насамперед російською широкомасштабною агресією проти нашої держави, надзвичайно загострюють питання інформаційної безпеки як складової забезпечення національної безпеки.

Конституція України забезпечення інформаційної безпеки країни визначає однією з найважливіших функцій держави, справою всього українського народу (ст.17 Основного Закону). Держава конституційно зобов'язана забезпечувати в межах наявних у неї засобів право на інформацію та ще низки визначених прав людини і громадянина в інформаційній сфері (ст.ст.3, 31, 32,34, 50 тощо) та гарантувати відповідний рівень інформаційної безпеки людини, суспільства в цілому.

У контексті реалізації прагнень європейської та євроатлантичної інтеграції, зокрема імплементовано безпекові положення Угоди про асоціацію між Україною та Європейським Союзом [1]. Розроблений і ухвалений за участі міжнародних експертів Закон України «Про національну безпеку України» від 21.06.2018 р., № 2469-VIII (поточна редакція — від 15.06.2022 р.), визначив (ст.3 закону), що державна політика у сферах національної безпеки і оборони спрямовується , разом з іншими її напрямами, на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, безпеки критичної інфраструктури, кібербезпеки України. Інформаційне середовище є одним із її об'єктів [2].

Інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки України і складним, різновекторним динамічним явищем: її різновидами є безпека людини, держави і суспільства в цілому. Така системність у свій час була закладена Законом України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» від 9.01.2007 р. 2007, № 537-V, за яким інформаційна безпека – це стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації (р.III, п.10 Закону).

На сьогодні інститут інформаційної безпеки разом із конституційними нормами, нормами відповідних міжнародно-правових актів складають положення, окрім вже названих, законів України: «Про інформацію», «Про державну таємницю», «Про доступ до публічної інформації», «Про основні засади забезпечення кібербезпеки України», «Про захист персональних даних»; а також чинного законодавства про Національну програму інформатизації, інформацію з обмеженим доступом тощо; підзаконних нормативно-правових актів (спеціальних актів Президента України, Уряду України, рішень Ради національної безпеки і оборони України, інших спеціальноуповноважених суб'єктів у вказаній сфері) стратегічних декларативних документів: доктрин, концепцій, стратегій, як в інформаційній, так і воєнній, екологічній, науково-технологічній та інших сферах, розроблених та затверджених переважно у мирний період. Окремо слід

наголосити на документах концептуального характеру, прийнятих за останні роки: Стратегії національної безпеки України [3], Стратегії кібербезпеки, затвердженої Указом Президента України від 15.03.2016 р. №96/2016 [4] та Стратегії кібербезпеки:безпечний кіберпростір – запорука успішного розвитку країни, затвердженої Указом Президента України від 26.08.2021 р., № 447/2021 [5].

Водночас, національне законодавство з інформаційної безпеки потребує подальшого узгодження з існуючими міжнародно-правовими актами загального та регіонального рівнів, імплементації існуючих міжнародно-правових стандартів у законодавство і практику його реалізації.

Як складову частину національної безпеки, будучи відображенням об'єктивної реальності, інформаційну безпеку визначила, зокрема, Стратегія інформаційної безпеки (надалі Стратегія), затверджена Указом України Президента України від 28.12.2021 р., реалізація якої була розрахована на період до 2025 р.

Зміст досліджуваного явища як стану захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом [6].

Відомо, що питання реалізації державної інформаційної політики, в тому числі у сфері інформаційної безпеки, досить вагомі доктринальні основи яких були сформовані за період незалежності, а також щодо відсутності системного і комплексного підходу до її нормативно-правового забезпечення, до прогнозування зовнішніх та внутрішніх загроз її національній безпеці, вироблення стратегії входження українського суспільства у світовий інформаційний простір тощо постійно були предметом обговорення вітчизняних науковців, практиків.

Вони наголошували, що забезпечення інформаційної безпеки в Україні завжди було актуальною для практики, однак, за переконання аналітіків, її реалізація не була системною.

Зокрема, організаційну систему забезпечення інформаційної безпеки - складової загальної системи національної безпеки України - відповідно до конкретних повноважень складає ціла низка органів публічної влади, спеціально уповноважених державних органів та установ, недержавних структур, інститутів громадянського суспільства (Верховна Рада України; Президент України; Рада національної безпеки і оборони України; Кабінет Міністрів України; Міністерство закордонних справ України; Міністерство оборони України; Міністерство

внутрішніх справ України, Міністерство культури та інформполітики, Національна рада України з питань телебачення і радіомовлення; Служба безпеки України, Служба зовнішньої розвідки України, Національний інститут стратегічних досліджень та ін.).

Втім, аналізуючи їх діяльність щодо здійснення державної інформаційної політики перед широкомасштабним російським вторгненням на територію нашої держави, спеціалісти зазначають, що проблема полягає в тому, що кожен із державних органів, які беруть участь у забезпеченні інформаційної безпеки України відповідає за свій сегмент і жоден, не відповідає за загальний стан протидії інформаційній агресії через відсутність суб'єкта юридичної координації зусиль забезпечення національної безпеки в інформаційній сфері [7].

Слід наголосити, що фахівці наполягають на висновку про неготовність держави, особливо на першій фазі російсько-української війни до інформаційного протистояння зовнішньополітичному впливу її спеціальноуповноважених органів з об'єктивних та суб'єктивних причин, до протидії сучасним викликам і названій сфері. Системна діяльність відповідних органів має бути спрямовувана на виконання конкретних завдань у сфері національної бепеки, надання належних умов для реалізації забезпечення інформаційної безпеки України.

Актуальними й нині залишаються основні стратегічні цілі забезпечення інформаційної безпеки України, визначені згаданою вже Стратегією, це, зокрема: протидія дезінформації та інформаційним операціям, насамперед держави-агресора, спрямованим, серед іншого, на ліквідацію незалежності України, повалення конституційного ладу, порушення суверенітету і територіальної цілісності держави, пропаганду війни, насильства, жорстокості, розпалювання національної, міжетнічної, расової, релігійної ворожнечі та ненависті, вчинення терористичних актів, посягання на права і свободи людини; забезпечення всебічного розвитку української культури та утвердження української громадянської ідентичності; підвищення рівня медіакультури та медіаграмотності суспільства; забезпечення дотримання прав особи на збирання, зберігання, використання та поширення інформації, свободу вираження своїх поглядів і переконань, захист приватного життя, доступ до об'єктивної та достовірної інформації, а також забезпечення захисту прав журналістів, гарантування їх безпеки під час виконання професійних обов'язків, протидія поширенню незаконного контенту; інформаційна реінтеграція громадян України, які проживають на тимчасово окупованих територіях та на прилеглих до них територіях України, до загальноукраїнського інформаційного простору, а також відновлення їх права на інформацію, що дає їм змогу підтримувати зв'язок з Україною, тощо.

Сьогодні, коли Україна активізує зусилля у безпековому та оборонному секторах, об'єктивна реальність така, що, наприклад, гарантування державою конституційних прав і свобод людини в повному об'ємі унеможливлюється, через

існуючі загрози, спрямовані проти існування самої держави, її громадян.

Інформаційні права та свободи людини і громадянина (зокрема, право кожного на гарантувану таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції; право кожного на невтручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України; право кожного на свободу думки і слова, на вільне вираження своїх поглядів і переконань, право на інформацію) також належать до прав, які можуть обмежуватися на період дії правового режиму воєнного стану в Україні. Водночас, забезпечення інформаційної безпеки полягає у створенні механізму, який би водночас максимально ефективно виконував поставленні завдання в контексті інформаційних обмежень та сприяв захисту прав і свобод громадян [8].

В умовах технологій інформаційної війни, коли мас-медіа, соціальні мережі є ефективною зброєю, яка використовується в сучасних гібридних війнах, має очевидний агресивний характер, спрямована на маніпулювання свідомістю населення, дестабілізацію ситуації в різних регіонах України, дискримінацію органів публічної влади тощо, не слід забувати про відносно невисокий рівень медіа-грамотності та медіа-культури в суспільстві, що негативним чином відображається на медіасоціалізації різних верств населення.

Зокрема, Стратегія інформаційної безпеки, визначаючи глобальні та національні виклики та загрози інформаційній безпеці, назвала серед таких вплив соціальних мереж на внутрішню і зовнішню суспільно-політичну ситуацію, стан додержання прав і свобод людини; недостатній рівень медіаграмотності (медіакультури), що, разом з тим, супроводжується некритичністю сприйняття інформації, створює підґрунтя для можливих маніпуляцій громадською думкою тощо.

Нині метою державної інформаційної політики має стати не тільки забезпечення інформаційної безпеки, національної безпеки в цілому, а й, зокрема, здійснення комплексу заходів для формування іміджу держави, її інститутів як у національному, так і у міжнародному інформаційних просторах, для однозначного розуміння пріоритетів державної інформаційної політики громадянами України, населенням на тимчасово окупованих територіях, міжнародною спільнотою. Зокрема, йдеться про поширення якісного інформаційного продукту (контенту), спрямованого на формування та зміцнення національної свідомості з метою консолідації суспільства та вироблення імунітету до ворожих інформаційних впливів. Якісна державна політика здатна посприяти тактичним і стратегічним перемогам.

Література

1. Про ратифікацію Угоди про асоціацію між Україною, з однієї сторони, та Європейським, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони України: Закон України від 16.09.2014, №

1678-УП Відомості Верховної Ради України. 2014. № 40. Ст.2021.

2. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

3. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 р. «Про Стратегію забезпечення державної безпеки» : Указ Президента України від 16.02.2022 р. № 56/2022. URL: https://zakon.rada.gov.ua/laws/show/56/2022#Text

4. Стратегія кібербезпеки України : Указ Президента України від 15.03.2016 р. № 96/2016. URL: https://www.president.gov.ua/documents/962016-19836

5. Стратегія кібербезпеки України: Указ Президента України від 26.08.2021 р. № 447/2021 URL: https://www.president.gov.ua/documents/4472021-40013

6. Про рішення Ради національної безпеки і оборони України від 15.10.2021 р. «Про Стратегію інформаційної безпеки»: Указ Президента України від 28.12.2021 р. №685/2021 URL: https://zakon.rada.gov.ua/laws/show/685/2021#n5

7. Дмитренко М. А. Проблемні питання інформаційної політики України та шляхи їхнього вирішення. Інформаційна безпека: сучасний стан, проблеми та перспективи: матеріали наук.-практич. конф. (м.Київ, 20.09.2019 р. Київ : НТУ України «Київський політехнічний інститут імені Ігоря Сікорського». Політехніка. 2019. URL: Конф інформбезпека.pdf

8. Котерлін І. Б. Інформаційна безпека в умовах воєнного стану у аспекті забезпечення інформаційних прав і свобод. Актуальні проблеми вітчизняної юриспруденції. 2022, № 1. URL: http://apnl.dnu.in.ua/1_2022/25.pdf

Сніцаренко П.М.
д.т.н., с.н.с.,
Передрій О.В.
к.військ.н., старший дослідник
Гордійчук В.В.
к.т.н., старший дослідник
Грицюк В.В.
д.філос.,
Національний університет оборони України імені Івана Черняховського

УДОСКОНАЛЕННЯ МЕТОДИЧНОГО ПІДХОДУ ДО АВТОМАТИЗОВАНОЇ КЛАСИФІКАЦІЇ ІНФОРМАЦІЙНИХ ПОДІЙ

В передових у воєнному відношенні державах світу останнім часом накопичено значний науковий, технічний та практичний досвід проведення інформаційних операцій, акцій, атак і актів при вирішенні завдань у ході воєнних конфліктів, коли об’єктами інформаційного впливу, зокрема, його різновиду – інформаційно-психологічного впливу, є особовий склад збройних сил (військових

формувань) противника. Особливої важливості для України ця обставина набула напередодні та в період воєнної агресії проти неї з боку Російської Федерації, коли гостро та відчутно проявилися наслідки зовнішнього негативного інформаційно-психологічного впливу на особовий склад Збройних Сил України (далі ЗС України). Ця обставина викликає потребу активної протидії.

Така протидія потребує реалізації системи управління протидією на основі своєчасного виявлення та адекватної оцінки рівня такого впливу на визначену цільову аудиторію (ЗС України). Звідси випливає потреба розв'язання задачі підвищення оперативності та зниження трудомісткості процесу виявлення та кількісної оцінки рівня негативного інформаційного впливу на особовий склад ЗС України в інтересах проактивної протидії такому впливу шляхом автоматизації зазначених процесів.

Питання протидії негативному інформаційному впливу на особовий склад ЗС України розглядалося в працях вітчизняних науковців [1–4]. Аналіз показує, що на сьогодні теорія протидії такому впливу обмежена на рівні концептуально-декларативних положень, а тому для практики є недосконалою. У ній бракує чітких формальних методів і методик для кількісних оцінок певних аспектів цієї сфери, у тому числі щодо виявлення та оцінки рівня негативного інформаційно-психологічного впливу на особовий склад ЗС України. З цієї причини його кількісна оцінка не проводиться, а оцінка морально-психологічного стану ЗС України, який є наслідком, зокрема, і такого впливу, здійснюється за якісними показниками на основі результатів моніторингу у військових частинах і підрозділах відповідно діючих інструкцій [5], тобто вже після наслідків інформаційних впливів, про що йдеться в матеріалах оперативних звітів. Зазначене не дозволяє проводити випереджувальні заходи для підтримки морально-психологічного стану військ (сил), отже ефективно протидіяти такому впливу. Зважаючи на це, була розроблена та верифікована методика виявлення та оцінювання негативного інформаційно-психологічного впливу на особовий склад військ (сил) [6–8].

В той же час, організація та реалізація єдиної системи протидії з використанням зазначеної методики за кібернетичним принципом дії сьогодні є завданням малоперспективним. Однією із головних причин цього є практична неможливість запровадження підсистеми моніторингу інформаційних процесів в інформаційному просторі держави із-за потреби залучення для цього операторів моніторингу багатьох структурних підрозділів МО України та ЗС України, функції, завдання і можливості яких є дотичними до організації та проведення заходів такої протидії, яка має бути взаємно координована, про що наголошується, зокрема, в роботах [8, 9]. Але цього, на жаль, поки що не відбувається. З цієї причини система розбалансована, процеси неавтоматизовані, отже трудомісткі, оцінки інформаційних подій здійснюються не за кількісною мірою, а на якісному рівні. Це не дає змоги реалізації протидії такому негативному інформаційному

впливу як системного управлінського процесу, а заходи протидії не проводяться як випереджувальні.

В той же час, виходячи із сутності відомої методики [6–8] виявлення та оцінювання негативного інформаційно-психологічного впливу на особовий склад ЗС України, її автоматизація потребує реалізації процесу класифікації інформаційних подій за 22 класами та 17 підкласами [7]. Розгляд особливостей такого завдання показує, що його важко реалізувати прямими рішенням із-за великої складності виконання процесів розподілу по такому об'ємному числу класів та підкласів. Складність спричинена потребою формування та уточнення адекватного лінгвістичного критерію класифікації або їх сукупності, що ускладнює і сам процес автоматизації. З цього приводу виникає необхідність скорочення розмірності ознак лінгвістичного критерію.

Зауважимо, що в сучасній теорії військового управління ще не обґрунтовано належного науково-методичного апарату щодо забезпечення машинного відбору та класифікації інформаційних подій на основі лінгвістичних ознак, що характеризують тональність повідомлень (тексту), які можуть справляти негативний вплив на особовий склад ЗС України, незважаючи на те, що певні напрацювання науковців, зокрема українських, у цій проблематиці спостерігаються протягом останнього часу [10, 11].

Аналіз результатів статистичних даних, отриманих під час процесу перевірки адекватності методики (тобто її верифікації), який було проведено шляхом "ручного" моніторингу інформаційного простору держави [8], підтверджує стабільність розподілу за класами відносної величини рівня негативного впливу інформаційних подій (їх інтенсивності) упродовж усього періоду моніторингу. При цьому найбільш суттєвими щодо інтенсивності та ваги впливу є лише два класи, які слід об'єднати в єдиний клас (в зв'язку з високою кореляцією їх змісту, вага цих класів враховується порівну). Змістовність цих класів стосується насичення вітчизняного інформаційного простору продукцією для впливу на індивідуальну та масову свідомість особового складу національних військових формувань (з боку іноземних ЗМІ, провокативних національних ЗМІ, непатріотичної частини населення власної держави) з метою послаблення їх готовності до оборони держави та погіршення іміджу збройних сил.

Зважена інтенсивність деструктивного інформаційного процесу обох класів є домінуючою серед усіх класів зафіксованих інформаційних повідомлень, а отже найбільш визначальною (інформативною) в загальному процесі негативного впливу на особовий склад ЗС України за певний період часу. У кількісному вимірі середнє значення сумарної ваги інформаційних повідомлень деструктивного характеру, що належать до цього об'єднаного класу, складає приблизно 67 % від загальної ваги усіх негативних повідомлень. Частка інших 20 класів складає близько 33 %, тобто вони формують загальний стабільний негативний фон інформаційного впливу.

Таким чином, завдяки цим ознакам відому та верифіковану методику можна звести до необхідності виявлення та обчислення сумарної “ваги” впливу лише негативних повідомлень, що за змістом належать до цього єдиного класу, зі збільшенням обчисленої «ваги» на 33%. Це означає скорочення числа критеріїв відбору (класифікації) та звуження спектру лінгвістичних ознак, а відтак – полегшення реалізації відповідної процедури (алгоритму) автоматизації.

Література

1. Толубко В.Б. Концептуальні основи інформаційної безпеки України / В.Б. Толубко, С.Я. Жук, В.О. Косевцов // Наука і оборона. – 2004. – № 2. – С. 19-25.

2. Руснак І.С. Розвиток форм і способів ведення інформаційної боротьби на сучасному етапі / І.С. Руснак, В.М. Телелим // Наука і оборона. – 2000. – № 2. – С. 18-23.

3. Основи стратегії національної безпеки та оборони держави: підруч. / О.П. Дузь-Крятченко, Т.М. Дзюба, А.О. Рось, ін. – 2-ге вид., доп. і випр. – К.: НУОУ, 2010. – 591 с.

4. Інформаційно-психологічна боротьба у воєнній сфері: монографія / Г.В. Пєвцов, А.М. Гордієнко, С.В. Залкін, С.О. Сідченко, А.О. Феклістов, К.І. Хударковський. – Х.: Вид. Рожко С.Г., 2017. – 276 с.

5. Наказ ГШ ЗС України від 29.04.2017 № 153 “Про затвердження Інструкції з оцінювання морально-психологічного стану особового складу ЗС України” (зі змінами, внесеними наказом ГШ ЗС України від 16.08.2017 № 287).

6. Сніцаренко П.М. Методичний підхід до виявлення та оцінювання негативного інформаційно-психологічного впливу на особовий склад військ (сил) / П.М. Сніцаренко, Ю.О. Саричев, Ю.І. Міхєєв, М.В. Праута // Наука і оборона. – № 3-4. – 2017. – С.18-25.

7. Сніцаренко П.М. Підсистема моніторингу інформаційного простору як необхідна складова системи протидії негативному інформаційно – психологічному впливу на особовий склад Збройних Сил України / П.М. Сніцаренко, Ю.О. Саричев, В.А. Ткаченко, О.А. Мотузяник // Наука і оборона. – № 1. – 2018 р. – С. 29-33.

8. Сніцаренко П.М. Комплексна система протидії негативному інформаційно-психологічному впливу на особовий склад Збройних Сил України / П.М. Сніцаренко, Ю.О.Саричев, В.А.Ткаченко, Л.В.Хоменко // Наука і оборона. – № 2. – 2018. – С. 40-45.

9. Сніцаренко П.М. Аналіз стану виявлення та оцінки негативного інформаційного впливу на особовий склад ЗС України в системі протидії такому впливу / П.М. Сніцаренко, В.В. Грицюк // Збірник наукових праць ЦВСД НУОУ ім. І. Черняховського. – 2019. – № 2 (66). – С. 52-61.

10. Ланде Д.В., Субач І.Ю., Бояринова Ю.Є. Основи теорії і практики інтелектуального аналізу даних у сфері кібербезпеки: навчальний посібник. – К.:

ІСЗЗІ КПІ ім. Ігоря Сікорського», 2018. – 297 с.

11. Стрижак О.Є. Засоби онтологічної інтеграції і супроводу розподілених просторових та семантичних інформаційних ресурсів / Стрижак О.Є. // Екологічна безпека та природокористування. – вип. 12 – 2013. – С. 166-17

Сокол Є.І.
д.т.н., проф. ректор Національного технічного університету
Харківський політехнічний університет
Євсеєв С.П.
д.т.н., проф. завідувач кафедри кібербезпеки Національного технічного університету Харківський політехнічний університет

УПРОВАДЖЕННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ В ОСВІТНІЙ ПРОЦЕС: СУЧАСНІ РІШЕННЯ ТА ПЕРСПЕКТИВИ РОЗВИТКУ

Вступ. Інноваційна діяльність закладів вищої освіти (ЗВО) та формування підприємницьких університетів інноваційного типу є однією з форм інтеграції систем вищої освіти країн у світовий освітньо-науковий простір, підтримки їх конкурентоспроможності. На основі виділення спіралі взаємодії університетів з економікою і соціумом, розроблена еволюційна модель взаємодії університету зі стейкхолдерами. Розуміння нової місії університетів дозволило виділити домінанти діяльності інноваційно-активного університету (ІАУ), розробити схему взаємозв'язку процесів управління і його основних функцій. Сформовано авторське трактування ІАУ та передумови побудови корпоративної інформаційно-освітньої системи (КІОС). З огляду на синергізм і гібридність сучасних кіберзагроз, зростання цільових атак в освітній сфері запропонована Концепція безпеки, яка забезпечує протидію комплексованим гібридним загрозам на основі адаптивної системи захисту інформації (АСЗІ). Базисом електронного документообігу є цифровий підпис (ЦП) Центру сертифікації ключів (ЦСК) на основі технології Public Key Infrastructure. Такий підхід дозволяє забезпечити ефективний розподіл ресурсів КІОС університету, зростання іміджу університету, діджиталізацію та автоматизацію документообігу, поширення цифрових послуг, які надаються студентам, створення умов підвищення рейтингу університету за критеріями міжнародного рейтингу університетів світу Ranking Web of Universities (Webometrics).

Підґрунтя побудови інноваційно-активного університету. Сучасний етап еволюції світового господарства характеризується радикальними соціально-економічними трансформаціями та переходом країн – ключових інноваторів до економіки знань. Її основними атрибутами стають інтернаціоналізація освітньої та наукової діяльності, технологічні зрушення у сфері освіти і науки, диверсифікація

механізмів фінансування досліджень, які здійснюються університетами, загострення конкурентної боротьби між ними.

Формування сучасної європеїзованої системи вищої освіти в Україні розпочалося після проголошення незалежності у 1991 році. Діяльність ЗВО України регламентується законодавчо-нормативними актами, від яких повністю залежить як функціонування, так і можливості та напрям розвитку сфери вищої освіти. За роки незалежності України відбулися значні зміни та перетворення в діяльності ЗВО, що були викликані змінами в законодавчому полі та глобалізаційними процесами та мали спрямованість на досягнення світових освітніх стандартів. Пріоритетним завданням формування нової самостійної освітньої політики університетів України стало створення національної системи освіти як основи відтворення інтелектуального потенціалу населення, виходу вітчизняної науки, техніки і культури на світовий рівень, національного відродження, становлення державності та демократизації суспільства в Україні.

В цей час університети мають серйозну конкуренцію з боку установ, які надають в онлайн формі освітні та тренінгові послуги. Причиною виникнення таких установ, як правило, є відсутність ефективної взаємодії між університетами та організаціями-роботодавцями, споживачами фахівців з вищою освітою та, як наслідок, виникнення сталого міфу про певне старіння компетентностей, отриманих в університетах, від потреб реальних секторів економіки, державного управління та соціуму. Все це обумовлює необхідність адаптації університетів до нових умов, і, як зазначають Henry Eyring і Clayton Christensen, потребує зміни структури університетської ДНК зсередини на основі перманентних інновацій.

По суті, процеси, характерні для сучасного етапу розвитку вищої освіти у світі толерантні підприємницьким процесам, де будь-яка фірма чи організація, що існує у конкурентному середовищі, шукає ефективні стратегії, способи, інструменти отримання конкурентної переваги. Глибокі дослідження джерел конкурентоспроможності у підприємницької діяльності, проведені на початку XX століття, дозволили виділити як ключовий фактор інновації. У зв'язку з цим, інноваційно-активна діяльність будь-якої організації визначається як створення, пошук та використання можливостей для нових способів ведення справ, що призводять до покращення продуктів та послуг, систем та способів керівництва / управління людьми та організаціями.

Критичний аналіз нормативно-правової бази процесу функціонування вітчизняних ЗВО та їх трансформаційного розвитку дозволив виділити 4 основних етапи модифікації законодавства України в сфері вищої освіти. Еволюційний вектор трансформаційних перетворень наведено на рис. 1 [1, 2].

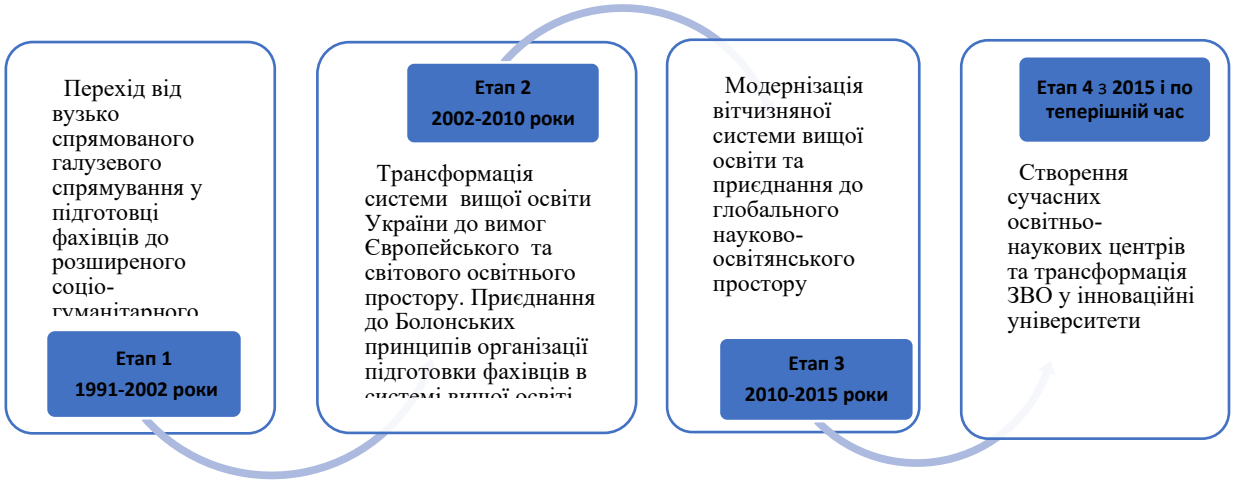


Рисунок 1 – Еволюційний вектор трансформації системи вищої освіти України

Отже, на початку XXI століття сформувалася нова парадигма розвитку університетів – університетів підприємницького типу, що у тому, що університети покликані служити суспільству передусім шляхом підтримки економіки та підвищення якості життя громадян. Нова парадигма докорінно змінює культуру відповідальності та систему цінностей університету, про що свідчить поширення управлінського підходу та використання принципу співвідношення ціни та якості у системах вищої освіти у всьому світі. Конкурентоспроможність та актуальність існування університету оцінюється, головним чином, відповідно до його внеску в економічний розвиток країн та людства в цілому. Щоб пристосуватися до нової парадигми, потрібна певна адаптація – адаптація відносин університету з навколишнім суспільством/основними стейкхолдерами, адаптація його внутрішніх процесів, основних цінностей, пошук нових інноваційних засад його розвитку за сучасних умов. На рис. 2 представлено взаємозв’язок процесів управління та основних функцій інноваційного університету з урахуванням розвитку е-освіти.

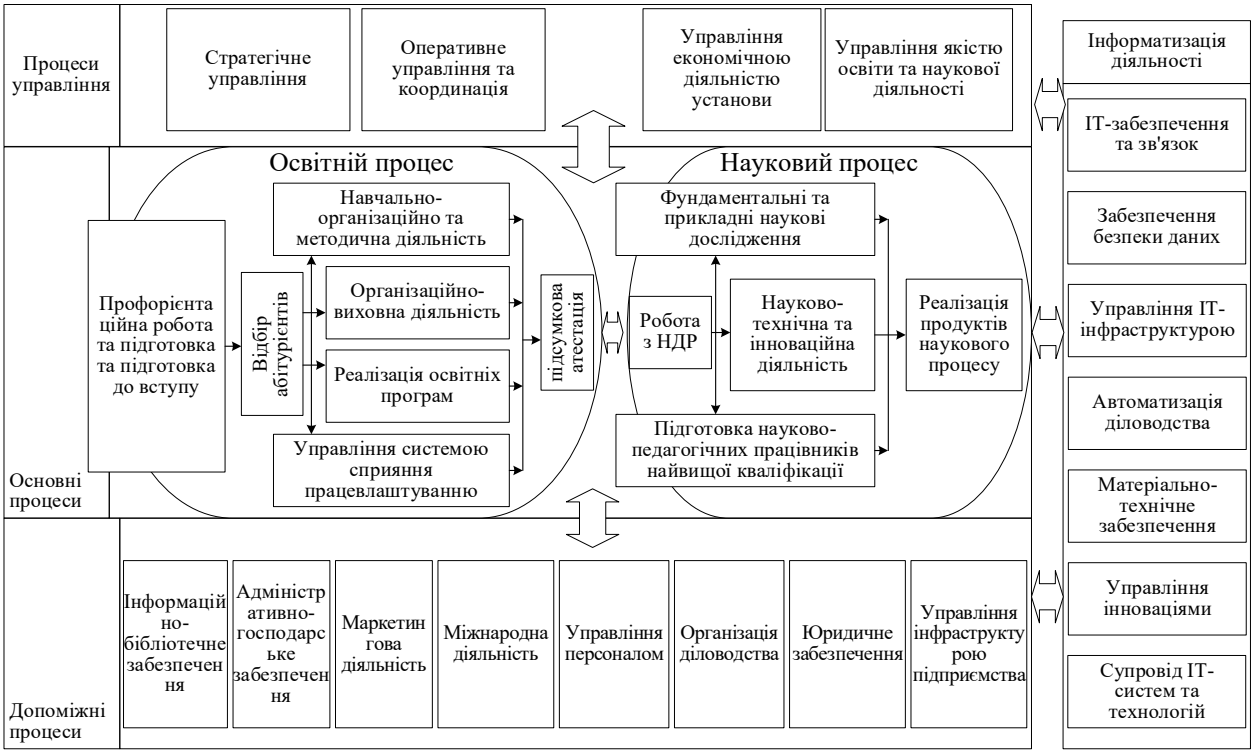


Рисунок 2 – Взаємозв’язок процесів управління та основних функцій інноваційного університету

В цей час існують два різні підходи до розуміння сутності підприємницького, інноваційно-активного університету1, 2].

Перший підхід трактує його як інститут, який робить все можливе для розвитку науки, винаходи нових технологій та стимулювання нових ринків та галузей, а підприємницький аспект діяльності університетів пов’язують виключно з бізнесом та комерціалізацією їхньої інтелектуальної власності. Ця думка значною мірою підкріплюється поглядами міжнародна спільнота (наприклад, організацією економічного співробітництва та розвитку (ОЕСР)), яке розглядає університети як джерела технологічних інновацій та “двигунів зростання”. При цьому критеріями інноваційності університету виступають кількість поданих національних та міжнародних патентів, їх цитованість при розробці нових патентів, вплив патентів тощо. ТОП-100 найінноваційних університетів світу” 1, 2].

Другий підхід розглядає ширше інноваційно-активну діяльність університету як сукупність нових ініціатив в організації та розвитку лідерства; експериментів у педагогіці, організації знань, впровадженні нових форм навчання та розробці релевантних запитів бізнесу та соціуму академічних програм; взаємодії внутрішніх та зовнішніх зацікавлених сторін; міждисциплінарної наукової діяльності, пов'язаної зі здобуттям нових знань, методів та комерціалізацією їх результатів. Цей підхід пов’язаний з концепцією підприємництва, яка фокусується на двох ключових завданнях: формуванні підприємливої людини та розвитку підприємницького мислення 1, 2].

Підтримуючи імперативи другого підходу, автори під інноваційно-активним університетом розуміють підприємницьку організацію, яка має ресурсну готовність, а саме, готовність системи управління, готовність кадрового, освітнього, наукового, фінансового, організаційного потенціалів, сприятиме прискореному розвитку економіки та соціуму шляхом інтенсивного трансферту нових, згенерованих в університеті знань та технологій на основі партнерської взаємодії із суб'єктами ринку праці, урядовими та громадськими організаціями.

У цьому контексті домінантами діяльності ІАУ виступають 1, 2]:

- наука як інструмент генерації нових знань на основі інтеграції із зовнішнім оточенням насамперед з підприємствами високих технологій;
- освіта як спосіб доведення знань до людей, формування інтелектуального потенціалу суспільства;
- взаємодія з промисловістю, урядом, суспільством як засіб узгоджених зусиль щодо забезпечення стабільного розвитку нації та цивілізації.

Платформою підтримки ефективної взаємодії між університетом та стейкхолдерами виступають сучасні інформаційні системи та технології. Тому невіддільна (частина/ознака) частиною системи управління ІАУ є система корпоративного управління наданням освітніх послуг, яка на основі використання сучасного програмного забезпечення створює ефективний електронний документообіг та є інструментом запобігання корупції в університеті. Крім того, в умовах посилення агресивності зовнішнього інформаційного середовища, сучасних гібридних загроз виникає потреба забезпечення безпеки інформаційних ресурсів корпоративної інформаційно-освітньої системи (КІОС) та створення моделей та інструментів підтримки безпечного контуру основних бізнес-процесів надання освітніх послуг.

Таким чином, запропонований підхід забезпечує об'єктивний контроль з боку суспільства за освітньою діяльністю навчальних закладів, що сприяє як якості формування основних послуг освіти, а й формуванню конкурентоспроможних якостей студентів ЗВО.

На рис. 3 наведена структурна схема основних підсистем корпоративної інформаційно-навчальної системи.

Вибір критеріїв побудови методологічних принципів формування КІОС інноваційно-активного університету в умовах протидії корупції. Базовою складовою пропонованої методології є корпоративна інформаційно-освітня система, заснована на моделі взаємодії відкритих систем (Open Systems Interconnection Basic Reference Model), яка використовує відкриті протоколи для забезпечення безпеки інформаційних ресурсів КІОС.

Проведені дослідження показали, що практично всі протоколи забезпечують функціонування в відкритому вигляді, що суттєво знижує можливість забезпечення безпеки (надання послуг безпеки) на всіх рівнях моді ISO/OSI.

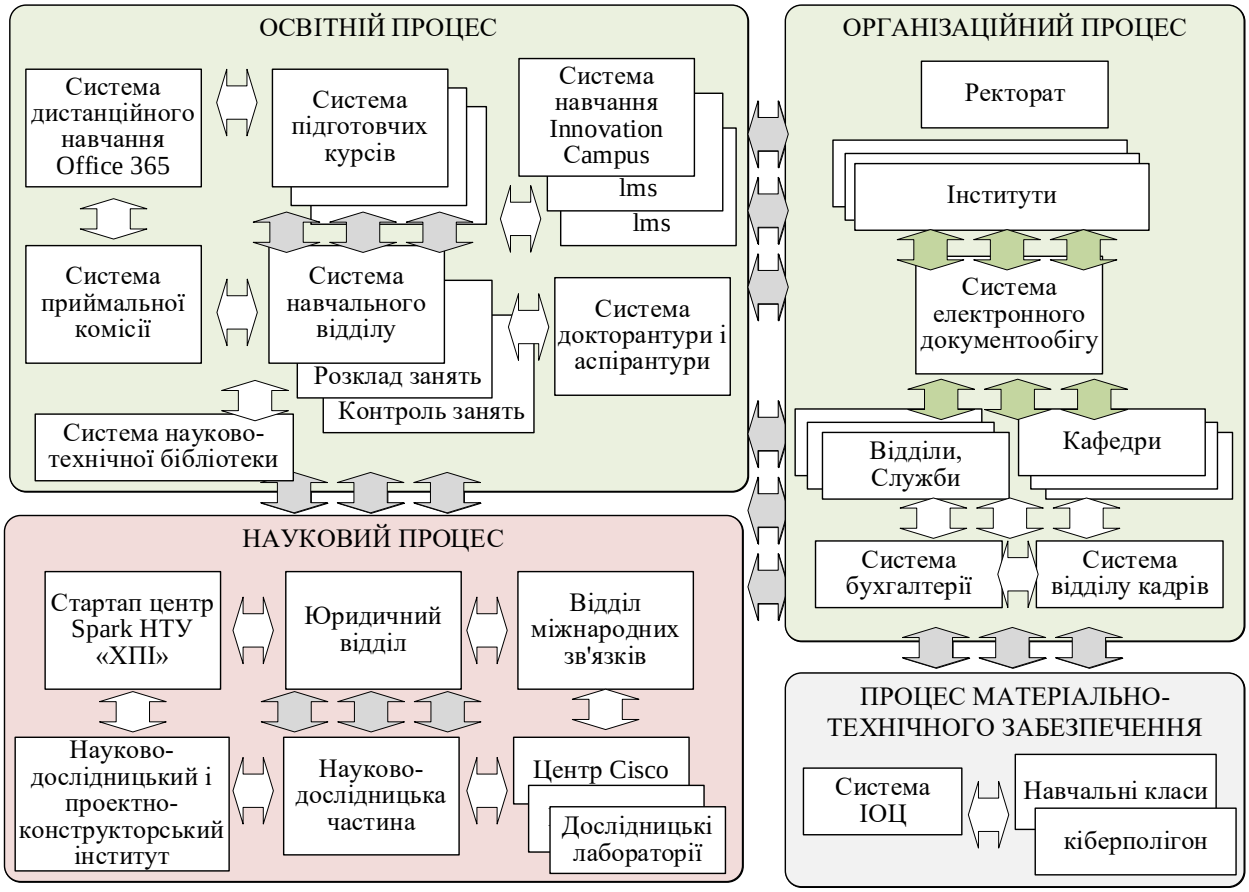


Рисунок 3 – Структурна схема КІОС

КІОС може відноситься до критичних кібернетичних систем, які впливають не тільки в умовах МОН України, та/або і на економічно-політичне середовище національної безпеки держави. Крім цього проведений аналіз показав, що з розвитком активного інноваційного університету, КІОС може розглядатися як синтез інформаційно-комунікаційних систем та кібернетичних фізичних систем, що дозволяє формувати можливі напади з двох напрямків векторів кібератак. Ця інтеграція є результатом досягнень в області інформаційних і комунікаційних технологій (ІКТ) для поліпшення взаємодії з фізичними процесами. Всі ці визначення підкреслюють постійне і інтенсивна взаємодія між кібер і фізичним світом. Однак їх розвиток визначило і новий напрямок у розвитку та / або модифікації старих загроз, що не тільки проявляється в можливості злому і несанкціонованого доступу до конфіденційної (персональної) інформації користувачів, а й можливістю проведення “енергетичного апокаліпсису”.

Таким чином, для запобігання або для підтримання контуру безпеки в кіберфізичних процесах для проведення аналізу відхилень від нормальної роботи і / або злому системи необхідне рішення уніфікованого підходу до побудови класифікації загроз з урахуванням їх синергізму і гібридності на всі складові безпеки: інформаційну безпеку (ІБ), кібербезпека (КБ) і безпеку інформації (БІ), в умовах їх подання з методами соціальної інженерії і нестачі коштів на забезпечення необхідного рівня безпеки.

Для забезпечення превентивних заходів боротьби з проявом елементів корупції на основі введення електронного обігу та елементів е-освіти в сучасні навчальні заклади пропонується використання технологій PKI, базисом яких є цифровий підпис (ЦП) на основі стандарту X.509.

Використання криптографічного стійкого механізму на основі цифрового підпису (ЦП) дозволяє забезпечити формування Концепції безпеки та протидії корупції в навчальних закладах. При цьому Концепцію слід розглядати як методологічну основу безпеки на різних рівнях управління.

Безпека функціонування інноваційного університету реалізується на наступних рівнях:

на *стратегічному рівні* – керівництво університету – створення умов неможливості внесення корупційних змін в керівні документи з організації навчального процесу, забезпечення основних комунальних та комунікаційних послуг діяльності університету, умов побуту студентів та прозорості надання освітніх послуг. Забезпечення ефективного контролю за виконанням графіка навчального процесу на факультетах університету;

на *оперативному рівні* – керівництво інституту, відділи та служби, залучені в системі надання послуг – запобігання корупційним змінам в об'єктивності оцінювання студентів в процесі навчання, нарахування стипендій (грантів і т.д.). Організація проведення іспитів протягом усього циклу навчального процесу, створення умов для ефективного контролю за виконанням графіка навчального процесу за спеціальностями факультету, запобігання корупції в відділах і службах університету;

на *тактичному рівні* – керівництво кафедр – підвищення рівня об'єктивності оцінювання студентів з окремих дисциплін, створення умов прозорого вибору студентами навчальних дисциплін з блоку вибіркової складової навчального процесу. Формування умов ефективного контролю за виконанням графіка навчального процесу викладачами кафедр.

Концепція безпеки та протидії корупції представлена на рис. 4, а, б, в.

а

б

Перший рівень описує загальну корпоративну стратегію університету і його функціональні стратегії в забезпеченні безпеки конфіденційних (персональних) даних при наданні освітніх послуг студентам. На даному рівні відповідно до синергетичним підходом розглядається загальна концепція забезпечення безпеки КІОС і формуються цілі та завдання забезпечення кібербезпеки. Функціональні стратегії одного рівня мають горизонтальними зв'язками та узгоджуються на рівні цілей з подальшою деталізацією на наступному рівні стратегічного набору.

в

Рисунок 4 – Концепція протидії корупції: *а* – стратегічний рівень; б – оперативний рівень; в - тактичний рівень

На другому рівні формується корпоративна стратегія інформаційної безпеки в КІОС, визначаються цілі та завдання основних бізнес-процесів, пов'язаних із захистом персональних даних юридичних і фізичних партнерів університету при наданні освітніх послуг.

На третьому рівні формується адаптивна система захисту інформаційних ресурсів КІОС на основі сучасних механізмів безпеки. При цьому рекомендується використання комерційних криптографічних систем з метою запобігання кріптозакладок.

Пропонований підхід враховує не тільки основні функції ієрархічної структури управління ІАУ, їх цілі та завдання, а й забезпечення протидії елементів корупції та комплексування гібридним загрозам на основі побудови АСЗІ. Основними елементами АСЗІ є ЦСК “Шифр-Х.509”, який забезпечує не тільки автентифікацію/авторизацію, але та автоматичний контроль електронного документообігу, що значною мірою знижує ризики прояви корупційних схем на всіх рівнях управління ІАУ.

Функціональним призначенням СКЗІ “Шифр-Х.509” є:

–забезпечення управління ключами та сертифікатами відповідно до ДСТУ *ISO/IEC 9594-8:2006*;

–забезпечення криптографічного захисту конфіденційної і відкритої інформації: обчислення і перевірка електронного цифрового підпису даних відповідно до ДСТУ 4145-2002, шифрування та імітозахист даних відповідно до ГОСТ 28147-89, формування геш-функції відповідно до ГОСТ 34.311-95.

СКЗІ “Шифр-Х.509” є програмним комплексом, засоби якого функціонують у середовищі ОС електронно-обчислювальної техніки та взаємодіють із загальним прикладним програмним забезпеченням, його загальна структура наведена на рис. 5.

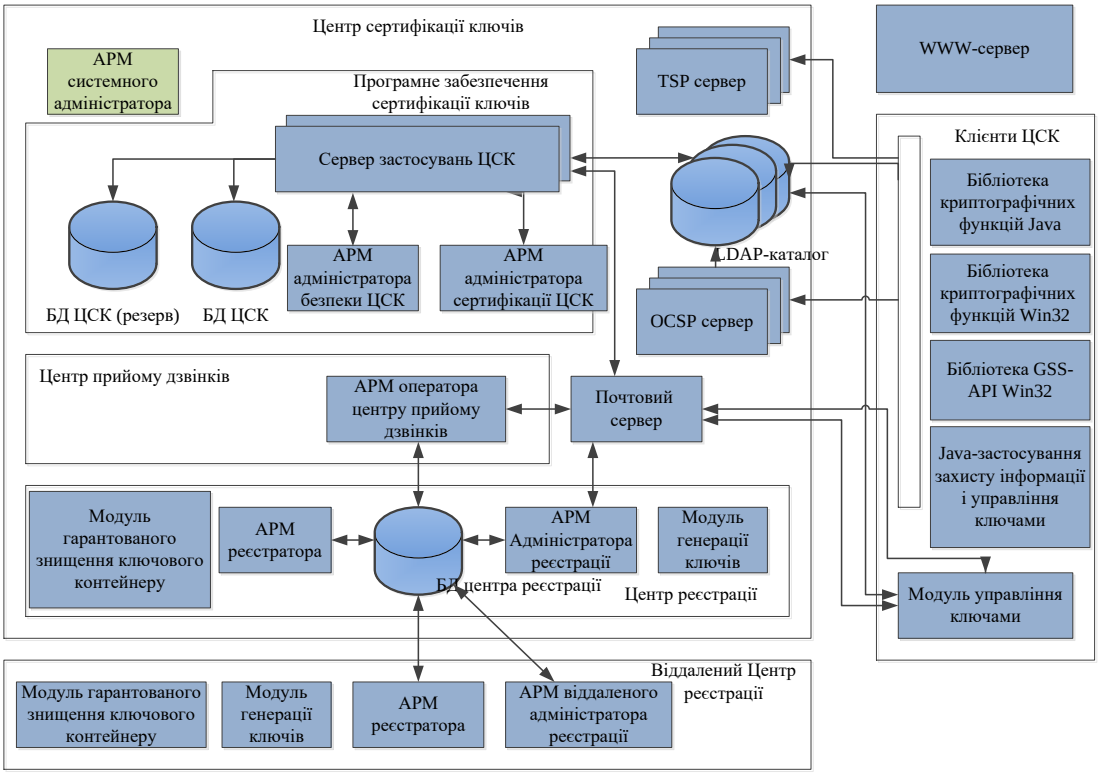


Рисунок 5 – Загальна структурна схема СКЗІ “Шифр-Х.509

За необхідністю, можливий доступ до сертифікатів що опубліковані у LDAP-каталозі. На рис. 6 приведена фізична віртуальна мережа для розгортання системи комплексного захисту інформації (СКЗІ) на основі інфраструктури PKI [52, 53]. Для верифікації ЦП використовується сертифікат ключа – електронний документ, виданий центром, що засвідчує (ЦП) або довіреною особою ЦП і підтверджують приналежність ключа перевірки ЦП власнику сертифіката ключа перевірки ЦП.

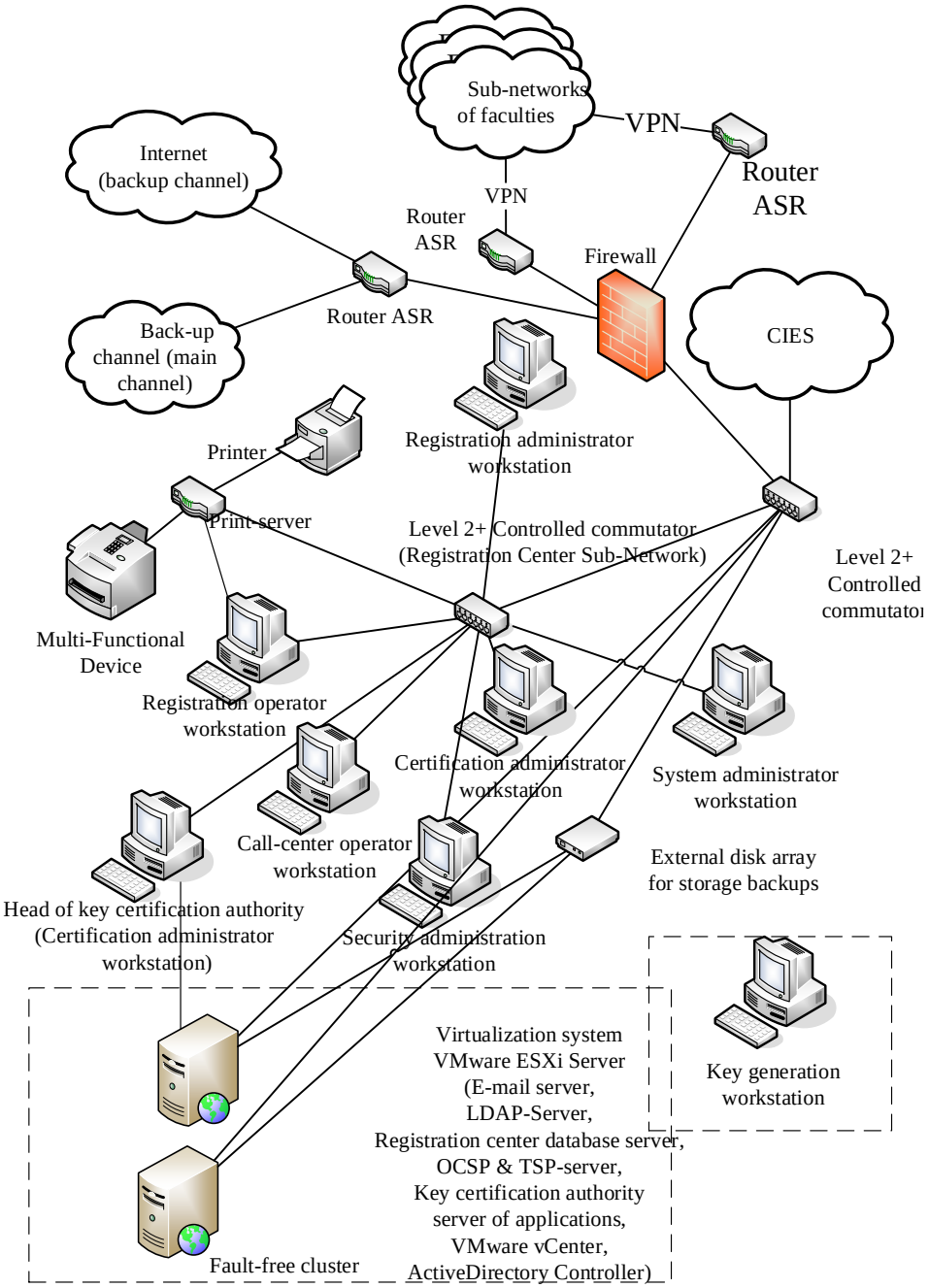


Рисунок 6 – Фізична мережа інфраструктури PKI

На рис. 7 представлений варіант структурної схеми КІОС ІАУ з урахуванням основних функцій управління і забезпечення безпеки інформаційних ресурсів (IP

КІОС) в умовах впливу гібридних загроз і можливих схем корупції.

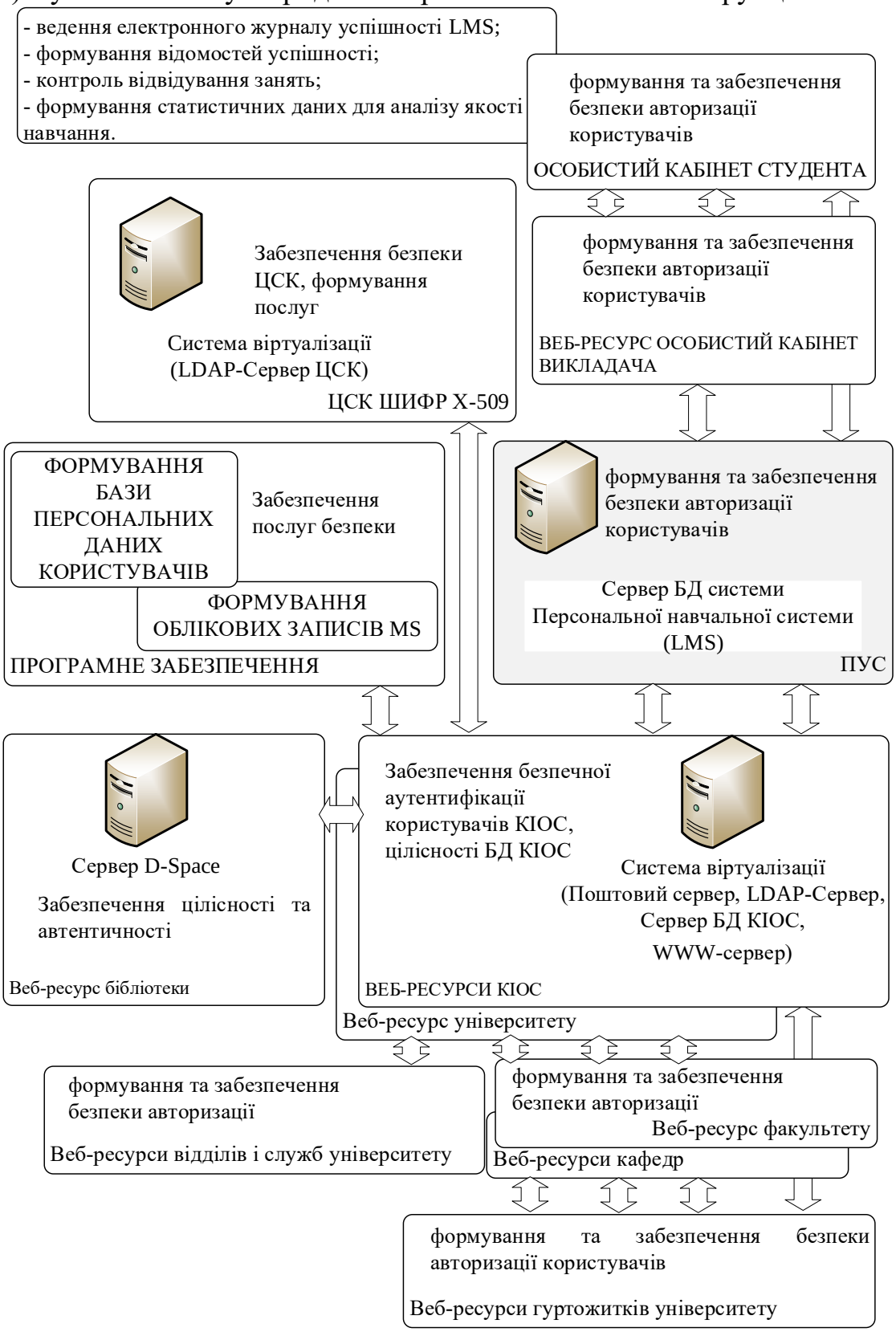


Рисунок 7 – Варіант структурної схеми КІОС інформаційно-активного університету.

Тому крім забезпечення автентичності ІР КІОС на основі ЦСК, для забезпечення конфіденційності та цілісності ІР пропонується використовувати комерційну реалізацію постквантових алгоритмів – крипто-кодових конструкцій Мак-Еліса і Нідеррайтера.

Такий підхід забезпечить не тільки необхідний рівень криптостійкості в умовах появи повномасштабного квантового комп'ютера, оперативності криптоперетворень на рівні блоково-симетричних шифрів, вірогідності, а й протидія кріптозакладкам на основі стандартів шифрування.

Технологія побудови модифікованої системи електронного документообігу в університеті

Створення внутрішньої університетської системи елементів документообігу, яка спрямована на підвищення ефективності контролю за наданням освітніх послуг закладом вищої освіти, об'єктивності оцінювання процесу навчання і запобігання корупції в ЗВО ґрунтується на КІОС ЗВО. Такий підхід є обов'язковим в умовах створення/переходу до ЗВО нового підприємницького типу – інноваційно-активного університету.

Відповідно до цього, запропонована технологія побудови системи електронного документообігу (СЕД), яка, спрямована на запобігання корупції при наданні освітніх послуг.

Технологія побудови системи електронного документообігу є елементом системи управління та прийняття рішень в КІОС університету. Її зміст складають управлінські процедури, пов'язані зі збиранням, рухом, зберіганням, обробкою, аналізом інформації, забезпеченням нею структурних підрозділів і окремих робочих місць працівників ЗВО. За цих підстав, в дослідженні розроблено комплекс завдань відповідно до запропонованих стадій технології.

Стадія 1. Розробка концептуальних основ проекту:

- обґрунтування необхідності введення нових світових підходів щодо запобігання корупції на основі використання сучасних криптографічних механізмів забезпечення основних послуг безпеки в систему електронного документообігу ІАУ;
- аналіз світового досвіду розгортання і впровадження системи електронного документообігу університету при наданні освітніх послуг;
- формування методології ієрархічної системи управління наданням освітніх послуг ІАУ;
- побудова концептуальних основ розробки програмної та технічної складової системи електронного документообігу.

Стадія 2. Реалізація проекту:

- розробка необхідного програмного забезпечення, адаптованого під корпоративну систему вузів на основі СКЗІ "Шифр Х.509";
- розробка необхідної документації з використання програмного забезпечення документообігу та використання спеціального програмного забезпечення СКЗІ

“Шифр Х.509” в КІОС ІАУ;

- формування основних вимог, ТТХ з впровадження системи СКЗІ “Шифр Х.509” в корпоративну мережу ЗВО;

- формування відповідних керівних документів щодо впровадження системи ефективного контролю за наданням освітніх послуг ЗВО;

- впровадження змін до посадових інструкцій відповідних посадових осіб, з контролю за використанням і роботою системи електронного документообігу;

- проведення конференцій, круглих столів, майстер-класів, які сприяють загальним цілям розгортання системи ефективності контролю у всіх ланках організації та управління наданням освітніх послуг студентам ЗВО, контролю об’єктивності системи оцінювання студентів під час всього циклу навчання, надання побутових та інших послуг під час перебування в вузі з метою запобігання корупції на всіх рівнях системи управління вузом;

- проведення компаній з інформування / пропаганди професорсько-викладацького складу з впровадження системи запобігання корупції при наданні освітніх послуг ІАУ, оцінки підтримки з боку керівного складу ЗВО з впровадження системи запобігання корупції, моніторингу зміни в ефективності роботи системи електронного документообігу;

- проведення тренінгів зі студентами ЗВО про переваги використання системи електронного документообігу ЗВО, спрямованої на запобігання корупційним діям;

- освітлення розробленої системи електронного документообігу як засобу запобігання корупції в соціальних мережах, регіональних засобах масової інформації;

- оприлюднення результатів запропонованої системи на сайті проекту.

Стадія 3. Еволюція проекту:

- проведення обговорень/круглих столів з усіма ланками ЗВО з працездатності системи електронного документообігу, побудованої на антикорупційних принципах на основі модифікованої системи електронного документообігу ЗВО при наданні освітніх послуг;

- внесення змін, уточнення в керівні документи з використання модифікованої системи електронного документообігу ЗВО;

- моніторинг працездатності системи при проведенні вступної компанії, проведення екзаменаційних сесій;

- проведення майстер-класів / тренінгів з представниками стратегічної, тактичної та оперативної ланки управління ЗВО з використання запропонованої системи електронного документообігу ЗВО при наданні освітніх послуг;

- проведення інформаційних / освітніх інтерактивних заходів серед студентів закладів вищої освіти з обговорення основ створення системи контролю за об’єктивністю оцінки та запобігання корупції в усіх ланках ієрархічної системи управлінням наданням освітніх послуг ЗВО;

- проведення дебатів серед громадськості по обговоренню впровадження

відповідних змін у процес надання освітніх послуг ЗВО;

- обговорення можливості впровадження розробленої системи в університетах МОН України.

Запропонований підхід забезпечує формування кібернетичної системи на основі технології відкритих ключів, що дозволяє з упевненістю боротись з проявами корупції в ЗВО на основі технічних рішень без участі людини.

Використання IT-технологій в процесі навчання як специфічний чинник інформаційного суспільства

Розвиток сучасних технологій суттєво розширює спектр послуг, які можливо використовувати в КІОС. Це в свою чергу суттєво впливає на рейтинг університету за критеріями міжнародного рейтингу університетів світу Ranking Web of Universities (Webometrics). Основні критерії наведені на рис. 9.

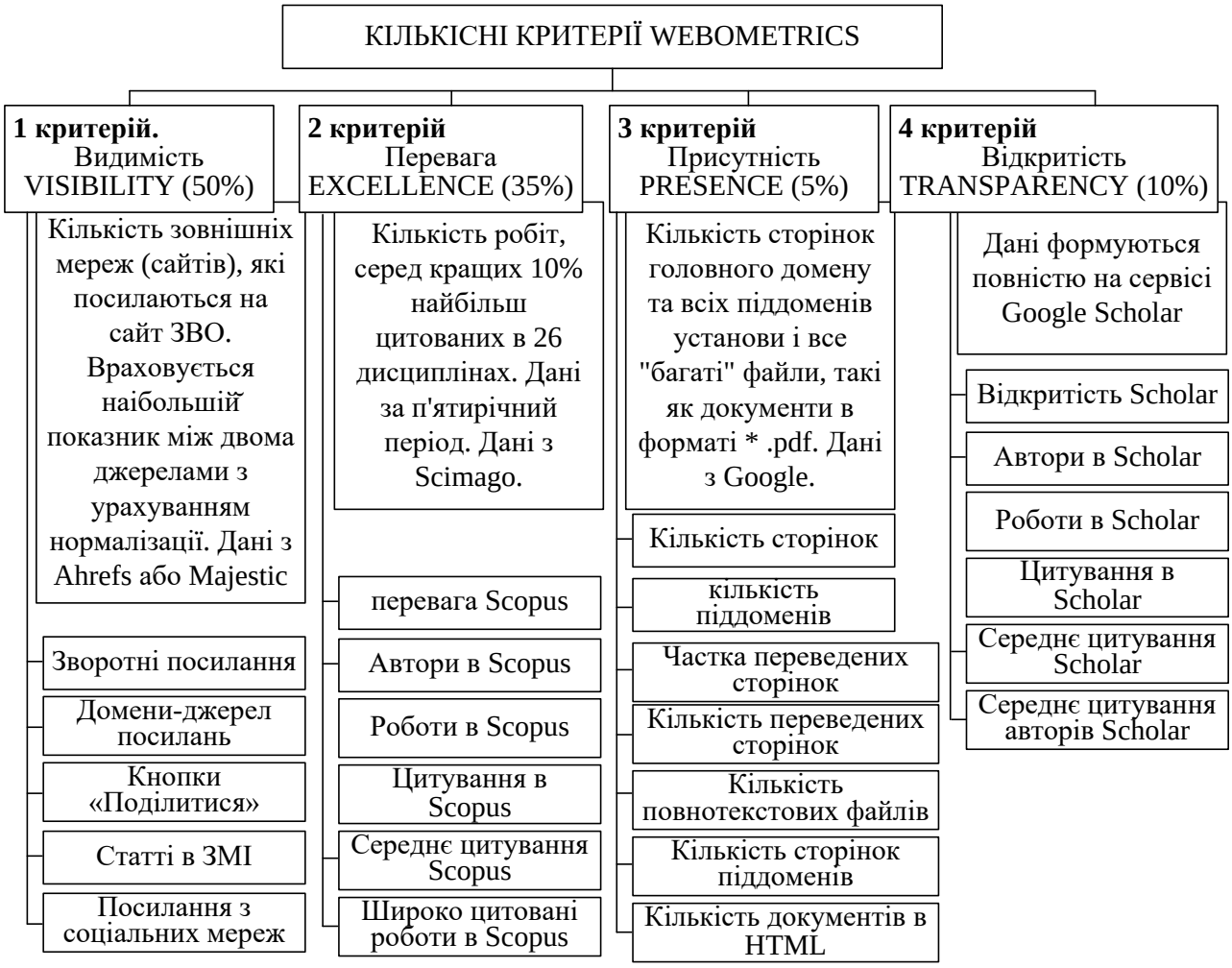


Рисунок 9 – Критерії оцінювання міжнародного рейтингу університетів світу Ranking Web of Universities

Проведений аналіз рис. 9 показав, що в першу чергу ЗВО необхідно мати потужні веб застосунки, усі дозволять висвітлювати практично усі напрямки

діяльності університету та забезпечити їх прозорість. Другим напрямком підвищення відповідного показника рівня є наукові досягнення професорсько-викладацького складу (ПВС) шляхом публікацій в журналах (відповідних міжнародних конференціях), які афілюються в науково-метричної базі Scopus. І останнім напрямком є прасування публікацій ПВС в метричній базі Google Scolar, що дозволяє підвищити рівень наукової складової ЗВО.

Однак на сьогоднішній час суттєві зміни в політиці безпеки ІТ-гігантів не дозволяють своєчасно та об'єктивно отримувати відповідні показники за критеріями міжнародного рейтингу університетів світу Ranking Web of Universities (Webometrics). Це пов'язане, в першу чергу, з відсутністю штатного підрозділу у ЗВО України, який забезпечував надійну безпеку вебзастосунків, їх розробку та впровадження. По-друге, вимоги створення АІУ висувають більш жорсткі вимоги щодо забезпечення послуг безпеки: конфіденційності, цілісності та автентичності, інформаційних ресурсів ЗВО: персональні дані студентів та ПВС (бази ЄДБО), персональні дані робітників ЗВО, конфіденційна інформація, ноу-хау відповідних лабораторій. По-третє, можливість реалізації загроз на КІОС шляхом зламу доменів (піддоменів) ботами/зомбі-ботами розвинутих держав та/або кіберзлочинців.

Для підвищення рівня першого критерію Webometrics, створення умов автоматизації окремих елементів документообігу при наданні освітянських послуг, протидії корупції у ЗВО пропонується створення вебзастосунків "Особистий кабінет викладача", "Особистий кабінет студента".

Основними функціями вебзастосунку "Особистий кабінет викладача" є:

– створення можливості розподілу навантаження керівником навчального відділу між підрозділами університету (кафедрами);

– створення можливості планування розподілу начальником кафедри навчального навантаження серед ПВС кафедри;

– автоматичне формування першої половини навантаження в індивідуальному плані викладачів кафедри;

– можливість індивідуального планування ПВС кафедри другої "половини дня";

– можливість автоматизації формування плану з науки кафедри шляхом індивідуального планування публікацій ПВС кафедри;

– доступність до особистих кабінетів в Scopus, Scolar, ORCID;

– доступність до ресурсів КІОС (LMS, електронного журналу викладача, сайту університету, бібліотеки, сайтів відповідного факультету, кафедри);

– можливість корегування електронного журналу викладача шляхом мобільного застосунку;

– доступ до керівних документів університету, МОН України.

Основними функціями вебзастосунку "Особистий кабінет студента" є:

– автоматичне формування індивідуального плану студента;

– можливість вибору вибіркової складової індивідуального плану студента через вебзастосунок;

– можливість перевірки результатів навчання (нарахування балів за освітніми компонентами, отриманих балів за екзамен і т.п.);

– можливість перевірки місця в рейтингу групи;

– можливість замовлення необхідної літератури через сайт бібліотеки ЗВО;

доступність до ресурсів КІОС (LMS, електронного журналу студента, сайту університету, бази бібліотеки, сайтів відповідного факультету, провідної кафедри);

– доступ до керівних документів кафедри, факультету, університету, МОН України.

Таким чином, розробка цих вебзастосунків дозволяє покращити рівень університету за першим критерієм міжнародного рейтингу університетів світу Ranking Web of Universities (Webometrics), а саме сформувати мультисайт з єдиною базою даних (на сайті університету), забезпечити своєчасне оновлення відповідних технологій вебзастосунків, безпеку їх використання в умовах сучасних загроз.

Таким чином, запропоновані напрямки підвищення рівня ЗВО за критеріями міжнародного рейтингу університетів світу Ranking Web of Universities (Webometrics) дозволяють об’єктивно впливати на перехід університетів на наступний рівень – активного інноваційного університету шляхом впровадження та використання сучасний веб технологій і застосунків, підвищення рівня наукової діяльності професорсько-викладацького складу університету (їх мотивації), впровадження нових інноваційних підходів в діяльність ЗВО.

Література

1. S. Yevseiev, V. Ponomarenko, and O. Rayevnyeva, “Assessment of functional effectiveness of the corporate scientific-educational network based on comprehensive indicators of service quality”, Eastern-European Journal of Enterprise Technologies, 6/2 (90), p. 4 – 15, 2017.

2. S. Yevseiev, O. Rayevnyeva, V. Ponomarenko, O. Milov, Development of methodological principles for the construction of a corporate information educational system of innovative-active University in the framework of anticorruption activities. Eastern-European Journal of Enterprise Technologies. 2020. 5/2(107). p. 6–28.

3. Ревак І.О. Корупція: теоретико-методологічні засади дослідження: монографія / І.О. Ревак. – Львів: ЛьвДУВС, 2011. – 220 с.

Стемпківська В.О.
Савчук В.С.
д.філос. (технічні науки)
Житомирський Військовий Інститут ім. С.П. Корольова

ЗАХИСТ ОСОБИСТИХ ДАНИХ ПІД ЧАС OSINT В ІНТЕРЕСАХ ПСО

До повномасштабного вторгнення, навіть до “Революції Гідності”, країна агресор – російська федерація, вела гібридну війну по відношенню до нашої держави. Спецслужби росії намагаються перемогти війну в інформаційному просторі шляхом дезінформації, кібератак, шантажування, військового обману та провокацій. Одною з операцій, які проводили спеціалісти російської федерації і набула широкого поширення у 2017 році є вірус “Петя” під час проведення кібератак російською федерацією. Він проникав на носії замаскованим під програмою-вимагачем та шляхом шифрування файлів на жорсткому диску, а також займався переписуванням і шифруванням головного завантажувального запису. В результаті всі файли, які були збереженні на комп’ютері, стають недоступними. Для більшості цих методів використовуються особисті данні осіб, які необізнані в безпечному використанні різного типу сайтів та мережі. Фахівцям ПсО під час виконання завдань за призначенням, особливо ведення OSINT необхідно зберегти данні для запобігання використання їх ворогом або розповсюдження особистої інформації. Для цього слід дотримуватись простих правил кібергігієни, адже спецслужби росії масово використовують OSINT для збору інформації в своїх цілях.

Доступний спосіб це використання не важливих даних під час реєстрації та автоматизації, які не будуть розкривати особу користувача, такі як, “липова” електронна пошта, неправдиві імена, надійні та непов’язані з особою паролі та номери, які ви не використовуєте в повсякденному житті. Важливо пам’ятати що данні, які ви оприлюднюєте в соціальних мережах, навіть після видалення все рівно не гарантують, що ці дані не були збережені іншими особами або ресурсами. Наприклад, Wayback Machine, яка працює як інтернет-архів, скануючи в собі дані з безлічі сайтів кожного для і зберігає їх. Під час проведення роботи на сайтах знайомств, соціальних мережах, форумах краще приховати свою реальну особу і створити реалістичну віртуальну сторонню особистість.

Використання VPN дозволить встановлювати віртуальну захищену мережу поверх інших мереж із меншим рівнем довіри. Дозволить захистити ваше інтернет-з’єднання і конфіденційність в мережі Інтернет. Крім того, VPN шифрує дані, що передаються між користувачем і запитаним ресурсом, що виключає перегляд переданих/прийнятих даних провайдером і інших зацікавлених осіб.

Також в мережі є можливість використання різного типу анонімайзерів, як Хамеленон, дозволяє блокувати файли cookie, шифрувати URL-адреси й сторінки,

видаляти скрипти та об’єкти, що дозволть користувачеві захистити свої данні. Чи HideMe, змінюючи ваш проксі на іншу країну на вибір. Вони забезпечать приховання інформації про комп’ютер чи користувача та не дозволить відслідковувати активність в інтернеті.

Для анонімного серфінгу створені безпечні браузери. Один з таких має назву TOR. Його можна запустити навіть з використанням флеш-накопичувача. Нічого не потрібно додатково налаштовувати. Через цей браузер данні нашаровуються постійним шифруванням та розшифровуванням, тому видозмінюються шляхом спотворення, тому початкові данні просто губляться в шарах маніпуляції над ними. Більш сучасним аналогом з розширеним функціоналом є VENATOR (браузер на базі FireFox).

Даний перелік засобів забезпечення конфіденційності в інтернеті не є вичерпним, проте є актуальним захисту своїх даних, тому варто використовувати та розумітись у них. Тим більше в умовах гібридної війни, коли за допомогою OSINT ви можете стати жертвою служб російської федерації. Ваші данні розійдуться у мережі, як через сайт Немезида або групу тлг “Берегиня”, ваші особисті данні можуть зіграти проти вас.

Література

1. Wayback Machine. Матеріал з Вікіпедії — вільної енциклопедії. Сайт URL:
https://uk.wikipedia.org/wiki/Wayback_Machine (дата звернення: 19.03.2023).
2. DROPBOX. Що таке VPN? Сайт URL: https://experience.dropbox.com/uk-ua/resources/what-is-vpn (дата звернення: 20.03.2023).
3. Кращі безкоштовні анонімайзери: VPN, онлайн, браузери. Для тих, кому важлива приватність. Сайт URL: https://dev.ua/news/best-free-anonymizers-vpn (дата звернення: 19.03.2023).
4. Про Tor Browser. Сайт URL: https://tb-manual.torproject.org/uk/about/ (дата звернення: 20.03.2023).
5. Григорій А. Кібератака вірусу Petya: що відомо. Сайт URL: https://www.dw.com/uk.

Степанишин Р.Д.
начальник кафедри зарубіжної воєнної інформації,
Військовий інститут КНУ імені Тараса Шевченка

РОЛЬ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ У ФОРМУВАННІ ФЕНОМЕНУ КОЛАБОРАЦІОНІЗМУ

З явищем колабораціонізму, відомим з давніх часів і широко

розповсюдженим в ході Другої світової війни, Україна безпосередньо зіткнулась з початком війни з рф у 2014 році. Наша держава виявилась не готовою протидіяти такого роду загрозам ні з політичної, ні з юридичної, ні з інформаційної точки зору. Особливо гостро це питання постало після початку повномасштабного вторгнення рф на територію України і окупацією російськими військами значних територій нашої держави. Певною відповіддю стало ухвалення законів України № 2107-IX "Про внесення змін до деяких законодавчих актів України щодо забезпечення відповідальності осіб, які здійснювали колабораційну діяльність" і №2108-IX "Про внесення змін до деяких законодавчих актів України щодо встановлення кримінальної відповідальності за колабораційну діяльність" від 15.03.2022 року. Разом з тим, зазначені закони мають ряд недоліків, не в повній мірі забезпечують юридичне регулювання відповідальності вчинення дій, які підпадають під визначення колабораційної діяльності.

Однією з причин такого стану речей є недостатнє дослідження колабораціонізму як складного соціально-політичного явища, визначення причин його виникнення, механізмів та інструментів впровадження в масову свідомість. Довгий період часу дослідження колабораціонізму в Україні обмежувалось "відбиттям" нападок російських істориків, для яких слова "Україна" і "український" фактично стали синонімами слів "націоналіст, колабораціоніст, каратель, зрадник". Це була важлива сфера роботи, але за історичними дискусіями повз дослідників "пройшла" проблема сучасного колабораціонізму і його пропаганда серед населення нашої держави.

Ми звикли до висловлювання, що основною причиною колабораціонізму серед громадян України є вплив російської пропаганди, насамперед телевізійної. Доля істини в цьому безумовно є, але на проблему потрібно дивитись більш широко, з позицій проведення рф масштабного інформаційно-психологічного впливу у різних сферах з використанням значного спектру інструментів і методик.

Не секрет, що масштаби колабораціонізму збільшувались пропорційно розвитку засобів розповсюдження інформації. Без широкого розповсюдження радіомовлення і використання його з пропагандистськими цілями важко собі уявити той розмах колабораціонізму, який спостерігався в країнах Західної Європи під час Другої світової війни (в ході Першої світової масштаб явища був на порядок меншим). Телебачення фактично зробило революцію у засобах масової інформації, поступово перетворившись на інструмент створення альтернативної реальності. Ера компютерних технологій та Інтернету ще більше розширило пропагандистські можливості. Здавалось, рішення проблеми лежить на поверхні – обмеження доступу до російських ЗМІ та поступове виведення населення з інформаційного простору рф. Такі рішення були прийняті впродовж 2014-2015 рр., але і у 2022 році ми стикаємось з судовими справами щодо розповсюдження проросійських наративів і виправдання дій російських військ навіть серед населення міст, які постійно піддаються атакам противника.

Корінь проблеми лежить в площині двох тверджень:

1. Колабораціонізм не виникає лише під час воєнних конфліктів. Це результат цілеспрямованого, розтягнутого в часі інформаційно-психологічного впливу на визначені цільові аудиторії. Вплив на різні цільові аудиторії різний, для кожної підбирається свій "ключик". Але в комплексі це дає змогу створити відповідне підґрунтя для колабораційної діяльності та сформувати готові до неї кадри (і це без врахування спеціально підготовлених на території противника осіб, які в подальшому перекидались на територію України).

2. Підривна діяльність проти власної держави у мирний час це також колабораціонізм. Важливо відмітити, що підривна діяльність може виглядати зовсім не так, як ми звикли її сприймати. Наприклад, пряма зрада представників партії ОПЗЖ і їх перехід на сторону окупантів, як це не прикро звучить, було справою очікуваною. Але як оцінити висунення рядом українських політиків тез про знищення рф як держави, розділення її на частини тощо? Саме базуючись на таких висловлюваннях путінська адміністрація змогла провести мобілізацію під гаслами "захисту батьківщини від зовнішньої загрози". "Ступінь ненавмисності" такої деструктивної діяльності є дискусійним питанням (можлива дія по необізнаності, необережності), але сам факт деструкту явний.

Підсумовуючи викладене можна зробити висновок, що явище колабораціонізму не виникає раптово та потребує певного часу для формування відповідних умов. Водночас це явище не є спонтанним, а в більшості випадків стає результатом цілеспрямованого методичного інформаційно-психологічного впливу з використанням як зовнішніх ресурсів, так і внутрішніх антидержавних елементів. Тому протидія колабораціонізму потребує високого рівня готовності до таких дій відповідних державних інституцій та наявності алгоритмів профілактики, раннього виявлення і реагування на появу ознак розповсюдження колаборційних ідей в суспільстві.

Тиква В.Л.
старший викладач кафедри ІБД
Національна академія СБ України

ВПЛИВ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ НА ТРАНСФОРМАЦІЮ ІНФОРМАЦІЙНОЇ ЗБРОЇ

Третє тисячоліття відзначається стрімким масштабним розвитком комп'ютерних інформаційних технологій, високошвидкісною передачею даних, масовим упровадженням інтернет можливостей у всі сфери суспільної діяльності. Такі темпи розвитку комп'ютеризації та інформатизації населення неминуче ведуть до створення спільного світового інформаційного простору, в якому

зосереджуються всі засоби збирання, накопичення, обміну та зберігання інформації. Дедалі інформаційний простір фактично стає полігоном воєнних дій, де кожна з ворогуючих сторін прагне отримати перевагу, а в разі необхідності розгромити противника. Розмах протистояння в інформаційному просторі досяг таких масштабів, що спонукало необхідність створення спеціальної концепції з назвою “інформаційна війна”.

В залежності від ситуації вона може носити наступальний або оборонний характер. Відповідно удосконалюються наявні та активно відпрацьовуються нові оборонні й наступальні методи ведення інформаційної війни, які дають можливість досягти інформаційної переваги над опонентами. Основним засобом ведення інформаційної війни є інформаційна зброя.

За одним із існуючих визначень, інформаційна зброя - це комплекс програмних і технічних засобів, створених для контролю інформаційних ресурсів об'єктів впливу та втручання в роботу їх інформаційних систем [1].

Сучасні процеси глобалізації якісно трансформували зміст і форми ведення інформаційних війн. Всесвітня глобалізація подвійно вплинула на характер сучасних конфліктів та війн: по-перше, спричинила деформацію державної влади та загострила соціальну уразливість, по-друге, створила нові можливості й економічні заохочення.

З урахуванням цього, інформаційну війну можна визначити як сукупність заходів інформаційного забезпечення, інформаційного наступу та захисту, які проводять за єдиним задумом з метою отримання інформаційної переваги над ворогом. Поширення деструктивних інформаційних компаній пояснюється можливістю досягнення (в короткий термін) політичних цілей завдяки проведенню масштабних (стратегічних) психологічних операцій для нав`язання відповідної вигідної системи поглядів, психологічного оброблення соціуму країни та сусідніх держав [2].

Чимало прикладів застосування інформаційної зброї продемонструвала Друга світової війна. Зокрема, Японія вдалася до комплексу заходів із формування як серед військовослужбовців, так і усього населення культу “камікадзе”. Не маючи військової переваги над ворогом, відтягуючи неминучий програш, японці намагалися залякати американців атаками смертників. В підсумку політична верхівка Японії досягла переваги в психологічній боротьбі - утримала свій статус у суспільстві.

Поширення явища інформаційна війна пояснюється неможливістю ведення в умовах світового порядку фронтальних агресивних бойових дій, використання зброї масового ураження. Тому акцентовані інформаційні впливи забезпечують досягнення політичних цілей, сприяють проведенню стратегічних психологічних операцій, формують позитивне ставлення міжнародної спільноти до таких дій. Психологічій обробці піддаються також і власні війська з метою підняття бойового духу, і формування в них культу визволителів, носіїв демократичних

цінностей тощо. На початку XXI століття вирішального значення в інформаційній війні набула також іміджева складова, яка передбачає деструктивний вплив на репутацію ворога, що впідсумку має привести до його ігнорування та дискредитації перед світовим співтовариством. Останні 10-15 років засвідчили суттєве зростання можливостей інформаційних технологій. Але саме зараз це питання постало як одне з ключових у боротьбі за світовий інформаційний простір [3].

Сучасні інформаційні технології кардинально вплинули на таку сферу міжнародних відносин, як інформаційне протиборство, зумовивши якісно новий рівень ведення інформаційних воєн.

Більшість країн - світових лідерів володіє потужним інформаційним ресурсом, який за певних умов забезпечить їм досягнення політичних цілей, враховуючи відсутність сформованих міжнародних юридичних норм щодо ведення інформаційної боротьби. Моніторинг публікацій у ЗМІ переконливо засвідчує, що основний тренд інформаційної боротьби полягає в підвищенні її ролі на міжнародній арені. Удосконалення нетрадиційних засобів протиборства на сучасному етапі науково-технічного прогресу призвело до виникнення зброї глобального ураження, системне застосування якої за певних умов здатне знищити середовище існування людства.

Використання інформаційних засобів і систем суттєво збільшує можливості державного впливу. Водночас зростає уразливість систем управління від цілеспрямованого впливу в інформаційному просторі. Ці тенденції об'єктивно приводять до розширення арсеналу методів і засобів ведення інформаційних війн, посилення їхнього впливу на хід і результат воєнних дій, зростання кількості задіяних сил і засобів [4].

Слід констатувати що пряме військове вторгнення рф до України у лютому 2022 року, фактично в центрі Європи, є скоріше виключенням ніж правилом. Здебільшого, на сучасному етапі історичного розвитку людства домінує тенденція розв'язання зовнішньополітичних конфліктів без застосування зброї. Інформаційне протиборство перестало бути другорядним чинником, доповненням до “основних” подій. Воно перетворилася на один із найважливіших механізмів «розв`язання» конфліктів, про який говорять нарівні з використанням звичайних видів озброєнь та військової техніки. Інформаційне протиборство в сучасному світі стало легітимним засобом політичної боротьби.

Інформаційні війни стали аксіомою сучасних міжнародних відносин і дають змогу досить ефективно, із залученням незначних фінансових та людських ресурсів, досягати потрібних цілей: все залежить від ступеня професіоналізму реалізаторів інформаційних операцій. Відстоювати свої позиції в інформаційному протиборстві буде набагато легше тим країнам, які матимуть гармонійно розвинуте й тому захищене інформаційне суспільство [5].

Література
1. Інформаційна безпека: підручник./ О.І. Фармагей та ін. Київ, 2021. 411 с.;
2. Горбулін В.П. Проблеми захисту інформаційного простору України: моногр. / В.П. Горбулін, М.М. Биченок // Ін-т пробл. нац. безпеки. – К.: Інтертехнологія, 2009. 136 с.;
3. Богуш В. Інформаційна безпека держави/ Володимир Богуш, Олександр Юдін,; Гол. ред. Ю. О. Шпак. -К.: "МК-Прес", 2005. 432 с. ;
4. Кормич Б. Інформаційна безпека: організаційно-правові основи: Навчальний посібник/ Борис Кормич,. -К.: Кондор, 2005. 382 с. ;
5. Про національну безпеку України: Закон України від 21.06.2018 (зі змінами від 22.04.2022 р.) [Електронний ресурс], – Режим досту- пу: http: // www.zakon.rada.gov.ua.

Тиква В.Л.
старший викладач КІБД
Національної академії СБ України
Радисюк А.А.
студент Національної академії СБ України

ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЮ ПОЛІЦІЄЮ УКРАЇНИ ПУБЛІЧНОЇ БЕЗПЕКИ І ПОРЯДКУ В УМОВАХ ВОЄННОГО СТАНУ

Забезпечення публічної безпеки і порядку є однією з основних функцій Національної поліції України. ЇЇ значення зумовлене створенням у державі захисту прав і свобод громадян, їх життя і здоров’я, запобігання кримінальним правопорушенням і проступкам, поваги до честі та людської гідності, дотримання норм суспільної моралі та порядку. Водночас актуальність забезпечення публічної безпеки та порядку сьогодні значно посилюється в умовах дії правового режиму воєнного стану.

Воєнний стан був оголошено 24 лютого 2022 року у зв’язку з повномасштабним вторгненням рф на територію України, що беззаперечно постало загрозою національній безпеці, територіальній цілісності, життю та здоров'ю громадян [1, с.88].

В умовах воєнного стану Національна поліція України має на меті забезпечення безпеки та порядку в країні, в тому числі: захист життя, здоров'я і майна громадян; захист від кримінальних правопорушень, терористичних актів, диверсій і шпигунства; контроль за додержанням порядку на дорогах та в громадських місцях; захист від дискримінації і насильства; розшук і затримання осіб, які здійснюють кримінальні правопорушення; забезпечення правопорядку та

дотримання законів.

Також, під час забезпечення публічної (громадської) безпеки і порядку в умовах дії правового режиму воєнного стану на уповноважені органи та підрозділи Національної поліції покладаються особливі вимоги щодо несення служби. До таких особливостей, наприклад, відносяться:

- несення служби щодо забезпечення публічної (громадської) безпеки і порядку під час комендантського часу, в умовах активних бойових дій під час звільнення окупованих територій та на блокпостах;
- виявлення та знешкодження диверсійно-розвідувальних груп ворога;
- участь у рятуванні людей та надання їм допомоги та забезпечення охорони майна, яке залишилося без догляду;
- під час взаємодії з підрозділами Національної гвардії України та добровольчими формуваннями територіальної громади тощо [2, с.68].

Отож, забезпечення Національною поліцією України публічної безпеки та порядку в умовах воєнного стану є одним із найважливіших завдань цього правоохоронного органу в таких складних умовах сьогоднішнього функціонування України.

Усе це потребує належного ефективного управління та злагодженості алгоритмів дій у тих чи інших ситуаціях, розрахунку сил і засобів, матеріально-технічного забезпечення тощо. Але ефективне управління силами та засобами Національної поліції України при забезпеченні публічної безпеки та порядку є неможливим без відповідної підготовки, основою якої є ефективне планування.

Література

1. Забезпечення публічної безпеки і порядку в умовах воєнного стану: матеріали Всеукраїнської науково-практичної конференції (м. Кропивницький, 1 липня 2022 року). Донецький державний університет внутрішніх справ. Кропивницький, 2022. 398 с.
2. Ковалів М.В., Іваха В.О. Діяльність органів внутрішніх справ в умовах воєнного стану. Вісник Національного університету «Львівська політехніка». Серія: Юридичні науки. 2016. № 837. С. 65-70.

Ткач Р.Л.
Національна академія СБ України

АКТУАЛЬНІ ПИТАННЯ ПРОТИДІЇ ІНФОРМАЦІЙНИМ, ПСИХОЛОГІЧНИМ ВПЛИВАМ НА ОСОБОВИЙ СКЛАД СТРУКТУР СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ В УМОВАХ ЗБРОЙНОЇ АГРЕСІЇ

За останні роки, чи навіть століття, розуміння та ведення воєнних конфліктів

суттєво змінилось. Це пов`язано з швидким розвитком інформаційних технологій, та технологій здійснення інформаційно-психологічного впливу (ІПВ). З плином часу, з`явилась потреба у надійному та своєчасному захисті від ІПВ та його деструктивного впливу.

На даний момент, у світі досить міцно закріпилась тенденція випередження, тобто намагатись діяти на декілька кроків попереду супротивника, тож проблема ІПВ постає особливо серйозно, так як несвоєчасне прийняття рішень по запобіганню та усуненню наслідків, можуть завдати колосальної шкоди та втратам серед особового складу. Важливість даного явища для України, стоїть на неймовірно високому рівні, через воєнний стан та бойові дії на території нашої держави, тому ми повинні приймати такі рішення, блискавично та безпомилково.

Зараз спостерігається величезна увага збоку рф, до розробки та впровадження різноманітних способів, форм та технологій ІПВ, на масову та індивідуальну свідомість людей. Ще з самого початку російської агресії в 2014 році, ворог демонстрував різні засоби та методи ведення «гібридної війни».

Насамперед, вплив полягав у комплексі спеціально спланованих та підготовлених дій та операцій, націлених на цивільну та військову інформаційну інфраструктури, свідомість людей, як індивідуальну, так і суспільну її складову, та на морально-психологічний стан, особового складу Збройних Сил України. Перш за все, для того щоб приймати адекватні та своєчасні міри захисту від ІПВ, ми повинні чітко розуміти характер дій супротивника, та прогнозувати його наступні кроки, а при успішному здійсненні впливу, якнайшвидше реагувати на нього.

Останнім часом наукова література, в якій йде мова про цілі, механізми, технології і засоби російської гібридної агресії в Україні та країнах Європи, постійно збільшується, тож в нас з кожним роком виникає все більше і більше можливостей акумулювати досвід не тільки за рахунок своєї історії, а і звернути увагу на роботи вчених та військових інших країн. Варто зауважити, що взаємовідносини України з іноземними партнерами, у секторі безпеки і оборони значно покращились за минулий рік, і ця тенденція тільки набирає обертів, що позитивно впливає на розвиток нашої країни у даній сфері, і наближає нас до довгоочікуваної перемоги.

Для впливу на свідомість противника використовуються різні способи, такі як інтернет-джерела, ЗМІ, аудіо і відеопродукція, друковані листівки чи листи, і звісно вплив за допомогою людей, які спеціально підготовлені для здійснення впливу, цей метод є неймовірно результативним, але потребує високого рівня навичок у людини, яка буде здійснювати ІПВ.

Особливу нішу займають впливові журналісти, військовослужбовці, політичні лідери та представники суспільства, так як користуються довірою своєї аудиторії.

Вдалий інформаційно-психологічний вплив, має негативні наслідки, які призводять до зміни відношення людини до держави та руйнюванню її

особистості.

На особовий склад ЗС України ворог здійснює постійний вплив, з надією змінити їх думку відносно держави та поглядів, які вони захищають, саме через це, проблематика цього питання надзвичайно важлива. Небезпекою також є те, що навіть при десяти відсотковій ефективності застосування ІПВ на людину, викликається висока ймовірність виникнення панічного стану.

Таким чином, об'єктом ІПВ виступає індивідуальна і масова свідомість. Військовослужбовці можуть піддаватись різного роду маніпуляціям за допомогою неправдивої інформації, і як результат, можуть отримати травми пов`язані з психологічним здоров`ям. Досить часто на ділянках ведення інтенсивних бойових дій, військовослужбовці особливо чутливі до дезінформації, так як вони в певній мірі, ізольовані від зовнішнього світу, і не мають змоги перевірити надійність інформації з різноманітних джерел. В таких умовах, людина може перетворитись на здобич в інформаційному полі, задля запобіганню цьому, повинна проводитись робота з особовим складом, яка буде базуватись на морально-психологічному забезпеченні і буде здійснюватись висококваліфікованими спеціалістами.

Подолання проблеми захисту військ від ІПВ супротивника, в сучасних умовах, які є в нашій державі – завдання досить складне, якщо звернути увагу на складну суспільно-політичну і соціально-економічну обстановку в державі. Тому при організації протидії ІПВ, ми повинні не забувати про велику кількість факторів, які можуть вплинути на результат, та проводити активну випереджувальну контрпропагандистську роботу. В подібну роботу, буде входити комплекс заходів, який зможе надійно захистити систему світоглядних стереотипів, орієнтирів чи настанов на яких базується високий Морально Психологічний Стан військ та здатність до опору агресора.

Захист військ від ІПВ противника, є комплексом заходів, що проводяться органами військового та державного управління усіх рівнів, командуючими, командирами, штабами, органами морально психологічного забезпечення (МПЗ) з метою запобігання, нейтралізації та усуненню наслідків такого впливу.

Також, слід ретельно перевіряти осіб які допускаються до роботи на засобах зв'язку і управління. Перш за все, вони не повинні бути психічно неврівноважені, невитримані чи боязкі, так як вплив на таку людину, може тягнути за собою наслідки набагато більшого масштабу, аніж на звичайного військовослужбовця або цивільну людину.

Командири відіграють не менш важливу роль в формуванні опору на вплив противника. Командир повинен рішуче припиняти прояви чуток чи поширення панічних настроїв, знищувати листівки які містять дезінформаційні матеріали. Військовослужбовці, які піддались деморалізації, повинні бути ізольовані від особового складу, до відновлення у них нормального стану.

Варто зазначити і роботу психологів, так як саме вони повинні працювати з військовими, першочергово як інформування та інструктаж особового складу, а

вже потім при потребі, задля роз'яснення та покращення психологічного та морального стану військовослужбовця.

Основою на якій можливе створення дієвих методів протидії дезінформації та різного роду деструктивних впливів, є знання своєї історії, що створить достатньо великі проблеми нав`язуванню ворожих наративів, які базуються на історичному факторі, та духовно-етичні цінності які створились за весь час існування нашої культури та державності, такі як, патріотизм, честь або Батьківщина. Кваліфікація і професійні навички війська, також важливі, тому що військовослужбовець який виконує свою роботу на високому рівні, в змозі протидіяти пропаганді в декілька разів краще.

Підсумовуючи все вище сказане, можна зробити висновок, що ІПВ - це досить серйозна зброя, яка стоїть на рівні з кулеметами та іншим озброєнням, так як впливає на свідомість людини, минаючи спротив при вдалому її застосуванні, якого не минути звичайним збройним шляхом.

Як було зазначено, ми виходимо на новий рівень відносин з нашими іноземними партнерами, і тому, ми в змозі дізнатись багато чого нового з їх моделі протидії ІПВ, і поєднати наш досвід з цими знаннями, що зможе значно покращити наші навички у цьому питанні.

Література

1. Агресія Росії проти України: історичні передумови та сучасні виклики / П.П. Гай-Нижник, Л.Л. Залізняк,І.Й. Краснодемська, Ю.С. Фігурний, О.А. Чирков, Л.В. Чупрій. – К.: МП Леся, 2016. – 586 с.

2. Історія інформаційно-психологічного протиборства / Я.М. Жарков, Л.Ф. Компанцева, В.В. Остроухов, В.М. Пет-рик, М.М. Присяжнюк, Є.Д. Скулиш. – К.: Науково-видавницький відділ НА СБ України, 2012. – 212 с.

3. Основи протидії інформаційно-психологічному впливовів особливий період / П.П. Ткачук, В.В. Шемчук,Ю.П. Сальник та ін. – Львів: НАСВ, 2015. – 189 с.

4. Власюк О.С. Національна безпека України: Еволюція проблем внутрішньої політики: Вибр. наук. праці /О.С. Власюк. – К.: НІСД, 2016. – 528 с.

5. Баровська А. Інформаційні виклики гібридної війни: контент, канали, механізми протидії / А. Баровська. – К.:НІСД, 2016. – 109 с.

6. Стасюк В.В. Психологічне забезпечення діяльності військ (сил) / В.В. Стасюк. – К.: НУОУ, 2014. – 504 с.

Ткаченко В.А.,
к.військ.н.,
ЦНДІ ЗС України
Ільяш А.О.,
ЦНДІ ЗС України
Єфименко Г.А.,
Національний університет оборони України

ВЕДЕННЯ ІНФОРМАЦІЙНОЇ КОМПАНІЇ РОСІЙСЬКОЮ ФЕДЕРАЦІЄЮ ПРОТИ УКРАЇНИ

З початком широкомасштабного військового російського вторгнення в Україну значно активізувалася інформаційна компанія, яку рф розпочала з 2014 року. Її значна частина пов'язана з масовим розповсюдженням на підконтрольних рф інформаційних ресурсах хибної або викривленої інформації, з метою створення в інтересах рф у різних цільових аудиторіях штучного уявлення про події та процеси, які відбуваються в ході військового конфлікту в Україні.

Мета доповіді полягає в тому, що на основі аналізу методів ведення інформаційної компанії, які застосовує рф для досягненні політичних і військових цілей у гібридній війні проти України, розробити пропозиції щодо протидії їй.

З початком широкомасштабного вторгнення в Україну інформаційна компанія рф трансформувалася, набула явної агресії та почала суперечити загальноприйнятій думці про ефективний вплив і комунікацію з боку уряду чи оборонних джерел, які традиційно наголошують на важливості правди, достовірності та уникнення протиріч.

До основних методів ведення інформаційної компанії рф проти України можна віднести:

– "Спрощення" (перетворення складного на просте) у поєднанні із "підміною понять" (прийняття об'єкту за таке, яким він не є). З часом, спрощений та підмінений вислів вкорінюється і починає функціонувати в суспільстві як єдино вірний. Аналіз використання термінів "демілітаризація" та "денацифікація" на початку війни показав, що більша частина населення рф не сприйняла їх значення [1]. З метою просування масової підтримки війни в російському інформаційному просторі з'явилася нова термінологія: замість "війна" – "спеціальна військова операція", "денацифікація" – "боротьба з неонацистами та фашистами", "захоплення територій" – "звільнення від нацистів", "ЗСУ" – "бойовики, каратели, нацики", "Верховна Рада" – "київська хунта", "відступ" – "жест доброї волі", "вибух" – "хлопока" тощо. Доказом того, що рф використовує слово "нацизм", як інформаційну зброю у своїх цілях став аналіз американського Центру штучного інтелекту Semantic Visions бази даних 8 мільйонів статей про Україну, які зібрано з понад 8000 російських сайтів з 2014 року [2].

– “Апелювання до страху” (зловживання почуттям страху використовується для підтримки пропозиції) тісно пов'язане із “фальшивою дилемою» (вихід із жахливої ситуації подається як єдина альтернатива пропонованому рішенню). Основні російські твердження, які лунали напередодні війни: “захід сформував в Україні антиросію, яка загрожує безпеці Росії”; “спецоперація” в Україні – це удар на випередження, адже руками України “колективний Захід” та США мали завдати шкоди Росії”; “Україна мала намір напасти на Білорусь, це була лише справа часу”; “Україна 8 років обстрілює Донбас”.

– “Брехня” (умисне введення в оману) та “викривлена реальність” (маскування під інформативність під виглядом об’єктивної реальності). Викривлена російська реальність полягає в тому, що їхнє суспільство звикло жити в агресивно-мілітаристському світі, винуватити в усіх внутрішніх негараздах, проблемах політичного, соціально-економічного характеру “колективний” Захід та США. Наведемо найбільш емоційні та абсурдні російські твердження, які є повністю вигаданими та покладаються на сфабриковані докази: “Україна не є самостійною державою, вона перебуває під зовнішнім управлінням та під владою маріонеток Заходу”; “на Україні при фінансування США діяли лабораторії з розробки військової біологічної зброї та збудників смертельних хвороб”; “нацисти-азовці прикриваються цивільними як живим щитом”; “Польща починає захоплення західних областей України”.

– “Вигаданий факт” (повідомлення факту, який не можна перевірити або отримати будь-яких свідчень) у поєднанні із “обходом з флангу” (присутність у фейкових повідомленнях конкретних деталей, що роблять їх переконливими). В публічних зведеннях МО рф вказує “точні адреси” місць дислокації підрозділів ЗСУ, “які розміщуються в небезпечній близькості до цивільних об’єктів” на кшталт: “В Одесі на території школи № 100 (Варненська) підрозділи ЗСУ розмістили бронетехніку, важку артилерію та РСЗО, по периметру розташували блокпости, при цьому евакуація мешканців не проводилася”. Протидіють цьому місцеві мешканці, які викривають такі “факти” разом із блогерами, що мають велику кількість підписників у соціальних мережах [3].

– “Замовчування” (приховування небажаної інформації, щоб знизити психологічний опір з боку суспільства та створити певну “перемогу”) та “витіснення” (відволікання уваги від важливих подій на менш значущі).

– “Ефект первинності” (дезінформація доведена до цільових аудиторії раніше, ніж правда) у поєднанні із “багатократним повторенням” дають поштовх у сприйнятті довіри та надійності джерела розповсюдження.

На основі проведеного аналізу методів ведення інформаційної компанії розроблені пропозиції на коротко, середньо та довгострокову перспективу щодо протидії їй, які ґрунтуються на Стратегії інформаційної безпеки держави та не суперечать її загальним цілям та напрямам реалізації [4].

1. Пропозиції для протидії методам ведення інформаційної компанії рф на

короткострокову перспективу:

– розроблення та постійне функціонування системи моніторингу з метою своєчасного виявлення, прогнозування та протидії поширенню дезінформації, спрямованої на запобігання, максимально швидке реагування держави і суспільства на деструктивну пропаганду;

– постійний аналіз будь-яких медіа-середовищ для виявлення ресурсів, які формують негативну думку різних цільових аудиторій з метою своєчасної протидії ним;

– запровадження дієвих механізмів виявлення, фіксації, обмеження доступу та/або видалення з українського сегмента мережі Інтернет інформації, розміщення якої обмежено або заборонено законом.

2. Пропозиції для протидії методам ведення інформаційної компанії рф на середньострокову перспективу:

– забезпечення ефективного функціонування системи стратегічних комунікацій. Зв'язки з українськими та іноземними ЗМІ щодо висвітлення заходів із забезпечення національної безпеки, відсічі і стримування збройної агресії. Це сприятиме кращому розумінню міжнародними партнерами внутрішньої і зовнішньої політики держави, забезпечить міжнародну підтримку України;

– створення тимчасових робочих груп з психологів, істориків, соціологів та медіаекспертів для розробки програм, промо-заходів, конференцій тощо довкола історичної спадщини Другої світової війни та радянської епохи. Спростування дезінформації ідеології радянської та сучасної російської історіографії, щодо минулого і сучасного України та її територій.

3. Пропозиції для протидії методам ведення інформаційної компанії рф на довгострокову перспективу:

– розробка та запуск спеціалізованих національних програм, просвітницьких кампаній, що сприятимуть розвитку критичного мислення, інформаційної стійкості та медіа грамотності. Основними орієнтирами є формування системного розуміння ведення сучасних мережевих, телевізійних інформаційно-комунікаційних протистоянь в інформаційному просторі;

– сприяння процесам практичної підготовки та постійного вдосконалення умінь та навичок фахівців із питань протидії деструктивної пропаганди.

На основі проведеного аналізу наведених методів ведення інформаційної компанії рф проти України, слід зробити висновок, що вони мають високий потенціал та значну ефективність впливу. Цей потенціал з використанням медійних технологій в інформаційній компанії використовується для встановлення контролю над свідомістю громадян, дискредитації ЗС України, вищого керівництва нашої держави, її політики, економіки, культури, як усередині країни так й на міжнародній арені. Запропоновані у тезах пропозиції на коротко, середньо та довгострокову перспективу щодо протидії російській методам ведення інформаційної компанії рф проти України допоможуть протистояти їй та значно

зменшать негативний вплив на різні цільові аудиторії.

Література

1. Рубин М., Ареніна Є. Як Росія виявилася не готовою до війни. - URL: https://www.proekt.media/narrative/kak-planirovali-voinu.

2. Смарт Ч. Як російські ЗМІ поширюють неправдиві твердження про українських нацистів,2022.-URL: https://www.nytimes.com/interactive/2022/07/02/ world/europe/ukraine-nazis-russia-media.html.

3. Казанський Д. Мешканці Одеси викрили брехню МО рф. URL: - https:// www.youtube.com/watch?v=vGaUAe-XS8g.

4. Указ президента України від 28 грудня 2021 року №685/2021 «Про Стратегію інформаційної безпеки».

Ткачук Н.І.
к.ю.н.,
доцент кафедри ІБД
ННІ ІБ СК НА СБ України

ПРОГНОЗУВАННЯ ТА ВИЯВЛЕННЯ ІНФОРМАЦІЙНИХ ЗАГРОЗ В СИСТЕМІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ВОЄННІЙ СФЕРІ

Широкомасштабне військове вторгнення рф на територію України підтвердило статус інформаційної сфери як системоутворюючої. Без сумніву, за цей час інформаційна безпека посіла «чільне місце в загальній структурі воєнної безпеки держави, а система її забезпечення – одне з ключових місць у СЗВБД (системі забезпечення воєнної безпеки держави – *авт.*) [1, С. 58]. Адже саме через інформаційний простір решта сфер воєнної безпеки держави, військово-технічна, воєнно-економічна тощо, зазнають впливу інформаційних загроз. Останні можуть мати нищівні наслідки для воєнної безпеки та національної безпеки держави. Своєчасне виявлення та усунення інформаційних загроз безпосередньо впливає на забезпечення воєнної безпеки держави. Саме цим зумовлена потреба в ефективній системі забезпечення інформаційної безпеки у воєнній сфері у загальній структурі воєнної безпеки держави.

Слід погодитися, що найбільш досконалі та потужні системи забезпечення інформаційної безпеки побудовані й успішно функціонують у тих країнах, які змушені створювати національні системи інформаційної безпеки, постійно перебуваючи під потужним зовнішнім інформаційним впливом (США, Велика Британія, Ізраїль. ФРН, Китай). Таким системам властивий ряд спільних ознак. Визначальне значення має активна складова, завдяки якій існує можливість проведення результативних інформаційно-психологічних операцій та

кібернетичних атак проти держав противників. Водночас, як свідчить аналіз найбільш характерних підходів до побудови систем забезпечення інформаційної безпеки у збройних силах провідних країн світу, важливою складовою таких систем є функціональна підсистема, орієнтована на вирішення наступних завдань:

- виявлення загроз інформаційний безпеці;
- аналіз і прогнозування загроз інформаційній безпеці;
- планування заходів протидії загрозам інформаційній безпеці;
- захисту від загроз ІБ;
- активного впливу; наукових досліджень та підготовки спеціалістів із питань інформаційної безпеки [2, С. 54].

На сьогоднішній день прогнозування та виявлення інформаційних загроз у воєнній сфері окреслено у Стратегії інформаційної безпеки України, зокрема, в контексті інформаційних заходів оборони держави. Останні визначено як сукупність скоординованих дій щодо прогнозування та виявлення інформаційних загроз у воєнній сфері, запобігання, стримування та відсічі збройній агресії проти України, протидії інформаційним загрозам з боку держави-агресора, а також здійснення інших необхідних дій в інформаційному протиборстві [2]. Такі заходи готуються та здійснюються суб'єктами забезпечення національної безпеки і оборони України в мирний час, в особливий період, в умовах воєнного або надзвичайного стану

Під час російсько-української війни потужний негативний інформаційний вплив, якого Україна зазнає фактично з набуття незалежності, сягнув апогея. Можна прогнозувати, що після її завершення, нинішні тенденції не лише збережуться, а й посилюватимуться. Тому побудова повнофункціональної системи забезпечення інформаційної безпеки у воєнній сфері, із врахуванням іноземного досвіду, національних та геополітичних чинників, сприятиме подальшому розвитку вітчизняної системи інформаційної безпеки держави. При цьому створення цілісної функціональної підсистеми, орієнтованої на виявлення та прогнозування інформаційних загроз, дозволить створити достатні можливості для завчасного прогнозування розвитку подій у сфері забезпечення воєнної безпеки держави, а також дозволить здійснювати ефективне планування, принаймні, на середньострокову перспективу.

Література

1. Левченко О. В. Система забезпечення інформаційної безпеки держави у воєнній сфері: основи побудови та функціонування : монографія /О. В. Левченко. – Житомир : Видавець ПП "Євро-Волинь", 2021. - 172 с.

2. Стратегія інформаційної безпеки України: Указ Президента України від 28 грудня 2021 р. № 685/2021. URL: https://www.president.gov.ua/documents/6852021-41069 (дата звернення: 14.03.2023).

Томашевський О.С.
Національний університет оборони України імені Івана Черняховського

СПОСОБИ ПСИХОЛОГІЧНОГО ВПЛИВУ НА МАСОВУ СВІДОМІСТЬ ВІЙСЬКОВОСЛУЖБОВЦІВ ЗБРОЙНИХ СИЛ УКРАЇНИ

На відміну від інформаційного впливу на органи військового управління, витонченим і винахідливим з точки зору його реалізації є психологічний вплив на масову свідомість військовослужбовців виглядає більш прямолінійним та агресивнішим і має таку спрямованість:

акції залякування противника (демонстрація військової могутності, політичного тиску, економічної блокади, згортання культурних і наукових контактів в соціальних мережах);

критика та збудження сумнівів серед військовослужбовців у правильності зовнішньої і внутрішньої політики країни в месенжерах;

засудження моральних і військових поглядів політичного, військового керівництва та лідерів держави, підрив їх авторитету, а також довіри до них в очах військовослужбовців в соціальних мережах та месенжерах;

дискредитація військово-політичної теорії, військової доктрини, військових концепцій;

формування серед особового складу збройних сил негативного ставлення до можливої війни;

розпалювання політичної, національної, релігійної, етнічної ворожнечі між різними групами особового складу збройних сил;

пропагування політичної, військової, економічної, технологічної, інформаційної переваги своєї держави і її союзників;

спонукання військовослужбовців до антигромадських вчинків, що дестабілізують нормальне повсякденне життя армії;

поширення серед військовослужбовців релігійних і націоналістичних забобонів;

ініціювання сумнівів серед особового складу в доцільності ведення бойових дій;

дезінформація військовослужбовців щодо реального стану справ на полі бою;

спонукання військовослужбовців до симуляції, дезертирства й самовільного залишення району бойових дій;

створення паніки, масових психозів, настроїв поразки серед військовослужбовців.

Основними прийомами здійснення психологічного впливу на військовослужбовців, особливо у фазі загострення відносин між державами до необхідності застосування воєнної сили, є такі [1]:

роз’яснення катастрофічних наслідків війни для країни в цілому, для окремої

людини (воїна) і його сім'ї;

нагнітання страху бути вбитим або отримати тяжкі фізичні каліцтва;

стимуляція почуття "стомленості від війни";

навіювання думки про можливість дезертирства;

акцентування уваги на реальних або вигаданих протиріччях між різними етнічними категоріями чи соціально-психологічними групами у збройних силах;

роз'яснення безглуздості опору;

заклики до непокори, масового саботажу, дезертирства, капітуляції.

Інформація такого спрямування поширюється за допомогою листівок, радіо- і телемовлення, Інтернету, засобів мобільного і гучномовного зв'язку, а також іншими каналами розповсюдження інформації. Техніка передачі таких повідомлень у ході бойових дій може змінюватися, але інформаційний сенс залишається незмінним – припинити бойові дії (опір) противником [2].

Базовими методами психологічного впливу, які застосовуються стосовно військовослужбовців, є переконання й навіювання.

Переконання – це метод впливу на свідомість людей, який звернений до їх власного критичного сприйняття і полягає у логічному обґрунтуванні певного судження або висновку. Застосовуючи метод переконання, виходять із того, що він орієнтований на інтелектуально-пізнавальну сферу людської психіки. Його сутність полягає у тому, щоб за допомогою логічних аргументів спочатку домогтися від людини її внутрішньої свідомої згоди, а потім на цій основі сформувати й закріпити нові установки (або трансформувати старі), що відповідають поставленій меті впливу.

У ході здійснення переконання цільової аудиторії (об'єктів інформаційно-психологічного впливу) додержуються наступних правил:

логіка переконання повинна бути доступною рівню інтелекту об'єкта впливу;

переконання здійснюється, спираючись на факти, що відомі об'єкту впливу;

крім конкретних фактів і прикладів інформація у переконанні містить й загальні положення (ідеї, принципи);

інформація, що викладається у переконанні, має вигляд максимально правдоподібної;

факти і загальні положення повинні викликати емоційну реакцію об'єкта впливу.

Таким чином, критерієм результативності психологічного впливу є переконаність об'єкта впливу (цільової аудиторії). Це глибока впевненість в істинності засвоєних ідей, уявлень, понять, образів. Вона дозволяє приймати однозначні рішення й здійснювати їх без коливань, займати тверду позицію в оцінках тих або інших фактів і явищ. Завдяки переконаності формуються установки людей, що визначають їхнє поводження в конкретних ситуаціях.

Література
1. Горбулін В.П. Проблеми захисту інформаційного простору України: Монографія / В.П. Горбулін, М.М. Биченок // Ін-т пробл. нац. безпеки. – К.: Інтертехнологія, 2009. – 136 с.
2. Інформаційна безпека (соціально-правові аспекти): Підручник / Остроухов В.В., Петрик В.М., Присяжнюк М.М. та ін. // За заг. ред. Є.Д.Скулиша. – К.: КНТ, 2010. – 776 с.

Федорчук В.Г.
Національна академія СБ України

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ЯК ОДИН ІЗ ВАЖЛИВИХ ЗАСОБІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ВОЄННОГО СТАНУ

Рівень проведення інформаційного забезпечення в умовах воєнного стану відбивається не тільки на єдності та національній свідомості особового складу збройних формувань структур сектору безпеки і оборони України (далі – збройних формувань ССБОУ), їх готовності до тривалої боротьби з агресором, а і на морально-психологічну підтримку військових підрозділів на передовій. Негативною тенденцією на сучасному етапі війни з агресором є недосконаліть комплексного системного підходу до інформаційного забезпечення як такої, яка не відповідає ступеню загрози.

Незважаючи на те, що питання інформаційного забезпечення є одним із ключових питань інформаційної безпеки держави, функціонування цієї системи в умовах воєнного стану досліджено недостатньо та потребує систематизації та ґрунтовного наукового забезпечення.

Існують серйозні виклики щодо інформаційного супроводження збройних формувань ССБОУ. Недосконале забезпечення інформаційної підтримки та протидії відбивається на зниженні морально-психологічної готовності до активних бойових дій, згуртованості в умовах військової агресії противника, віри в перемогу.

Пріоритетними напрямами інформаційного забезпечення *в умовах* воєнного стану є:

- ✓ визначення сил та засобів реалізації системи інформаційного забезпечення;
- ✓ координація визначених структур та осіб, відповідальних за інформаційне забезпечення особового складу;
- ✓ виявлення інформаційних загроз щодо зниження боєготовності та морально-психологічного стану особового стану військових підрозділів;
- ✓ створення умов для формування патріотичного відношення особового

складу збройних формувань, їх відданості та готовності до захисту Батьківщині;

- ✓ інформування особового складу щодо воєнної обстановки в районах бойових дій, способів протидії інформаційно-психологічних впливів рф;
- ✓ роз'яснення особовому складу прийнятих нормативно-правових документів, інструкцій, що стосуються усіх сфер необхідного забезпечення бойових дій;
- ✓ роз'яснювальна робота з питань зовнішньої політики України у сфері надання військової та гуманітарної допомоги;
- ✓ підтримання і розвиток національних традицій України;
- ✓ здійснення моніторингу стану інформаційного забезпечення тощо.

Інформаційне забезпечення в умовах воєнної агресії повинно спрямовуватися для підвищення рівня обізнаності особового складу у питаннях:

- ➢ оперативних новин агресії рф проти *України* та останніх найважливіших зведень *бойових дій;*
- ➢ *героїчних вчинків наших співвітчизників* в ім'я свободи й незалежності України*;*
- ➢ *продовольчого, речового, грошового забезпечення військових підрозділів; наявністю необхідного для перемоги озброєння;*
- ➢ першочергових завдань та здобутків усіх гілок влади;
- ➢ досягнень у боротьбі з корупцією;
- ➢ державної допомоги переселенцям тощо.

Основними принципами інформаційного забезпечення є:

- ➢ об'єктивність інформації;
- ➢ боротьба з дезінформацією;
- ➢ оперативність та зрозумілість доведення інформації;
- ➢ безперервність;
- ➢ плановість, системність та послідовність;
- ➢ розвиваючий характер та зворотний зв'язок.

Основними завданнями інформаційного забезпечення є:

- ➢ формування патріотизму, прагнення до перемоги, підвищення рівня відповідальності за виконання покладених обов'язків;
- ➢ усвідомлення воєнної політики України, рішень керівництва держави, командирів (начальників) військових формувань, цілей та завдань, які стоять перед особовим складом;
- ➢ роз'яснення місця і ролі особового складу у забезпеченні обороноздатності держави, специфіки виконання визначених завдань за призначенням;
- ➢ захист особового складу від негативного впливу інформації рф, пов'язаної з маніпуляціями та дезінформацією;

- розвиток системи морально-духовних цінностей, досягнення необхідного рівня громадянської, моральної свідомості для ефективного виконання поставлених завдань шляхом поширення прикладів мужності, героїзму, взаємодопомоги;
- формування правової поведінки особового складу військових формувань в умовах підвищеного ризику для життя;
- підвищення комунікації з питань соціального і правового захисту військовослужбовців та членів їх сімей.

Слід зауважити, що, саме у воєнний час потреба у наданні особовому складу військових формувань *ССБОУ* необхідної інформації надзвичайно велика. Особовий склад стикається з багатьма проблемними питаннями, які не в змозі зрозуміти або вирішити. До того ж агресор систематично вкидає інформацію, спрямовану на деморалізацію, дезорганізацію та зневіру у перемозі. У даній ситуації начальники усіх рівнів виступають в ролі арбітра, наставника, фахівця, побратима, які повинні аналізувати, робити висновки та надавати посильну допомогу, актуальну інформацію з рекомендаціями, пропозиціями, інструкціями тощо.

Невід'ємною складовою інформаційного забезпечення при постійній агресії рф проти України є підтримання емоційної складової військових колективів, спрямованої на підвищення стресостійкості особового складу та збереження самовладання в умовах постійного стресу.

Отже, під час повномасштабної війни проти України інформаційне забезпечення має бути для особового складу *збройних формувань ССБОУ* носієм патріотизму, національної ідентичності та гуртування навколо головних моральних цінностей – непохитності в перемозі України, готовності до самопожертви в ім'я незалежності України, прагнення жити у своїй власній країні.

Література

1. Указ Президента України від 28 грудня 2021 року № 685/2021 Стратегія інформаційної безпеки.

2. Наказ Генерального штабу Збройних Сил України від 04.01.2017 № 4 Про затвердження Інструкції з організації інформаційно-пропагандистського забезпечення у Збройних Силах України.

3. Мужанова Т. М. Інформаційна безпека держави: навч. посіб. Київ, 2019. 131 с.

4. Інформаційна безпека особистості, суспільства, держави: підручник / Жарков Я. М., Дзюба М. Т., Замаруєва І. В. та ін. Київ : Видавничо-поліграфічний центр «Київський університет», 2008. 274 с.

5. Богуш В. М., Кривуца В. Г., Кудін А. М. «Інформаційна безпека: термінологічний навчальний довідник» / за ред. Кривуци В. Г. Київ, 2004. 508 с.

Черниш Р.Ф.
к.ю.н., доцент, доцент КІБД,
Національної академії СБ України
Сидоренко Д.С.
студент Національної академії СБ України

МІФ ПРО ТЕ, ЩО УКРАЇНА РОСІЯ ТА БІЛОРУСЬ – ЄДИНИЙ НАРОД

24 лютого 2022 року змінило життя українців на до і після. Після повномасштабного вторгнення росії в Україну в нашій державі було запроваджено правовий режим воєнного стану. Як наслідок, надзвичайно велика кількість прав громадян України була обмежена, що не відповідає Конституції України. Це все відбулось внаслідок того, що путінський режим перейшов всі рамки дозволеного та, нажаль велика частина людей, що проживають на території росії, підтримали ці воєнні дії. Також не будемо забувати про ще одних наших «сусідів», які боялись протирічити країні-агресору та стали на її бік. Білорусь з перших днів висловила підтримку дій росії та навіть була готова також йти в наступ проти України, але доки це не сталось. Проте неодноразово з даної країни випускали ракети в бік України, що досі гублять життя українців. Чи можна вважати цю країну агресором? Однозначно так, оскільки вони приймають росіян на навчання до себе та всіляко допомагають країні-терористу в багатьох питаннях , що стосуються війни.

Міф, який вигаданий дуже багато років про те, що Україна, росія та білорусь є братськими народами не має зараз жодного значення і ніяка людина не буде вважати, що це правда. Ми не можемо бути одним народом тільки через те, що ми розуміємо їхню мову та колись слухали їхню музику. Російська пропаганда наголошує на дружбі народів, їх спільній боротьбі в минулі часи, визначає ворогів, які заважають Україні та росії бути разом. Але вони не розуміють, що у України є чіткий вибір – бути в Європейському Союзі.

Слід зазначити, що міфи про «братні народи» чи «єдиний народ» – абсолютно штучні, а концепція «братніх народів – це витвір радянської пропаганди на заміну російської імперської концепції «триєдиного народу». Це спроба знов насильно прив'язати українську історію до російської та заперечити право українців і білорусів на власний історичний вибір.

Україна не залежить від росії, як би росії цього не хотілося**.** Українці швидко почали скидати з себе ярмо енергетичної залежності. Анексія Криму та події на сході України також значно обвалили рівень доброго ставлення до росії. Російські пропагандисти давно знали, що між державами палають мости. Тож постійно вигадували міфи про те, чому ми маємо «бути разом» на правах «молодшого брата». Але Україна самостійна, а у**країнці – сучасна політична нація.**

Україна, росія та білорусь - є різними країнами зі своєю унікальною історією,

культурою, мовами та політичними системами. Хоча ці країни мають певні культурні та історичні зв’язки через їхнє минуле як частини Радянського Союзу, вони не є єдиною нацією.

По-перше, Україна, росія та білорусь мають різні мови. Офіційною мовою України є українська, а в Росії та Білорусі – російська. Білорусь також визнає білоруську державною мовою. Мовні відмінності відображають різні культурні особливості та історію кожної країни.

По-друге, ці країни мають різні політичні системи. Україна — парламентська республіка, росія — федеративна напівпрезидентська республіка, а білорусь — президентська. Кожна країна має свої унікальні політичні традиції та інститути, що відображають різний історичний досвід і сучасні обставини.

По-третє, Україна, росія та білорусь мають відмінну культурну та історичну ідентичність. Україна має багату культурну спадщину та довгу історію боротьби за незалежність і державність. Росія має культурну ідентичність, яка була сформована її величезною територією, різноманітними етнічними групами та довгою історією. Білорусь також має свою самобутню культуру, мову та фольклор.

Підсумовуючи, слід зазначити, що хоча Україна, росія та білорусь мають деякі спільні риси, що сформувалися в часи СРСР, вони не є єдиною нацією. Кожна країна має свою особливу культурну, мовну та політичну ідентичність, яка відображає її унікальну історію та традиції.

Література

1. Чому українці та росіяни історично – не «братні народи» (інфографіка). Український інститут національної пам'яті - офіційний веб-сайт. URL: https://uinp.gov.ua/informaciyni-materialy/rosiysko-ukrayinska-viyna-istorychnyy-kontekst/chomu-ukrayinci-ta-rosiyany-istorychno-ne-bratni-narody-infografika (дата звернення: 03.03.2023).

2. Розвінчуємо історичні міфи : чому Українці з росіянами ніколи не були братськими народами - офіційний веб-сайт. URL:https://ranok.ictv.ua/ua/2022/04/07/rozvinchuyemo-istorichni-mifi-chomu-mi-z-ukrayintsi-z-rosiyanami-nikoli-ne-buli-bratskimi-narodami/ (дата звернення: 03.03.2023).

Чеховська М.М.,
д.е.н., проф.,
Кирилюк О.С.,
к.т.н., ст. дослідник,
Лісовська О.Л.,
к.е.н., доц.
Національна академія Служби безпеки України

ВИКОРИСТАННЯ СОЦІАЛЬНИХ МЕРЕЖ У ЗБРОЙНІЙ АГРЕСІЇ РОСІЇ ПРОТИ УКРАЇНИ

До початку повномасштабного вторгнення російської федерації на територію України 24 лютого 2022 року, соціальні мережі, на думку вітчизняних науковців, використовувалися здебільшого як інструмент інформаційно-психологічних операцій. У той же час практично з дня повномасштабної російської навали, соціальні мережі стали зброєю як в руках нападників, так і захисників Української держави.

Так, аргументом на користь першого твердження є використання соціальних мереж, зокрема, месенджерів Instagram, TikTok, Twitter, Facebook, Telegram, Viber, WhatsApp, YouTube на користь загарбників за умов розміщення у зазначених мережах інформації про розташування військовослужбовців, військової техніки, стратегічних об’єктів, руху вантажів тощо, а після обстрілів – публікація в мережі світлин з обсягами пошкоджень, у тому числі, з метою коригування подальших обстрілів. Крім того, непоодинокими були випадки викладання світлин в месенджерах із зазначенням геолокації вказаних об’єктів.

Є багато свідчень про отримання з месенджерів, у тому числі підлітками у формі он-лайн гри, інструкцій із розставлення так званих «міток», радіолокаційних пристроїв, сигнальних засобів, що використовувалися росіянами для завдання повітряних ударів як по об’єтах критичної інфраструктури, так і для просування окупаційних військ.

Серед аргументів для другого твердження, а саме використання месенджерів українцями як зброї у війні за свою незалежність, виступає перш за все, на нашу думку, громадянська активність мешканців нашої держави.

Так, саме через соціальні мережі повідомляється інформація про пересування ворожих військ, пункти дислокації окупантів та логістичні шляхи, актуалізується напрямок польоту «Шахедів», надаються достовірні відомості про діяльність органів державної влади, поширюється інформація про збір коштів для потреб сил оборони тощо.

Крім того, через соціальні мережі оприлюднюється інформація спеціально для росіян про умови здачі в полон українським військовим; здійснюється пошук та ідентифікація російських окупантів.

Окремою складовою є використання месенджерів військовослужбовцями сектору безпеки і оборони України.

Так, корисною практикою є, на наш погляд, досвід Міністерства оборони США, де розроблено та впроваджено посібник із захисту в соціальних мережах для забезпечення безпеки і конфіденційності особового складу підрозділів [1]. Забороненою до публікації у месенджерах є інформація щодо: подробиць місії підрозділу та його безпекових аспектах; місця та часу розгортання підрозділів; смерті військовослужбовця до того, як буде повідомлено найближчих родичів і інформація буде оприлюднена Міністерством оборони США; пошкодженого обладнання та спорядження; проблем морального духу підрозділу тощо [2].

Крім того, у жовтні 2022 року було оголошено про нову політику Міністерства оборони США у сфері використання армією соціальних мереж [3]. Так, зазначена політика визначає, якою інформацією військовослужбовці можуть ділитися у своїх особистих облікових записах і з яких облікових записів можуть робити дописи армійські посадові особи. Документом також вимагається додаткове навчання для персоналу, прозорість під час видалення публікацій і обмеження на використання нових, неперевірених платформ соціальних мереж до того моменту, як вони будуть офіційно перевірені [4].

У той же час не можна обійти увагою заборону, зокрема, Єврокомісією, Європарламентом, США, Канадою та Данією використовувати на службових телефонах додаток TikTok, адже існують побоювання, що особисті дані можуть бути використані з неправомірною метою, а сам додаток є елементом шпигунської програми [5].

Таким чином, соціальні мережі, зокрема, сучасні месенджери, широко використовуються у війні, розв’язаної російською федерацією проти України. Варто наголосити на подвійному характері використання месенджерів, адже технології, що використовуються окупантами, не менш ефективно застосовуються й проти них. Зважаючи на зазначене, важливою передумовою користування соціальними мережами є забезпечення власної інформаційної гігієни та здійснення просвітницької роботи щодо заходів безпеки під час використання соціальних мереж.

Література

1. Social Media Protection: A Handbook For Security And Privacy Settings. 2021 Edition. URL : https://www.army.mil/e2/downloads/rv7/socialmedia/social_media_protection.pdf. (дата звернення: 11.03.2023).

2. U.S. Army Social Media Guide. Safety and Security Guidance. URL : https://www.army.mil/socialmedia/safety/ (дата звернення: 27.09.2022).

3. Army Social Media Policy. URL : https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN36766-ALARACT_0732022-

000-WEB-1.pdf. (дата звернення: 27.09.2022).
4. Jonathan Lehrfeld. New Army Social Media Policy Pushes Stricter Rules. URL : https://www.militarytimes.com/news/your-military/2022/10/31/new-army-social-media-policy-pushes-stricter-rules/ (дата звернення: 27.09.2022).
5. Давід Ель. Як країни Заходу забороняють TikTok у державних установах. URL : https://www.dw.com/uk/dedali-bilse-krain-zaboronaut-vikoristovuvati-tiktok-u-derzavnih-ustanovah/a-64852059. (дата звернення: 27.09.2022).

Чеховська М.М.,
д.е.н.,
професор, завідувач кафедри ФЕБ
Національної академії СБ України
Косянчук М.І.,
студент Національної академії СБ України

ГРОМАДЯНСЬКА ВІЙНА В УКРАЇНІ ЯК ГОЛОВНИЙ ФЕЙК рф

Актуальність дослідження полягає в тому, що повномасштабне вторгнення держави-агресора російської федерації ведеться не лише на полі болю, але й в інформаційному середовищі, оскільки там ведеться боротьба не за територію, а людей, що там проживають, за їх свідомість та почуття. Дане дослідження буде присвячено аналізу політичного міфу/фейку про громадянську війну в Україні, як одного із компоненту гібридної війни проти України, так і в загальному контексті війн інформаційного (постіндустріального) періоду.

Інструмент політичної міфології, який цілком усвідомлено задіяний в інформаційних війнах і оснований на знанні людської природи. Автори «Політологічного енциклопедичного словника» так визначають цей феномен: «Політичний міф – стійкий витвір із штучно створеним уявленням про реальні соціально-політичні феномени і дії, навмисно або ненавмисно прикрашені різними припущеннями, вигадками, фантазією…». При цьому, політика стає раціональною формою використання ірраціональної сутності мас. Тому керування масою спирається на знання архетипу, найдавніших психічних установок, основних емоційних станів.

До політичних міфів належать також фейкові новини. Фейк-ньюз – це те, що протистоїть правилам, які підтримують суспільний лад, і навіть підривають їх. Фейк-ньюз є повідомленням, стилістично створеним як справжня новина, але є хибним повністю або частково.

Одним із головних і найвідоміших фейків держави-агресора є наратив, що в Україні триває громадянська війна. Таку тезу російські пропагандисти почали

розвивати після того, як українці остаточно визначилися із західним вектором, що не влаштовувало російську федерацію.

У класичному варіанті громадянська війна визначається як війна за владу всередині держави між різними соціальними групами. Проте, варто зазначити, що для громадянської війни характерним є об'єктивні умови та великий процес непорозуміння щодо внутрішньополітичного життя. Коли ми говоримо про події 2013-2014 рр. в Україні, то об'єктивних передумов зіткненню народних мас Сходу та Заходу України не було. Навпаки, у січні-лютому 2014 р. на вулицях багатьох міст Донбасу, зокрема Донецьку, можна було побачити багатотисячні проукраїнські мітинги на підтримку України.

Пропагандистський штамп «громадянська війна в Україні» можемо розділити на три складові, які взаємопов'язані: «не Революція Гідності, - а державний переворот, влаштований нацистами в Києві при підтримці колективного Заходу»; «громадянська війна» почалася через бажання людей «Південно-Східної України» залишитися частиною «руського миру» та говорити російською»; «Росія – не сторона конфлікту на Донбасі».

З аналізу даних можемо зробити висновок про те, що пропагандистські ідеї рф мають вертикальний характер: ідея вигадується у високих кабінетах Кремля, а уже потім її ретранслюють рупори пропаганди на федеральних телеканалах.

Для того, щоб розвінчати зазначений фейк, то основу доказової бази складають вислови та факти, які були представлені російською стороною або її прихильниками, також наведено нейтральні загальновідомі факти та твердження.

Перша теза – в Україні відбувся державний переворот. Державний переворот – одна з форм насильницької зміни існуючого політичного режиму неконституційним шляхом. У політологічному сенсі державний переворот завжди призводить до ще більшого насильства. У цьому контексті події Революції гідності як до, так і після не призвели до політики «закручування гайок», не було оголошено ні надзвичайного, ні воєнного стану в державі. Інший аспект, на який треба звернути увагу: повалення режиму Януковича відповідає ліберальній доктрині та міжнародному праву, яке базується на природньому праві. Ще один аргумент полягає у тому, що росія визнала нову владу в Україні. Таку позицію держави прокоментував голова МЗС, Сергій Лавров.

Друга теза - участь росіян у військовому конфлікті. Ігор Стрєлков (Гіркін) – колишній так званий міністр оборони квазідержавного утворення «ДНР», даючи коментар одному із російських видань говорить про роль росії, її армії та свою власну в подіях початку війни на Донбасі. Він також заявив, що важливу роль у бойових діях відіграли російські військовослужбовці, які нібито приїхали на Донбас, перебуваючи «у відпустці».

Третя теза пропагандистського наративу – утиски російської мови та взагалі російськомовних в Україні. Головним їх доказом цього є пропагандистський художній фільм «Крим». Справа у трьох складових цього фільму: по-перше,

режисер цього фільму – О. Піманов за сумісництвом – гендиректор пропагандистського телеканалу Міноборони рф «Звезда»; по-друге, фільм було знято за гроші міністерства оборони рф, а міністр оборони С. Шойгу особисто брав активну участь в розробці сценарію фільму; по-третє – фільм, нібито, засновано на реальних подіях, що зазначається у кінцевому титрі стрічки. Сюжет фільму намагається поєднати усі міфи та фейки з 2014 року. Однак найцікавіші події розгортаються щодо питання мови. Російська пропаганда стверджує, що за російську мову бендерівці можуть вбити, хоча у фільмі усі (навіть «націоналіст Микола») говорять ідеальною російською, що піддає сумніву цей російський наратив.

У висновку можемо зазначити, що у процесі розвінчування міфу навіть посилання на російські джерела ЗМІ та публічних людей дозволили зробити висновок про те, що російські наративи та пропагандистські кліше не мають доказової бази, не витримують навіть уточнюючих запитань, які можна зробити на основі їх заяв чи вчинків.

Література

1. Требіна М. П., Герасіна Л. М., Погрібна В. Л., Поліщук І. О. Політологічний енциклопедичний словник. Вид.: Право. 2015. – 816с.

Чіпуріна Г.М.
старший викладач кафедри інформаційної безпеки держави
ННІ ІБ СК Національна академія Служби безпеки України

РОЗВИТОК МЕДІАГРАМОТНОСТІ ЯК ЗАХИСТ ВІД ДЕСТРУКТИВНИХ ІНФОРМАЦІЙНИХ ВПЛИВІВ

Сьогодні у зв’язку із швидкоплинним зростом темпів інформатизації людство знаходиться на етапі формування та розвитку глобального інформаційного суспільства, характерними рисами якого є стрімкий прогрес у сфері цифрових технологій та, як результат, значне розширення доступу громадян до різноманітних інформаційних ресурсів, серед яких, в тому числі, соціальні медіа. Створення умов для розвитку інформаційного суспільства в Україні є сьогодні одним із основних напрямів державної інформаційної політики [1], який розширить можливості рівного доступу громадян до інформації та забезпечить реалізацію ними інформаційних прав.

Разом з очевидними перевагами, стрімкий розвиток інформаційного простору, зокрема, соціальних мереж, несуть певні виклики та загрози, такі як глобальні дезинформаційні кампанії, що особливо посилилися у зв’язку з веденням рф війни проти України, масованими деструктивними інформаційними

впливами – дезінформаціями, маніпуляціями, залякуванням.

У Стратегії інформаційної безпеки України визнано, що значне розширення джерел доступу до інформації в умовах стрімкого розвитку цифрових технологій та водночас недостатнього рівня медіаграмотності (медіакультури) супроводжується зменшенням критичності сприйняття інформації, створює підґрунтя для можливих маніпуляцій громадською думкою, що сприяє зростанню впливу дезінформації та деструктивної пропаганди, популярності конспірологічних теорій [2] У зв'язку з цим, підвищення рівня медіаграмотності визнано однією із стратегічних цілей Стратегії, спрямованих на забезпечення інформаційної безпеки.

Актуальні проблеми інформаційного простору України, роль засобів масової інформації у розвитку та становленні медіаграмотності досліджено у роботах О.Литвиненко, Д.Вербицького, Ю.Сікори, Ю.Руденко та ін.

В.Різун вважає, що медіаграмотність – це результат медіаосвіти, і є тотожним поняттям «медіакомпетенції» [3]. Його підтримує О.Тугарова, яка досліджує зв'язок медіаграмотності та медіаосвіти [4].

Відповідно до досліджень ГО «Детектор медіа», опублікованих у 2021 році, медіаграмотність 15% українців є низькою, у третини (33%) — нижча за середню, 44% аудиторії характеризує вищий за середній рівень медіаграмотності і 8% — високий. Дослідження виявили залежність рівня медіаграмотності від освіти. Чим нижчим є освітній статус, тим нижчим є й рівень медіаграмотності. Так, серед опитаних із загальною середньою освітою частка осіб із показником низьким та нижчим за середній складає 63%, а серед тих, хто має повну/ неповну вищу освіту, — лише 30% [5].

Однак потребує подальшого вивчення питання розвитку медіаграмотності як механізму протидії деструктивним інформаційним впливам.

Член Національної ради України з питань телебачення і радіомовлення О.Ніцко вважає медіаграмотність важливим чинником у протистоянні загрозам інформаційної війни і підкреслює важливість систематичної реалізації проектів з медіаграмотності [6].

Варто відзначити, що в останні роки кількість проєктів із розвитку медіаграмотності постійно зростає. Особливо зазначені проєкти важливі в галузі освіти. Разом з тим дослідники повідомляють, що рф постійно вдосконалює форми та методи ведення інформаційної війни проти України, наприклад, поширення дезінформації [6]. У зв'язку з чим пропонується систематичне впровадження проектів з розвитку медіаграмотності, що є актуальною вимогою сьогодення та необхідною складовою освітнього процесу у сучасному демократичному суспільстві, зокрема:

- створення державної системи підтримки проектів медіаграмотності;
- впровадження медіаграмотності в освітні програми на різних рівнях;
- здійснення популяризації медіаграмотності серед населення;

- сприяння діяльності громадських організацій з поширення медіаграмоотності.

Література

1. Про Інформацію: Закон України від 2 жовтня 1992 року № 2657-XII URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text
2. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України від 28.12.2021 № 685/2021https://zakon.rada.gov.ua/laws/show/685/2021.
3. Медіаосвіта та медіаграмотність: підручник / Ред.-упор. В. Ф. Іванов, О. В. Волошенюк; За науковою редакцією В. В. Різуна.— Київ: Центр Вільної Преси, 2013. — 352 с.
4. Тугарова О. К. Медіаосвіта як фактор забезпеченя інформаційної безпеки // Актуальні проблеми інтелектуального, інформаційного, інтернет права та ІТ права: збірник матеріалів П'ятої Всеукраїнської науково-практичної конференції (Львів, 28 травня 2021 р.) – Львів: Юрид.фак.-т Львівського національного університету ім. І.Франка – 2021. – 224 с.
5. Індекс медіаграмотності українців: аналітичний звіт за результатами комплексного дослідження, ГО «Детектор медіа», 2023 р., режим доступу: https://detector.media/doc/images/news/archive/2021/186435/UA_REPORT_MEDIALITERA%D0%A1Y_INDEX-DM.pdf
6. Росія винайшла нові способи поширення своєї дезінформації, режим доступу: https://www.unian.ua/world/rosiya-vinayshla-novi-sposobi-poshirennya-svoyeji-dezinformaciji-analitiki-12001620.html

Чіпуріна Г.М.
старший викладач кафедри інформаційної безпеки держави
ННІ ІБ СК Національна академія Служби безпеки України
Кіценко Р.С.
студент Національної академії СБ України

ДЕСТРУКТИВНІ ВПЛИВИ рф НА ІНФОРМАЦІЙНИЙ ПРОСТІР КРАЇН ЗАХОДУ

В останні десятиліття цивілізований світ зіткнувся із загрозою великого масштабу – деструктивними російськими інформаційними впливами. Кремлівські керманичі обрали наступальну стратегію інформаційно-психологічного протиборства із Західним світом. Провідні країни Заходу довгий час не приділяли достатньої уваги можливим викликам на інформаційному фронті з боку російської федерації, користуючись зростанням глобального виробництва, підіймали рівень

власного добробуту. Виявивши вразливість до російського зловмисного інформаційного впливу, демократичний світ почав шукати шляхи захисту і протидії. Успіх у цій боротьбі має безпосередній зв'язок із успіхом нашої держави у відбитті російської агресії. Сьогодні російські інформаційно-пропагандистські впливи на шкоду Україні здійснюються у трьох основних напрямках: в інформаційному просторі України, у власному інформаційному просторі агресора, до якого інтегровано інформаційний просторі республіки Білорусь, та тимчасово окупованих територій, а також в інформаційному полі країн Заходу. При чому в останньому випадку об'єктом впливу є зарубіжна аудиторія, а кінцевою метою – нанесення шкоди Україні. Позбавлення України західної підтримки через дискредитацію українського керівництва, ЗСУ і навіть українських біженців [1], є першочерговим пріоритетом агресора, тому ми маємо докладати зусиль для своєчасного виявлення та знешкодження російського зловмисного впливу на Західний світ.

Сучасна росія опанувала радянські стратегії інформаційного протиборства та пристосувала їх до нових реалій глобалізованого світу. Більше того, тепер вона не обмежена ідеологічними рамками, тривалий час їй вдавалось імітувати миролюбну демократичну державу та не сприйматись як однозначний ворог Заходу. Глобальна мережа та супутникове мовлення не мають кордонів, сучасне інформаційне поле набагато складніше контролювати, а отже росія оволоділа можливостями проводити активні заходи у будь-якому куточку світу.

Сьогодні у інформаційному просторі місце радіо та друкованих ЗМІ посіли онлайн медіа. На відміну від років Холодної війни, більшість європейських урядів, особливо у країнах Західної та Південної Європи, перестали вважати росію істотною загрозою, а отже підігравали її проникненню у їхній інформаційний простір протягом перших десятиліть 21 століття. Російські інформаційні ресурси встигли завоювати широку аудиторію у цих країнах. За відсутності яскравої ідеології (як її мав срср), російська пропаганда змогла створити у її споживачів «когнітивний фільтр», який використовує конспірологічні теорії та викликає появу категоризації «свій/чужий» (стосовно людей, поглядів, цінностей), що проявляється у непримиренності та поляризованості позицій тих, хто піддався її впливу. У них формується «альтернативне світосприйняття», яке відкидає будь-які факти, що не вкладаються у цей світогляд та пригнічує здатність до критичного мислення. Після цього, будь-яка дезінформація, навіть найбільш безглузда та алогічна, може сприйматись як істина [2].

Російські наративи мало чим відрізняються від колишніх радянських. Топ п'ять тем російської дезінформації за версією Державного Департаменту США наступні: «занепад західної цивілізації неминучий», «росія невинна жертва, яка змушена оборонятись від агресивних дій Заходу», «народні рухи у інших країнах – це фінансовані Сполученими Штатами проекти кольорових революцій», «росія – держава-переможець нацизму», «у будь-якій події за участі рф не все так

однозначно (у цей час російська пропаганда вигадує сотні суперечливих версій подій для розпорошення уваги і спантеличення аудиторії)». Особи, що сприйняли ці наративи можуть діяти у російських інтересах, а саме: голосувати за крайні радикальні політичні сили, що пропонують послаблення партнерства з США / ЄС / НАТО, виходити на акції протесту проти окремих урядових ініціатив (рух «жовтих жилетів» у Франції), підтримувати проросійських кандидатів на виборах, виступати за реалізацію російських проектів (обхідні газопроводи), протистояти впровадженню антиросійських санкцій тощо [3].

Окремої уваги заслуговує російський вплив у кіберпросторі. Інноваційною тактикою інформаційного впливу є використання «ботоферм» у соціальних мережах. Маси акаунтів несправжніх людей (які однак видають себе за резидентів цільової країни) залишають сотні коментарів та публікацій розроблених російськими пропагандистами у всіх куточках інтернету. Люди, які потрапляють під постійний потік дезінформації від різних джерел схильні рано чи пізно повірити у неї. Дослідження Pew Research Center показало, що 86 відсотків американців отримують новини із смартфону, а їх переважна більшість використовує для цього соцмережі. Серед них 70 відсотків підтвердили, що читають коментарі під публікаціями [4]. Інше дослідження віднайшло залежність між негативними коментарями та рівнем довіри до джерела та достовірності інформації. Довіра значно падає, якщо більшість не підтримує історію [5]. Саме тому найчастіше російські боти залишають негативні та провокативні коментарі. Вони поширюють плітки та наклеп на окремих державних діячів, критикують політику уряду, розпалюють ненависть серед прихильників протилежних політичних таборів / етнічних / релігійних / соціальних груп тощо.

Новітні технології надають нові можливості для використання підробок. Фабрикування графічних матеріалів стало набагато простішим для виконання та складнішим для викриття. Дослідник А. Халкуп та ін. наводять схему виробництва такої підробки. Спочатку зловмисники отримують доступ до якогось приватного/секретного документу. Потім вони модифікують його зміст, щоб донести потрібне повідомлення. Надалі вони зливають цей документ (а краще цілий пакет) у мережу, зберігаючи його реальне походження. Такий злив виглядає як звичайний витік документів, проте у дійсності закидається підробка, яка досягає своєї мети, адже виглядає як автентичний документ.

У площині інформаційного впливу росія перейняла усі елементи радянських «активних заходів» та пристосувала їх до новітніх технологій. Скориставшись образом дружнього партнера, росія здобула лояльну аудиторію у середині європейських країн, доступу до якої колишній Радянський Союз не мав. Тепер вона невпинно транслює дезінформацію та пропаганду, в тому числі, на шкоду інформаційній безпеці України, впливаючи на громадську думку за допомогою супутникового телебачення і соціальних мереж. Головними методами російської інформаційної війни є: маніпулятивний характер повідомлень, використання

підставних медіа, сталі наративи визначені керівництвом, використання внутрішніх суперечностей у середині суспільства цільової країни, апелювання до емоцій, поширення теорій змови, підробка документів, масований потік фейків, використання вад алгоритмів соціальних мереж (ботоферми, підставні групи/канали тощо), кібератаки та викрадення секретної інформації.

Література

1. Від брехні та мови ненависті до насильства. Як російська пропаганда атакує українських біженців URL: https://spravdi.gov.ua/vid-brehni-ta-movy-nenavysti-do-nasylstva-yak-rosijska-propaganda-atakuye-ukrayinskyh-bizhencziv/(24.03.2023).
2. Asmolov. G. Why Propaganda Survives in the 21st Century: Eight Points about Russian Propaganda. [Electronic source]. – LSE, 07.06.2022. – URL: https://blogs.lse.ac.uk/medialse/2022/06/07/why-propaganda-survives-in-the-21st-century-eight-points-about-russian-propaganda/ (06.03.2023).
3. Russia's Top Five Persistent Disinformation Narratives. US Department of State. [Electronic source]. – URL: https://www.state.gov/russias-top-five-persistent-disinformation-narratives/ (06.03.2023).
4. Shearer E., Mitchell A. News Use Across Social Media Platforms in 2020 [Electronic source]. – Pew Research Center, 12.01.2021. – URL: https://www.pewresearch.org/journalism/2021/01/12/news-use-across-social-media-platforms-in-2020/ (06.03.2023).
5. Waddel. T. What does the crowd think? How online comments and popularity metrics affect news credibility and issue importance. [Electronic source]. – Sage Journals, 2017. – URL: https://journals.sagepub.com/doi/full/10.1177/1461444817742905 (06.03.2023).

Шевченко А.М.
КНУ імені Тараса Шевченка

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Закон України Про критичну інфраструктуру та її захист встановлює принципи та напрями розбудови державної системи захисту критичної інфраструктури, визначає правові та організаційні засади забезпечення її діяльності і є складовою частиною законодавства України у сфері національної безпеки [1]. Об'єкти критичної інфраструктури (енергетичні, транспортні, телекомунікаційні, кредитно-фінансові системи, системи газо- і водопостачання) є складними, просторово розподіленими, багатокомпонентними системами, стійка

робота яких критично важлива для функціонування економіки та життєдіяльності суспільства й держави. Об’єкти критичної інфраструктури (ОКІ) мають багаторівневу структуру, яка включає: рівень технічних компонентів (машини, обладнання та апаратура); соціальний рівень (персонал, що обслуговує технічні компоненти ОКІ) ; організаційний рівень (взаємодія служб компанії, що експлуатує об’єкти) та рівень державного управління (нормативні та контролюючі органи, які здійснюють нагляд та державне регулювання у сфері діяльності ОКІ). Складність критичних інфраструктур обумовлюється: складністю їх структури (складними взаємозалежностями та нелінійними зв'язками між компонентами та рівнями системи, а також між різними ОКІ); складним характером явищ та процесів, що мають місце в ході експлуатації ОКІ [2].

Елементами ОКІ є технічні об'єкти, на яких здійснюються зберігання, переробка/перетворення або транспортування/передача небезпечних речовин, енергії та/або інформаційних потоків. Ці об'єкти можуть бути джерелами важких аварій і катастроф, які є предметом традиційного аналізу ризиків, на основі якого будуються карти ризиків для територій розміщення об'єктів критичних інфраструктур і приймаються рішення про будівництво або їх модернізацію.

Наявність тісних взаємозв'язків між компонентами ОКІ є їх важливою особливістю, яка надає визначальний вплив на характер їх функціонування в штатних і позаштатних ситуаціях. З одного боку, пов'язаність елементів ОКІ підвищує їхню ефективність, дозволяючи раціонально використовувати та перерозподіляти наявні ресурси та потужності, а з іншого - робить їх схильними до великомасштабних катастроф, величезний розмір збитків від яких не дозволяє нехтувати ними, незважаючи на низьку ймовірність реалізації ризиків.

Щодо аналізу ризиків взаємопов'язаних інфраструктурних систем доводиться мати справу з двосторонніми залежностями між компонентами ОКІ, тому прийнято говорити про взаємозалежність елементів ОКІ. Ці взаємозалежності існують як для елементів, що належать до однієї інфраструктури, так і для елементів, що належать до різних інфраструктур. В останньому випадку говорять про взаємозалежності між різними ОКІ. Відповідно розрізняють каскадні сценарії, що реалізуються всередині окремих інфраструктур, та міжінфраструктурні каскади, які (завдяки наявності міжінфраструктурних зв'язків) можуть поширюватися по всій сукупності інфраструктурних систем та призводити до колапсу в цілому регіоні.

Наявність сильних зв'язків між елементами ОКІ робить їх схильними до каскадних сценаріїв аварій, які охоплюють велику кількість об'єктів інфраструктури, причому хід реалізації аварії визначається структурою зв'язків між елементами. Крім масштабів потенційних аварій, наявність внутрішньо- та міжінфраструктурних залежностей надає визначальний вплив на динаміку поширення аварій, призводячи до реалізації комбінованих механізмів досягнення граничних станів, різкої інтенсифікації процесів деградації та потоку відмов

елементів ОКІ.

Через складну структуру ОКІ та складний характер взаємодій між значною кількістю елементів можливості проведення сценарного аналізу за допомогою традиційного інструментарію (дерев подій, дерев відмов, байєсових мереж) виявляються обмеженими. Для опису розвитку збурень у критичних інфраструктурах застосовуються мережеві моделі, які активно використовують математичний апарат теорії графів. Мережі є надзвичайно гнучкою абстракцією, яка може широко застосовуватися при вивченні інфраструктурних систем. При цьому може бути побудована ієрархія математичних моделей різної складності, що дозволяють описати різні аспекти ризиків інфраструктурних систем по відношенню до можливих впливів, що ініціюють. За допомогою зазначених моделей вдається описати багато властивостей та особливостей мережевих систем: хаос, самоорганізація, статечні розподіли, критичність [3].

Завдяки бурхливому розвитку інформаційних технологій в останні десятиліття ОКІ стають все більш складними. Це означає, що на оцінку безпеки ОКІ впливає дуже багато чинників. Внаслідок складних нелінійних взаємодій між компонентами ОКІ, сильної зв'язаності між різними підсистемами, а також того факту, що ОКІ та навколишнє середовище починають змінюватися швидше, ніж вони можуть бути описані та досліджені. Тому виникає ситуація нестачі інформації про ОКІ і, отже, обмеженість можливостей прогнозування їх поведінки та управління ними. При цьому на певних режимах неможливо детально описати закони функціонування і розробити правила управління.

Відмінність між повністю визначеними та не повністю визначеними системами стає надзвичайно важливою при розробці комплексу заходів щодо безпеки. Особливість не повністю певних систем у тому, що виявляється неможливим повний опис їхньої поведінки та прогнозування їх стану за різних умов та на різних режимах експлуатації. Внаслідок цього для таких складних систем, як критичні інфраструктури практично неможливо створити закритий перелік проектних впливів, яким система може піддатися протягом її експлуатації. У зв'язку з цим традиційна стратегія забезпечення безпеки ОКІ, заснована на розробці комплексу захисних бар'єрів, які враховують проектні впливи, але динамічне середовище спотворює ці впливи і не може бути успішною.

Тому необхідно розробити методи забезпечення безпеки, що дають змогу мати справу з недовизначеними системами. При цьому повинні використовуватися підходи, що розвиваються в рамках поняття, що отримало назву теорія забезпечення кіберстійкості технічних систем до екстремальних впливів. Ця поняття концентрує увагу на створенні систем, які здатні: продовжувати (принаймні частково) виконувати запропоновані ним функції після того, як вони зазнають пошкоджень, зазнавши запроектних впливів; досить швидко відновлювати свій вихідний функціональний рівень після запроектного впливу.

Стійкість до екстремальних впливів є ключовим поняттям у випадках запроектних впливів та запроектних сценаріїв аварій у складних технічних системах, до яких належать ОКІ. Сучасні інфраструктурні системи (системи водо-, електро- і газопостачання, транспортні, телекомунікаційні мережі) стають дедалі складнішими, взаємозалежними, які динамічно змінюються, дедалі більше виявляють нелінійні властивості. У зв'язку з цим стає неможливо заздалегідь - при проектуванні - спрогнозувати багато несприятливих подій або їх поєднання, а також сценарії відмов, які вони ініціюють, і, отже, заздалегідь передбачити повний комплекс захисних заходів, що дозволяє побудувати системи захисту від вичерпного переліку запроектних впливів/сценаріїв. При цьому на перший план виходить завдання підвищення кіберстійкості інфраструктурних систем до проектних впливів. Традиційні заходи щодо зниження ризику та забезпечення безпеки технічних систем, що передбачають створення систем захисту від проектних впливів та аварій, повинні доповнюватися заходами щодо забезпечення стійкості до запроектних впливів та аварій.

Після великомасштабної катастрофи довкілля може зазнати істотних змін (приклад Чорнобильська АЕС), тому може виникнути необхідність, щоб інфраструктурна система, що розглядається, не поверталася до вихідного стану, а адаптувалася до умов, що змінилися, і вийшла на рівень, що відрізняється від вихідного.

Існуючі в даний час методики безпеки технічних систем розроблені для систем, що мають чіткі межі і добре визначені переліки загроз. Для цих систем можуть бути створені бази даних зі статистики аварій, які дозволяють кількісно оцінювати та верифікувати моделі. Ці методики, що базуються на побудові сценарних "дерев" (моделі типу "дерево" подій, "дерево" відмов), були розроблені без урахування запроектних впливів і не дозволяють належним чином врахувати складність критичних інфраструктур, функціонування яких визначається взаємодією технічних, організаційних та соціальних. факторів.

Традиційний підхід до моделювання аварій не дозволяє описувати сценарії відмов у складних системах, які, як правило, відбуваються не внаслідок окремої події, що ініціює (технічної відмови елемента системи або помилки оператора), а є наслідком декількох взаємопов'язаних факторів, що діють на різних рівнях системи . Дослідження критичних інфраструктур як соціо-технічних систем потребує оцінки складних взаємодій між технічними, соціальними та організаційними рівнями системи. Тому ОКІ слід розглядати як єдине ціле. При цьому необхідно наголошувати на одночасному спільному розгляді технічних, організаційних та соціальних факторів, що визначають стан системи та динаміку її розвитку. Щоб забезпечити безпеку таких систем, необхідно вийти за рамки традиційного підходу до оцінки проектних ризиків та перейти до нової парадигми, що ґрунтується на забезпеченні безпеки ОКІ за критерієм кіберстійкості до запроектних впливів. У зв'язку з необхідністю включити до розгляду запроектні

аварії на ОКІ, рамки досліджень мають бути суттєво розширені. Заходи щодо забезпечення безпеки повинні бути спрямовані не тільки на створення захисних бар'єрів, які дадуть можливість попередити реалізацію проектних аварій, але і на підвищення кіберстійкості та живучості ОКІ у разі запроектних впливів, тобто зосередитися на запобіганні великомасштабних катастроф і тривалих перерв у функціонуванні.

Можливість запроектних впливів, що мають низьку ймовірність реалізації та тяжкі наслідки, має враховуватися під час проведення оцінок захищеності критичних інфраструктур. Це вимагатиме реалізації додаткових заходів, спрямованих на підвищення кіберстійкості ОКІ при запроектних впливах.

Необхідно вийти за рамки традиційних моделей оцінки ризиків, заснованих на побудові «дерев» відмов та «дерев» подій, що обмежуються розглядом проектних впливів та проектних сценаріїв розвитку аварій, та почати вивчати реакції ОКІ на можливі запроектні дії. Нова парадигма забезпечення безпеки ОКІ та інших складних систем має концентрувати увагу не тільки на створенні захисних бар'єрів та реалізації охоронних заходів, спрямованих на парирування проектних аварій, а й на підвищенні стійкості ОКІ щодо запроектних аварій. Причому новий підхід до забезпечення безпеки ОКІ, що розробляється, повинен розглядатися не як заміна, а скоріше як доповнення традиційного підходу.

Література

1. Закон України Про критичну інфраструктуру.

2. Slipachuk, L., Toliupa, S., & Nakonechnyi, V. (2019). The Process of the Critical Infrastructure Cyber Security Management using the Integrated System of the National Cyber Security Sector Management in Ukraine. In 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT 2019 - Proceedings (pp. 451–454). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/AIACT.2019.8847877

3. Toliupa, S., Parkhomenko, I., & Shvedova, H. (2019). Security and regulatory aspects of the critical infrastructure objects functioning and cyberpower level assesment. In 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT 2019 - Proceedings (pp. 463–468). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/AICT.2019.8847746.

Шемаєв В.М.
д.військ.н., проф.
доцент кафедри інформаційної безпеки держави
ННІ ІБ СК НА СБ України

МОДЕЛЮВАННЯ СЦЕНАРІЇВ ІНФОРМАЦІЙНОГО УПРАВЛІННЯ З ВИКОРИСТАННЯМ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ MENTAL MODELER

Сучасна інформаційна війна – це війна цінностей, наративів, війна за громадську думку та емоції, війна, що використовує інформацію як зброю. Дезінформація, пропаганда, фейки, вербальне озброєння та роззброєння, лінгвістична агресія, та лінгвістичний збиток, інформаційне гетто, мова ворожнечі тощо – це інформаційні інструменти військового протистояння з боку рф проти України та усього цивілізованого світу.

Актуальності набуває загальна проблема дослідження, розроблення та впровадження в практику діяльності методів інформаційного протиборства з урахуванням інформаційного (в т.ч. рефлексивного) управління процесами прийняття рішень у сфері безпеки із застосуванням сучасних інформаційних технологій.

Концепції інформаційного протиборства базуються на теорії інформаційного управління, яку створено значно раніше. Розглянемо місце та роль інформаційного управління серед інших типів управління. Класифікація типів управління може будуватися на урахуванні особливостей тих компонентів об'єкта управління (точніше, його моделі), на які здійснюється вплив при використанні управління того або іншого типу:

- *інституціональне управління* (спрямоване на зміну припустимих множин дій і результатів дій. Є найбільш жорстким і полягає у тому, що суб'єкт управління цілеспрямовано обмежує множини можливих дій і результатів діяльності об'єкта управління. Такі обмеження можуть здійснюватися явними або неявними впливами – правовими актами, морально-етичними нормами тощо);

- *мотиваційне управління* (спрямоване на зміну цільової функції. Є більш «м'яким», ніж інституціональне і полягає у цілеспрямованій зміні цільової функції об'єкта управління. Такі зміни можуть здійснюватися введенням системи штрафів і/або заохочень за вибір тих чи інших дій і/або досягнення визначених результатів діяльності.);

- *інформаційне управління* (спрямоване на зміну інформації, яку об'єкт управління використовує при прийнятті рішень. Є найбільш «м'яким» (непрямим) у порівнянні з інституціональним і мотиваційним є інформаційне управління. Інформаційне управління – це процес розроблення та реалізації управлінських рішень в ситуації, коли управляючий вплив носить неявний, прихований характер та спрямований на формування у об'єкта управління такого інформаційного

уявлення про ситуацію, на основі якого об'єкт управління як би "самостійно" приймає бажане з точки зору суб'єкта управління рішення та обирає відповідну лінію своєї поведінки. Модель інформаційного управління наведено на рис. 1.1.

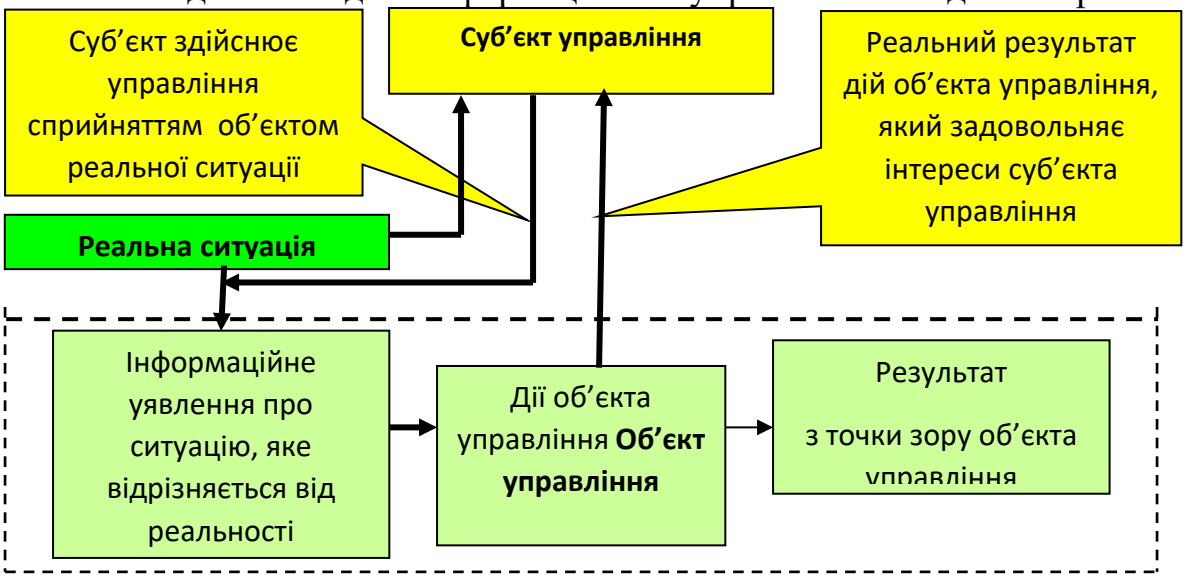


Рис. 1. Модель інформаційного управління

В останні роки інформаційна складова вектора управління знаходить все більше використання. Це обумовлено такими основними чинниками:

потреба в "м'якому" управлінні як найменш помітному;

результати досліджень по психології поведінки людини;

розвиток засобів і технологій інформаційного впливу, зокрема мережі Інтернет.

Інформаційне управління як потужний засіб впливу має ряд переваг, а саме:

- прихованість, яка суттєво ускладнює виявлення факту інформаційного впливу та джерела цього впливу;
- висока вибірковість і в той же час практична відсутність обмежень впливу;
- легка адаптація, швидка перебудова методів і засобів впливу залежно від обставин;
- можливість оперативної концентрації зусиль у визначений час на певному об'єкті, регіоні, соціальній групі;
- порівняльно невеликі витрати на розроблення і реалізацію управлінських рішень.

Інформаційне управління можна класифікувати на види за об'єктами, про які надається інформація:

інформаційне регулювання – цілеспрямований вплив на інформацію про стан природи;

активний прогноз – цілеспрямоване повідомлення про майбутній стан об'єкта;

рефлексивне управління – цілеспрямований вплив на прийняття рішень з

урахуванням психологічних характеристик людини.

Рефлексивне управління, як теорія, у своєму розвитку пройшло чотири періоди: дослідницький (с початку 1960-х років до кінця 1970-х); практично-оріентований (з кінця 1970-х до початку 1990-х); психолого-педагогічний (с початку та до середини 1990-х); психосоціальний (розпочався наприкінці 1990-х). Широке розгортання цих досліджень у значній мірі пов'язано з розробленням фахівцем США В. Лефевром оригінальних ідей, які були народжені у зв'язку з потребами великих проектів у військовій сфері.

Рефлексія в її традиційному філософсько-психологічному розумінні - це здатність встати в позицію «спостерігача», «дослідника» або контролера по відношенню до свого тіла, своїх дій, своїх думок. В. Лефевр розширив таке розуміння рефлексії і запропонував вважати, що рефлексія – це також здатність встати у позицію дослідника по відношенню до іншого суб'єкта, його дій і думок. Таке більш широке розуміння рефлексії дозволяє побудувати цілісний предмет дослідження і виявити рефлексивні процеси як відособлений феномен, який визначає специфіку взаємин «об'єкт-дослідник».

З урахуванням того, що людина не тільки створює, генерує, обробляє інформацію, але є об'єктом інформаційного впливу, змістом рефлексивного управління є процес розроблення і реалізації управлінських рішень в ситуації, якщо вплив має непомітний характер, а об'єкту впливу подається інфор-маційна картина, на підставі якої він самостійно обирає лінію своєї поведінки.

Загальним завданням рефлексивного управління є формування суб'єктом управління такої структури інформованості об'єкта управління, при якій вектор дій об'єкта забезпечує максимальне значення цільової функції суб'єкта. **Тому загальна проблема розроблення методів інформаційного протиборства з урахуванням рефлексивного управління процесами прийняття рішень у сфері національної безпеки набуває для України наукової та практичної актуальності.**

Паралельно з дослідженням рефлексивного управління розвивалась теорія системної динаміки Дж. Форрестера. Математичний апарат методу системної динаміки, заснований на нечітких когнітивних картах, дозволяє проводити аналіз ситуації і синтез стратегій управління нею.

Однак, в існуючих розробках дотепер не створені засоби, які дозволяють враховувати властивості рефлексії і формувати стратегії рефлексивного управління на основі когнітивних моделей, тому необхідна комбінація апарату когнітивного моделювання з моделями рефлексивного управління, що було вперше запропоновано в роботі, що наведено на рис.2. Для реалізації цього методу здійснюється створення імітаційних моделей з використанням сучасних інформаційних технологій, зокрема, за допомогою програмного забезпечення *Mental Modeler* (ментальное моделювання).

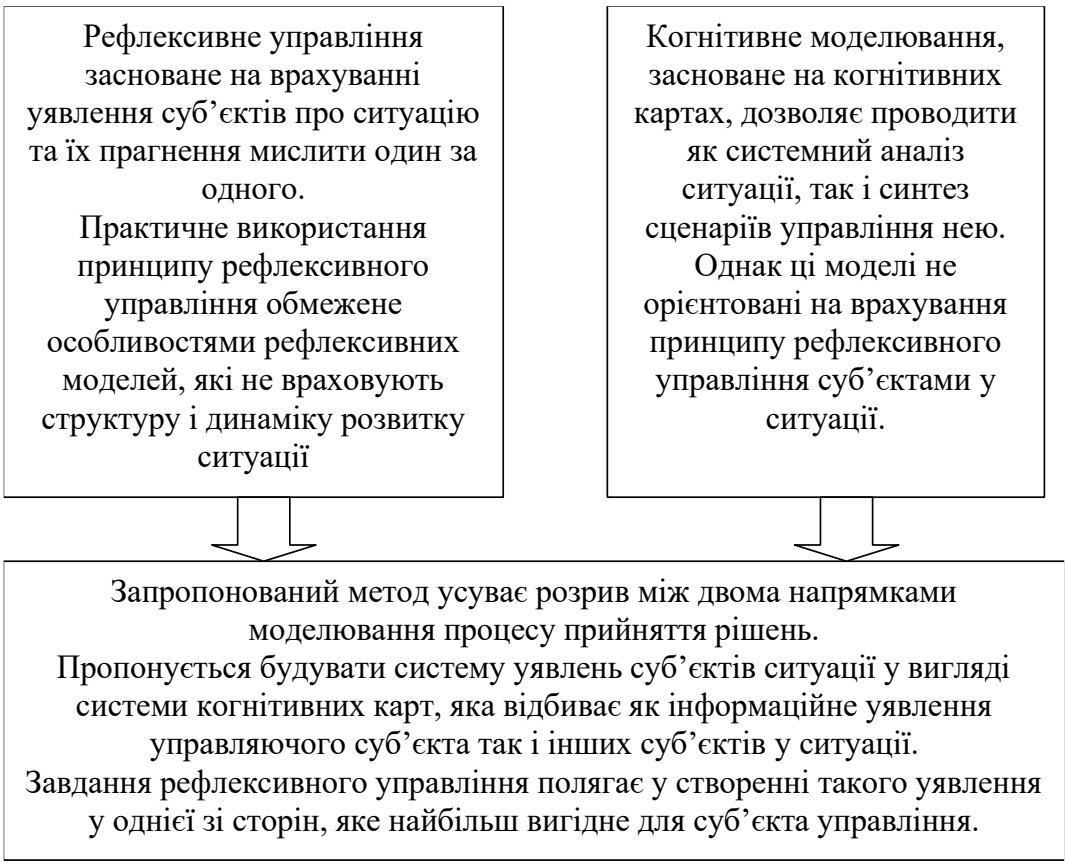


Рис.2. Зміст методу когнітивного моделювання рефлексивного управління

Mental Modeler — це програмне забезпечення для моделювання допомагає окремим особам і спільнотам зберігати свої знання в стандартизованому форматі, який можна використовувати для аналізу сценаріїв управління.

На основі когнітивної карти (рис.3) користувачі можуть легко розробити напівкількісні моделі екологічних, політичних, безпекових, економічних, соціальних проблем в Mental Modeler за наступним алгоритмом:

1. Визначте важливі компоненти системи;
2. Визначте зв'язки між цими компонентами;
3. Запустіть скрипти "що якщо", щоб визначити, як система може відреагувати на ряд можливих змін.

Mental Modeler був розроблений для підтримки прийняття групових рішень, дозволяючи користувачам спільно представляти і перевіряти свої припущення про систему в «режимі реального часу». Крім того, він також використовувався як інструмент дослідження соціальних наук для вимірювання індивідуальних або спільних "ментальних моделей", які часто лежать в основі прийняття людських рішень.

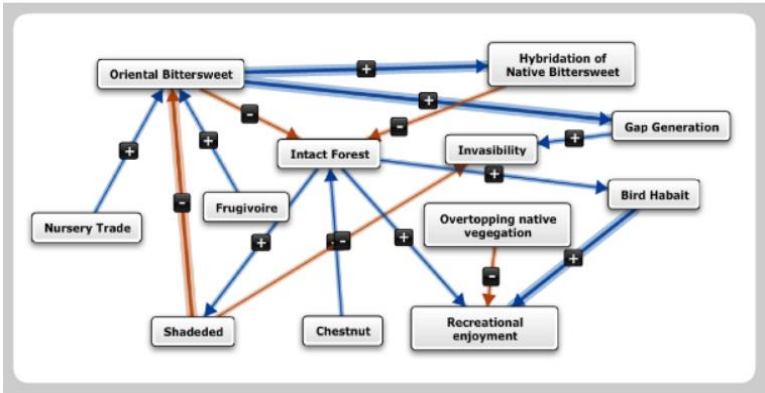


Рис. 3. Схема когнітивної карти, що використовується в *Mental Modeler*

Mental Modeler був розроблений доктором Стівеном Греєм за фінансування Міністерства сільського господарства США та Національного наукового фонду. Працюючи з низкою інших дослідників з різних дисциплін та установ, програмне забезпечення в даний час впроваджується в декількох проектах планування та досліджень на основі громад.

Отже, важливими умовами реалізації національних інтересів у сфері безпеки й оборони в умовах повномасштабної агресії проти України з боку рф є застосування інформаційного протиборства з використанням можливостей інформаційного управління в якості теоретичної основи. Загальним завданням інформаційного управління є формування суб'єктом управління такої структури інформованості об'єкта управління, при якій вектор дій об'єкта забезпечує максимальне значення цільової функції суб'єкта. Застосування при цьому моделювання сценаріїв інформаційного управління з використанням програмного забезпечення mental modeler дозволяє реалізувати це завдання.

Шемаєв В.М.
д.військ.н., професор, доцент КІБД,
Національної академії СБ України
Малко А.О.
студент Національної академії СБ України

МІФ ПРО ТЕ, ЩО РОСІЯ МОГЛА САМОТУЖКИ ПЕРЕМОГТИ У ДРУГІЙ СВІТОВІЙ ВІЙНІ

Розуміння об'єктивної дійсності, запобігання будь-яким спекуляціям та відсутність викривлення історичної правди найголовніше завдання для громадян України та всього цивілізованого світу. Друга світова війна стала найжахливішою подією у XX столітті, її кровопролитні битви увійшли в історію як жорстокі м'ясорубки, які забрали життя мільйонів людей. Загинуло у Другій світовій, за

оцінками істориків, близько 50 мільйонів людей і з них українців – 10 мільйонів. У війні брали участь 62 держави з 73, що існували на той час. Бойові дії велися на території Європи, Азії, Африки та всіх океанів. Гітлерівська Німеччина та її союзники були розгромлені, незважаючи на те, що спочатку проти нацистського блоку виступало близько 20 країн. Лише одна з них вірила, що зможе виграти війну без сторонньої допомоги.

Усі нації колишнього Радянського Союзу зробили свій внесок у перемогу, проте тільки одна колишня республіка зараз в особі російського диктаторського режиму намагається стерти з історії ту неймовірну жертву, яку поклали на вівтар перемоги над нацизмом союзники, зокрема й тодішня Україна та її народ. Путін та його посіпаки вбивають в голову свого народу, що вони були здатні виграти війну самостійно. Проте кожна республіка колишнього Радянського Союзу зробила свій внесок у перемогу, і лише одна колишня республіка розповсюджує міф, що могла б виграти війну самостійно.

Крім того, важливо в деталях розглянути події, які були безпосередньо пов'язані з відкриттям другого фронту, тобто висадкою англійських та американських військ на узбережжі Франції та дійти висновку, яку роль це відіграло в кінцевій перемозі над нацистською Німеччиною.

Міф про те, що Радянський Союз переміг самотужки, відомий не тільки в росії, але і в інших країнах, і має значний вплив на політичну та історичну свідомість суспільства. Мета розвінчування даного міфу полягає в його розкритті та дослідженні фактів, які свідчать про те, що Радянський Союз не міг перемогти війну без допомоги союзників. Розвінчування допоможе краще зрозуміти історичну правду про події Другої світової, оскільки наразі під загрозою історична пам’ять, ідентичність. Російська пропаганда заборонила Україні мати власну історичну перспективу, а будь-яку протидію її імперським ідеям називає «нацизмом». Росіяни хочуть мінімізувати роль інших країн у розгромі нацистів та нівелювати той подвиг народів вільного світу, який вони зробили.

Розповідати людям правду про те, що росія не могла перемогти сама у Другій світовій війні, є важливим з кількох причин:

- по-перше, це допомагає зберегти історичну правду і запобігти маніпулюванню та переписуванню історії;
- по-друге, це допоможе уникнути повторення історичних помилок. Якщо люди будуть свідомі про те, що росія не сама перемогла у Другій світовій війні, то вони будуть розуміти, що війна - це не рішення, а останній вихід, і що потрібно зробити все можливе для того, щоб уникнути війни;
- по-третє, це допоможе змінити спотворене сприйняття історії, яке пропагується в останні роки в Росії. Штучно створювані міфи про славу і велич росії у Другій світовій війні мають на меті змінити історичну свідомість росіян і створити у них відчуття образи та несправедливості. Але без допомоги союзників росія не могла перемогти нацистську Німеччину, і це не позбавляє росіян відваги і

героїзму, які вони виявили під час війни, а лише висвітлює історичну правду;

- по-четверте, розповідати людям правду про історію - це важливо для зміцнення міжнародних відносин і міжкультурного діалогу. Не можна будувати партнерські відносини на базі хибної інтерпретації історії та відхилення від правди. Лише шляхом відкритого та об'єктивного вивчення історії можна досягти взаєморозуміння і поваги між країнами та народами.

Офіційні державні пропагандиські ЗМІ росії активно поширюють ідею генетичної спорідненості радянського солдата і російського військового. Через це російські пропагандисти навмисно поширюють неправдиві матеріали, щоб відобразити українську владу як «фашистську». Такий пропагандистський штамп сприяє створенню ілюзії спадковості, ніби нинішнє покоління вже «бореться з фашизмом» у сучасних умовах так само, як їх діди воювали проти фашизму.

Під час прямого ефіру з президентом росії путіним 16 грудня 2010 року прозвучала всім відома фраза: «Я дозволю з вами не погодитися, коли ви зараз сказали, що якби ми були розділені, ми не перемогли б у війні. Ми все одного перемогли б, тому що ми країна переможців», – заявив путін під оплески.

Посилаючись на статистику часів Другої світової війни, російський лідер зауважив, що «найбільші втрати зазнала саме російська федерація – понад 70 відсотків». Це означає, що війна виграна, не хочу нікого ображати, але за рахунок людських та індустріальних ресурсів російської федерації, заявив володимир путін [1].

Розповсюдження міфу про те, що росія могла перемогти сама у Другій світовій війні може призвести до викривлення історичних фактів та спричинити недооцінку ролі союзників у перемозі над нацистською Німеччиною, міф може призвести до забуття внеску інших народів у перемогу над нацизмом. Це може бути образливим для тих, хто втратив своїх рідних від німецької агресії та боровся на боці союзників. Ну і як наслідок, цей міф може використовуватись для політичних цілей, щоб посилити націоналістичні настрої серед населення та легітимізувати агресивну зовнішню політику, що зараз росія й робить.

Цей міф є деструктивною складовою всієї величезної машини пропаганди рф. Заяву путіна щодо виключної та переможної ролі росії у перемозі над нацизмом у Другій світовій війні, ще у 2010 році прокоментував відомий політолог Володимир Цибулько. «Путін володіє історичним матеріалом тільки в необхідному йому обсязі. Тобто для того, щоб нав’язати власну позицію, а не для того, аби встановити істину. Що вдієш – Україна залишається політичним больовим фантомом для радянської свідомості. А путін саме є носій радянської свідомості. І нинішній російський істеблішмент культивує цю свідомість – незважаючи на те, що зовнішньополітичні обставини, загальний рух історії вже давно її поховав. Радянська свідомість виявилась не просто неконкурентною, вона виявилась тупиковою гілкою розвитку. І такі лідери, як путін, ведуть росію в цей тупик, в оцю безвихідь, - ще й видають це як якусь суттєву перевагу, національну

особливість і світову місію Росії», – співчуває Цибулько [2].

Отже, цей міф є небезпечним для розуміння історії, політики та міжнародних відносин. Важливо продовжувати розповідати правду про роль союзників та внесок різних націй у перемогу над нацизмом, щоб зберегти історичну справедливість та запобігти повторенню історичних помилок.

Література

1. Драч М. Путін: Росія виграла б Другу світову війну і без України [Електронний ресурс] / Мар'яна Драч. – 2010. – Режим доступу до ресурсу: https://www.radiosvoboda.org/a/2250403.html (дата звернення 08.03.2023).

2. Лігостова О. Путін: Росія перемогла б у війні і без України [Електронний ресурс] / Оксана Лігостова. – 2010. – Режим доступу до ресурсу: https://ukrainian.voanews.com/a/putin-2010-12-16-112019064/237398.html (дата звернення 08.03.2023).

Шемаєв В.М.
д.військ.н., професор, доцент КІБД,
Національної академії СБ України
Осика Р.Є.
студент Національної академії СБ України
Кравчук Н.В.
студент Національної академії СБ України

ПОПУЛЯРНІСТЬ АНОНІМНИХ МЕДІА: НЕПЕРЕВІРЕНА ІНФОРМАЦІЯ, ФЕЙКИ ТА ВОРОЖІ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНІ ОПЕРАЦІЇ

З початком повномасштабного вторгнення російської федерації на територію України великого попиту набули медіа-ресурси новинного та експертного характеру. У епоху Інтернету, коли можна спостерігати за подіями з будь-якої точки планети в режимі реального часу, приховувати події з полів бойових дій від великих мас людей стало складніше, ніж це було навіть у минулому столітті. За допомогою інтернету люди можуть миттєво обмінюватись інформацією на великій відстані, факт чого породжує у людей жагу знати оперативну обстановку з місць, де ведуться активні бойові дії, з чого випливають постійні обговорення війни «тут і зараз» у соціальних мережах.

Як наслідок, основним джерелом новин з фронту в українців наразі є соціальні мережі. Не зважаючи на те, що у більшості відомств Сил безпеки та оборони України є акаунти в усіх найпопулярніших соціальних мережах, де викладається достовірна інформація, люди звертаються «на сторону» за «експертною думкою» або «ексклюзивом з місця подій» у контексті війни [1].

У випадках з «експертною думкою», люди хочуть зрозуміти як працюють і чому відбуваються ті чи інші процеси на війні. Однак, не всі хочуть заглиблюватись у даному питанні, звертаючись до наукових робіт, написаних справжніми експертами у галузі, які зазвичай мають військовий досвід та науковий ступінь. На зміну їм приходять, так звані, «диванні генерали» – люди, що зазвичай не мають достатньої кваліфікації у питанні, популістично висвітлюючи події, іноді викривляючи подію так, як це вигідно їм або певному колу людей. Це є небезпечним явищем, адже мало того, що викривлена картина подій шкодить консолідованому суспільству та має безумовні негативні наслідки у тотальній війні, але й може завдяки популістичному поданню інформації сприяти просуванню ворожих наративів [2].

Ще однією проблемою медіа під час війни є подання «ексклюзивного» матеріалу. Правильний та достовірний ексклюзивний матеріал є той, що є акредитованим та перевіреним військовими першоджерелами. Однак, є такі, які не відповідають вимогам воєнного стану або не виконують зобов'язання перед першоджерелом. До прикладу, можна порівняти репортаж журналіста Дмитра Комарова з центру бойового управління Збройних сил України та репортаж катарської телекомпанії «Al Jazeera» з командного пункту на Бахмутському напрямку. Репортаж Комарова відповідає всім вимогам воєнного стану та не несе жодної небезпеки першоджерелу [3]. А у сюжеті «Al Jazeera» не були заблюрені монітори командування, і в такому вигляді цей сюжет вийшов у відкритий доступ, що, можливо, надало додаткову інформацію ворогу на полі бою і несе значну загрозу обороноздатності України. Проте, варто зазначити, що на момент написання роботи знайти цей відеоматеріал в оригінальному вигляді неможливо, адже «Al Jazeera» видалила цей сюжет [4].

Іншою стороною недобросовісних «ексклюзивів» є новинні медіа. Наприклад, можна зазначити новинний портал «ТРУХА», що має багатомільйонну авдиторію у соціальних мережах. Ці медіа відомі своїми фото «прильотів» російських ракет по українській критичній інфраструктурі. Ще з початку повномасштабного вторгнення відомства Сил оборони України наголошували на тому, що громадянам заборонено викладати у мережу фото, відео та будь-яку інформацію про влучання російських ракет деінде, зберігаючи оперативну тишу. Однак такі новинні ресурси, як «ТРУХА», ігнорують ці заклики, і тільки набирають собі більшу авдиторію за рахунок таких «ексклюзивів». З одного боку, такий контент користується попитом у суспільстві, однак з іншого боку, це дає додаткову інформацію ворогу, за допомогою якої наступний ракетний удар може бути скоригований більш точно [5].

Підсумовуючи, можна зробити висновок, що багато з перерахованих факторів медіапростору несуть загрозу визначеному ходу війни у різних масштабах. Це може впливати як на оперативну обстановку бойових дій, так і на суспільні настрої в країні. Безумовно, це питання має стояти на порядку денному, і постійно

моніторитись та регулюватись відповідними державними службами.

Також через збільшення кількості користувачів месенджера Telegram збільшилася і кількість анонімних каналів отримання інформації, які використовують зловмисники та спеціальні служби ворожих до України країн. Так, у березні 2022-го року, Служба безпеки України оприлюднила список анонімних телеграм-каналів (85), які координуються Головним центром спеціальної служби Головного управління Генерального Штабу Збройних Сил рф та спрямовані на проведення інформаційно-психологічних операцій проти населення України [6].

Загалом месенджер Telegram став основним джерелом інформації для українців і росіяни використовують його, щоб посіяти сумніви, недовіру та страх в Україні. Велика кількість анонімних медіа-ресурсів спричинила появу значної кількості фейкової та недостовірної інформації, яка негативно впливає на свідому оцінку ситуації та подальші дії [5].

Отже, під час повномасштабної війни та воєнного стану поширення чуток та брехливої інформації, що викликає емоційні реакції у користувачів, є загрозою національній безпеці та обороні України і вимагає негайних дій з боку спеціальних служб та відділів боротьби з кіберзлочинністю у Національній поліції України. Але також запорукою перемоги у війні та захисту від загроз в інформаційній сфері є розвиток критичного мислення українців і постійна перевірка інформації у декількох акредитованих державною владою медіа-ресурсах.

Література

1. Дивимося, читаємо, слухаємо: як змінилося медіаспоживання українців в умовах повномасштабної війни. Українська правда: сайт. URL: https://www.pravda.com.ua/columns/2022/06/22/7353987/ (дата звернення: 05.03.2023)

2. Маляр розповіла, як коментарі «військових експертів» нашкодили ЗСУ. ГЛАВКОМ: сайт. URL: https://glavcom.ua/country/incidents/maljar-rozpovila-jak-komentari-vijskovikh-ekspertiv-nashkodili-zsu--866096.html (дата звернення: 05.03.2023)

3. РІК – авторський документальний проєкт Дмитра Комарова | Частина друга. YouTube: сайт. URL: https://www.youtube.com/watch?v=rlkzADUfb3s (дата звернення: 05.03.2023)

4. Fierce fighting continues over Ukraine's eastern city of Bakhmut. The Australian: сайт. URL: https://www.theaustralian.com.au/news/fierce-fighting-continues-over-ukraines-eastern-city-of-bakhmut/video/d7b6c18ddf247daa022865deb165f5a9 (дата звернення: 05.03.2023)

5. UPD:Труха. Як популярний телеграм-канал розганяє фейки і придумує відмазки, коли це помічають. TEXTY.ORG.UA: сайт. URL:

https://texty.org.ua/articles/107377/informacijna-telehram-smittyarka-dlya-2-miljoniv/ (дата звернення: 05.03.2023)

6. СБУ викрила агентурну мережу спецслужб рф, яка дестабілізувала ситуацію в Україні через Telegram-канали. Служба безпеки України: сайт. URL: https://ssu.gov.ua/novyny/sbu-vykryla-ahenturnu-merezhu-spetssluzhb-rf-yaka-destabilizuvala-sytuatsiiu-v-ukraini-cherez-telegramkanaly (дата звернення: 05.03.2023).

Ширшов Р.А.
Національна академія СБ України

OSINT - ФРЕЙМВОРК, ДЛЯ ОТРИМАННЯ ІНФОРМАЦІЇ З ВІДКРИТИХ ДЖЕРЕЛ

OSINT (Open source intelligence) - фреймворк, який призначено для отримання та використання військової, політичної, економічної та іншої інформації з відкритих джерел. Використовується для прийняття рішень у сфері національної оборони та безпеки, забезпечення діяльності спеціальних служб, проведення розслідувань, досліджень, здійснення розвідувальних та контррозвідувальних заходів, тощо.

Перші OSINT дослідження почали проводитись під час другої світової війни. Тоді у США наприкінці 1940 року створили FBMS (Foreign Broadcast Monitoring Service) службу моніторингу іноземного мовлення, яка була створена, насамперед для аналізу німецької пропаганди

Станом на сьогоднішній день основним джерелом для OSINT дослідників стала мережа Інтернет. Ключовими джерелами інформації для проведення OSINT є:

- ЗМІ: друковані газети, журнали, радіо та телебачення з різних країн.
- Інтернет: онлайн-публікації, блоги, дискусійні групи, медіа громадян (наприклад, відео з мобільних телефонів, вміст, створений користувачами), YouTube та інші відео-хостинги, вікі-довідники та інші вебсайти соціальних медіа (наприклад, Facebook, Twitter, Instagram та ін.). Ці джерела також випереджають безліч інших джерел через своєчасність і легкість доступу.
- Державні дані (Public Government Data), публічні урядові звіти, бюджети, слухання, телефонні довідники, прес-конференції, вебсайти та виступи. Хоча ці джерела походять з офіційних джерел, вони є публічно доступними і можуть використовуватися відкрито і вільно.
- Професійні та академічні публікації (Professional and Academic Publications), інформація, отримана з журналів, конференцій, симпозіумів, наукових праць, дисертацій та тез.

- Комерційні дані (Commercial Data), комерційні зображення, фінансові та промислові оцінки, бази даних.
- Сіра література (Grey literature), технічні звіти, препринти, патенти, робочі документи, ділові документи, неопубліковані роботи та інформаційні бюлетені.

За даними агентств Міністерства оборони США до 90% розвідувальних даних отримуються безпосередньо з відкритих джерел.

OSINT та війна між Україною та росією.

Якщо розглядати OSINT під час війни, то слід взяти до уваги всю релевантну інформацію: політичну, економічну, військову з усіх доступних джерел. Використовуючи результати OSINT дослідження військово-політичне керівництво держави може приймати більш точні та зважені рішення у сфері національної безпеки та оборони.

Використовуючи OSINT дослідження можна визначати розташування на місцевості живої сили та техніки. Завдяки аналізу соціальних мереж можна зробити висновки щодо переміщення військових частин.

Результати OSINT досліджень активно використовуються в розвідувальній та контррозвідувальній діяльності, зокрема для виявлення місцезнаходження та кола контактів особи.

Однак, слід зауважити, що ворог використовує такі самі методи та підходи для отримання аналогічних результатів.

Одним з багатьох ефективних прикладів застосування OSINT є запобігання намаганням рф приховати інформацію про воєнні злочини в Бучі. Після відступу з Київської області, російські посадовці намагались приховати та заперечити результати своїх дій.

Україною були отримані супутникові знімки Бучі під час знаходження там окупаційних сил, на яких були тіла вбитих. Ці тіла пізніше були знайдені українськими військовими після звільнення Бучі відповідно до наданих знімків.

Таким чином, шляхом співставлення даних супутникових знімків та інформації від ЗСУ було доведено, що росіяни вкотре збрехали про свою невинуватість.

Основні вимоги до проведення OSINT

Вимога 1: Склад набору засобів та джерел для проведення OSINT.

Основний набір інструментів OSINT щонайменше повинен включати:

Доступ до соціальних мереж (аналізуються фотографії, інформація з особистих сторінок, використовуються методи соціальної інженерії), картографічних сервісів (Google Maps, Bing Map, Yandex Map), доступних реєстрів різного роду та призначення (майданчики проведення тендерів, реєстри послуг та ін.), відкриті бази даних, інформація з форумів та тематичних груп та ресурси Dark Web.

Вимога 2: Оцінка контексту проведення дослідження

Без оцінки контексту об’єкту дослідження неможлива коректна інтерпретація результатів та даних, отриманих з відкритих джерел. Також, вкрай необхідним є поставлене завдання на OSINT, яке має містити в собі чіткі та зрозумілі метрики.

Вимога 3: Використання геоданих

Необхідно, щоб всі знахідки (за можливістю) були географічно прив’язані. Фотографії чи відеоролики, якими публічно діляться соціальні медіа, часто містять інформацію про місця розташування фотографій.

Вимога 4: Перевірка

Будь які дані, отримані під час пошуку, мають перевірятися/мати підтвердження з декількох джерел, такий підхід зможе підвищити якість та точність дослідження.

Вимога 5: Конфіденційність

Під час дослідження має бути забезпечена конфіденційність дослідника, механізмів та результатів OSINT для збереження його цінності та забезпечення особистої безпеки дослідника.

Необхідність підготовки спеціалістів з OSINT

Станом на 2023 рік системної академічної підготовки фахівців з OSINT не ведеться, а існуючий шлях підготовки (онлайн-курси, статті і ґайди, лекції в Youtube) не забезпечує достатнього рівня опанування цього фреймворку без виконання великої кількості практичних завдань.

Якщо ж йдеться про більш глибоке опанування інструментарію і подальше його використання для державної чи військової служби, краще необхідно пройти ґрунтовне навчання. Це має бути повноцінний учбовий курс, який повинен викладатися в вищому учбовому закладі.

СЕКЦІЯ 2
ПРОБЛЕМИ ПРОТИДІЇ КІБЕРНЕТИЧНИМ АТАКАМ рф НА ОБ’ЄКТИ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Авдєєнко С.М.
Національний університет оборони України імені Івана Черняховського

КОМПЛЕКСНА СИСТЕМА КІБЕРЗАХИСТУ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ

У зв’язку з високим державним статусом операцій з обміну інформацією в інформаційній інфраструктурі, інформаційна безпека та кіберзахист набуває

особливої ваги. Інформаційна безпека в інформаційній інфраструктурі базується на реалізації наступних основних принципів:

- централізоване управління системою;
- послідовність рубежів безпеки;
- адекватність та ефективність захисту;
- збереження захисту при відмові;
- захист засобів безпеки;
- безперервність захисту;
- невидимість захисту.

В практику збройної боротьби активно впроваджується концепція інформаційного протиборства, яка передбачає ведення активних розвідувальних дій щодо об'єкта нападу або потенційного порушника та дій, спрямованих на захист національних інтересів від впливу внутрішніх і зовнішніх кібернетичних втручань та загроз. Наслідком таких дій можуть стати так звані кібернетичні війни, основними методами ведення яких на тактичному рівні вже нині визнані кібератаки, а на стратегічному та спеціальному рівнях – кібероперації [1].

Під кібернетичною безпекою розуміється стан життєво важливих інтересів власника інформації від зовнішніх та внутрішніх загроз, пов'язаних з використанням ресурсів кіберпростору.

Завдання, які стоять перед підсистемою кіберзахисту:

здійснювати підготовку до застосування ЗС України в умовах "кібервійни";

створювати можливості для відбиття військової агресії в кіберпросторі з урахуванням нових викликів та загроз;

захищати військову інформаційну інфраструктуру від реальних та потенційних кіберзагроз, у тому числі зовнішніх та внутрішніх загроз;

постійно контролювати реальний рівень захищеності інфраструктури та сервісів;

контролювати доступ привілейованих користувачів (адміністраторів) до критично важливих компонентів інфраструктури, зберігати інформацію щодо такого доступу та дій під час доступу до критично важливих компонентів інфраструктури;

створити систему підготовки кадрів у сфері кібербезпеки для потреб ЗС України;

встановити обов'язкові вимоги щодо кіберзахисту критичних об'єктів інформаційної інфраструктури, порядку їх захисту та контролю за їх дотриманням;

здійснювати заходи реформування системи захисту інформації з обмеженим доступом задля уникнення витоків такої інформації;

посилювати боротьбу з кібертероризмом та кібершпигунством на критичних об'єктах інформаційної інфраструктури.

Обсяги інформації та бази даних в теперішніх інформаційних системах з кожним роком збільшуються у геометричній прогресії. Зростають вимоги не

тільки до швидкості роботи з величезними обсягами інформації, але і до якості та надійності зберігання даних, накопичувачів інформації, до можливостей швидко відшукати потрібний інформаційний елемент. Саме тому правильно обрана система зберігання даних – важлива складова загальної побудови інформаційної інфраструктури [2].

Системи зберігання даних необхідні для забезпечення інформаційної безпеки функціонування інформаційної системи. Це досягається завдяки високому рівню конфіденційності, централізації даних, аудиту та контролю доступу до даних, розмеження доступу, резервного копіювання даних, архівації. Завдяки сучасним системам зберігання даних, збільшується швидкість обробки інформації, а також пошук необхідних даних у величезних інформаційних і дискових масивах. Вся нова інформація, наскільки великим би не виявився її обсяг, повністю записується і надійно зберігається в системі зберігання даних.

Таким чином, кібербезпека є невід'ємною складовою інформаційної безпеки. Водночас інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки, яка характеризує стан захищеності національних інтересів в інформаційній сфері від кіберзагроз.

Література

1. Левченко О.В. Концептуальний підхід до комплексної оцінки стану інформаційної безпеки / О.В. Левченко // Наука і техніка Повітряних Сил Збройних Сил України. – 2015.№3(20). – С.47–50.

2. Косогов О.М. Методика визначення заходів протидії інформаційним загрозам державі у воєнній сфері // Системи обробки інформації. – 2016, №3(140). С.25–29.

Бондаренко І. Д.
к.ю.н.,
Національна академія СБ України

КІБЕРАТАКИ НА ЕНЕРГОСИСТЕМУ УКРАЇНИ 2015-2016 РОКІВ

У 2015 та 2016 роках Україна стала жертвою двох значних кібератак на свою енергетичну систему, які спричинили серйозні перебої у роботі національній системі електропостачання. Атака, яка відома за назвою використаного шкідливого програмного забезпечення «BlackEnergy», стала безпрецедентною у світовій історії, адже це перша відома атака, що призвела до відключення електропостачання на рівні цілого регіону [1].

23 грудня 2015 року в результаті кібератаки мав місце істотний збій у роботі енергетичної системи на підприємствах «Прикарпаттяобленерго», без

електропостачання залишилися 225 000 споживачів. Були атаковані низка електропідстанцій в регіоні: підстанція «Добровляни» була відключена від енергосистеми на 6 годин. На декілька годин обмежена робота підстанцій «Калуш», «Стрий», «Долина», «Татарів». Атаковані були і деякі об'єкти електроенергетики в Івано-Франківській, Львівській та Чернігівській областях.

Державна служба спеціального зв'язку та захисту інформації України спільно зі спеціалістами енергопідприємств здійснювала розслідування інциденту. СБ України також долучилася до розслідування кібератаки. В Україну була направлена міжвідомча робоча група країни-партнера, США, у складі представників: Національного центру кібербезпеки та комунікаційної інтеграції (NCCIC) / Групи реагування на кібернетичні надзвичайні ситуації промислових систем управління (ICS-CERT), Групи готовності до комп'ютерних надзвичайних ситуацій США (US-CERT), Міністерства енергетики, Федерального бюро розслідувань та North American Electric Reliability Corporation [2].

Низка приватних антивірусних компаній міжнародного рівня вивчали ситуацію з BlackEnergy, прямо чи опосередковано були задіяні у розслідуванні. В цій роботі, зокрема, брали участь представники компанії FireEye, яка спеціалізується на кібербезпеці та протидії кіберзлочинності. Декілька кібербезпекових компаній випустили за результати власних розслідувань звіти про кібератаку, а саме компанії: FireEye, ESET, Dragos, Symantec, Crowdstrike. Також у 2016 році ICS-CERT видала відповідний звіт «Analysis of the Cyber Attack on the Ukrainian Power Grid». У своїх звітах експерти одностайно стверджують, що ситуація, яка сталася на Прикарпаттяобленерго є результатом умисних протиправних дій сторонніх осіб. Кібератака була синхронізована та скоординована, що досяглося завдяки попередній ретельній розвідці мережі Прикарпаттяобленерго, вірогідно, із залученням фахового персоналу сфери енергетики, який розуміється у топології та логіці внутрішніх мереж енергокомпанії.

Першим етапом кібератаки була адресна розсилка зловмисниками фішингових листів електронної пошти. В них містився вкладений текстовий документ розширення .doc. Після його завантаження програма Microsoft Word пропонувала включити макроси, це в свою чергу і активізувало роботу шкідливого програмного забезпечення, яке не початковому етапі отримувало логін і пароль від аккаунту працівника у внутрішній корпоративній мережі енергетичної кампанії.

Наступним етапом було отримання доступу до мережі SCADA, що була відокремлена від корпоративної мережі брендмауерами. Перебуваючи в середині корпоративної мережі протягом багатьох місяців зловмисники здійснювали вивчення її топології, отримали доступ до контролерів домену Windows, де містяться облікові записи користувачів для мереж. Вони отримали облікові дані працівників, які використовувалися для віддаленого входу в мережу SCADA. Отримавши доступ до мережі SCADA зловмисники в першу чергу здійснили

переконфігурацію джерел безперебійного живлення (UPS), що забезпечували резервне живлення центрів керування. Це дозволило їм під час активної стадії атаки залишити самих операторів енергосистеми без власного енергозабезпечення. Зловмисники перепрограмували PLC в системі SCADA на більш ніж 10 електропідстанціях, замінивши їх штатну прошивку на спеціально створену [3]. Це позбавило операторів можливості увімкнути електронні вимикачі після їх несанкціонованого вимкнення зловмисниками в момент «Ч».

Приблизно о 15:30 23 грудня 2015 року зловмисники (використовуючи попередньо здобуті дійсні облікові дані) віддалено зайшли у мережу SCADA. Дистанційне керування здійснювалося із зовні за допомогою наявних інструментів віддаленого адміністрування на рівні операційної системи або клієнтського програмного забезпечення віддаленої системи промислового керування (ICS) через з'єднання віртуальної приватної мережі (VPN).

Оператори чергової зміни фіксували факт самостійного відключення електронних вимикачів підстанцій Прикарпаттяобленерго, але були позбавлені можливості управляти процесом. В цей час зловмисники надіслали команди для вимкнення систем безперебійного живлення, які вони попередньо вже переконфігурували. Ними було здійснено послідовне відключення електронних вимикачів.

Паралельно було здійснено так-звану TDoS атаку (підвид DDoS атаки) на кол-центри енерго-кампанії. Завдяки ній телефонна лінія кол-центру була перевантажена тисячами фальшивих дзвінків, які надходили з Москви, а постраждалі від відключення електроенергії абоненти не могли повідомити операторів про проблеми. Останні таким чином не знали про кількість підстанцій, що були атаковані.

В подальшому зловмисниками були знищені деякі системи завдяки використанню програмного забезпечення KillDisk, яке стерло системні файли, знищило завантажувальний сектор (boot record), програмне забезпечення пристроїв Serial-to-Ethernet. В одному випадку також було знищено штатне програмне забезпечення людино-машинного інтерфейсу (HMI) на основі Windows, віддаленого терміналу (RT). Оскільки KillDisk перезаписав головний завантажувальний запис, заражені комп'ютери не могли бути перезавантажені. Програмний засіб KillDisk у більшості випадків запускався вручну, але у двох випадках зловмисники використовували логічну бомбу, яка автоматично запускала KillDisk приблизно через 90 хвилин після атаки [4,5].

Українська влада звинуватила Росію в кібератаках на енергетичну мережу Прикарпаттяобленерго в 2015 році. Зокрема, тодішній Президент України Петро Порошенко в інтерв'ю заявляв про те, що кібератака на Прикарпаттяобленерго була здійснена з боку російських хакерів, а Росія намагалася знищити енергетичну мережу України та створити хаос у країні. Міністр закордонних справ України Павло Клімкін на засіданні Ради Безпеки ООН в 2016 році заявив, що Росія була

ініціатором кібератак на Україну, зокрема на енергетичну мережу. Він наголошував на тому, що ці кібератаки мали на меті не лише дестабілізацію енергетичної мережі України, але й загострення політичної ситуації в країні [6,7].

США, Канада та Німеччина, а також ЄС засудили умисні атаки на українську енергосистему. США в рамках програми «Кібергігант» виділили $25 млн для підтримки українських інституцій у сфері кібербезпеки та надали Україні доступ до спеціалізованих технічних засобів та інструментів, які суттєво підвищили рівень кіберспроможності України.

Література

1. Industrial Control Systems Cyber Emergency Response Team (ICSCERT), Alert (ICS-ALERT-14-281-01E), Ongoing Sophisticated Malware Campaign Compromising ICS (Update E), Idaho Falls, Idaho, December 9, 2016 // ICSCERT site – Режим доступу до ресурсу: https://bcourses.berkeley.edu/courses/1471305/files/73388800/download?verifier=ThtkNVY503zme7lim5oFYbWbg77Ms9NyU3vzw1Pn&wrap=1

2. Department of Homeland Security (DHS) and Federal Bureau of Investigation (FBI), Joint Analysis Report (JAR-16-20296A): GRIZZLY STEPPE – Russian Malicious Cyber Activity, December 29, 2016 [Електронний ресурс] // NCCIC – Режим доступу до ресурсу: https://www.cisa.gov/sites/default/files/publications/JAR_1620296A_GRIZZLY%20STEPPE-2016-1229.pdf

3. Ukraine power outage was a cyberattack – U.S. doesnt finger Russia (officially) – Russian Malicious Cyber Activity, December 29, 2016 [Електронний ресурс] // Computer World – Режим доступу до ресурсу: https://www.computerworld.com/article/3039772/ukraine-power-cyberattack-russia-itbwcw.html

4. BlackEnergy 3: Threat Actor Targeting Ukrainian Critical Infrastructure [Електронний ресурс] // Dragos – Режим доступу до ресурсу: https://dragos.com/blog/industry-news/blackenergy-3-threat-actor-targeting-ukrainian-critical-infrastructure/

5. Sandworm Team: An In-depth Look at the Energetic Bear [Електронний ресурс] // iSIGHT Partners – Режим доступу до ресурсу: https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-sandworm.pdf

6. Dragonfly: Western energy sector targeted by sophisticated attack group [Електронний ресурс] // Symantec – Режим доступу до ресурсу: https://www.symantec.com/blogs/threat-intelligence/dragonfly-western-energy-sector-targeted-sophisticated-attack-group

7. Analysis of the Cyber Attack on the Ukrainian Power Grid [Електронний ресурс] // ICS-CERT – Режим доступу до ресурсу: https://ics-cert.us-

cert.gov/sites/default/files/documents/Analysis%20of%20the%20Cyber%20Attack%20Against%20Ukraine%E2%80%99s%20Power%20Grid.pdf

Буяло О.В.
к.т.н., с.н.с.,
Ковтун О.М.
Войтко В.В.
к.т.н., ст. дослідник,
Воєнна академія імені Євгенія Березняка

АНАЛІЗ МОЖЛИВОСТЕЙ ВИКОРИСТАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ЗАХИСТУ ВІД КІБЕРНЕТИЧНИХ ЗАГРОЗ У СУЧАСНИХ УМОВАХ

З появою нових кібернетичних загроз в умовах російської агресії та швидким розвитком цифрових технологій у світі традиційні засоби кібернетичного захисту такі як антивірусні програми та фаерволи, які зазвичай використовують правила та сигнатури для виявлення відомих загроз можуть виявитися недостатньо ефективними.

Аналіз показав, що актуальними засобами для протидії кібернетичним загрозам у таких умовах можуть стати програмні засоби та системи на основі використання штучного інтелекту оскільки забезпечують автоматизацію та високу швидкість виявлення і реагування на кіберзагрози. Програмні засоби (ПЗ) на основі штучного інтелекту (AI) здатні аналізувати величезні масиви даних та виявляти в них найменші ознаки аномальної поведінки, що може свідчити про потенційну кібератаку. У сучасних умовах системи кібернетичного захисту на основі штучного інтелекту можуть використовуватися для виявлення та аналізу потенційних загроз, для автоматичної реакції на загрози, наприклад, для блокування підозрілих дій чи відключення шкідливого ПЗ, для контролю доступу до різних ресурсів, наприклад, до конфіденційної інформації.

Штучний інтелект дозволяє розширити можливості кіберзахисту, дозволяючи автоматизувати процеси виявлення, аналізу та реагування на загрози. Він може використовуватися для аналізу великих обсягів даних та виявлення аномальних патернів незвичних, складних атак, які можуть бути пропущені людиною-оператором що може допомогти виявляти невідому шкідливу діяльність. Також, штучний інтелект може використовуватися для прогнозування можливих загроз та планування відповідних захисних заходів.

Складні математичні моделі та алгоритми AI такі як, машинне і глибинне навчання та навчання з підкріпленням що формалізують функціонування AI може допомогти підвищити ефективність систем кібернетичного захисту. AI може

використовуватись для розробки моделей ПЗ, яке навчається розпізнавати шаблони поведінки зловмисників та виявляти загрозу у реальному часі. Глибинне навчання дозволяє штучному інтелекту розуміти складні залежності між великою кількістю даних, а навчання з підкріпленням може використовуватись для прогнозування розвитку ймовірних кіберзагроз для покращення їх виявлення у реальному часі.

Наведемо спрощену класифікацію сучасного ПЗ для вирішення задач забезпечення кіберзахисту за функціональністю та способом застосування.

Антивірусне програмне забезпечення – використовуються для відслідковування та блокування шкідливого ПЗ, яке може створювати ризики для безпеки. Фаерволи – призначені для керування мережевим трафіком та фільтрації небезпечного вхідного і вихідного трафіку.

Системи виявлення та запобігання вторгненням (*IDS/IPS*) - використовуються для виявлення та блокування вторгнень у мережу та систему яка захищається.

Системи управління подіями безпеки (*SIEM*) - забезпечують збір та аналіз журналів подій з різних джерел, що дозволяє виявляти та відстежувати потенційні загрози.

Системи управління конфігураціями (*SCM*) - допомагають забезпечити безпеку та стабільність функціонування шляхом управління конфігурацією та виявленням потенційних проблем.

Системи захисту електронної пошти - відслідковують та блокують небезпечні повідомлення електронної пошти, що містять шкідливий вміст. Системи захисту веб-додатків - використовуються для виявлення та запобігання кібератак на веб-додатки.

Системи контролю доступу (*Access Control*) - забезпечують контроль доступу до різних ресурсів мережі та інформаційних систем. Вони використовують методи аутентифікації та авторизації, щоб забезпечити, що тільки авторизовані користувачі можуть отримати доступ до захищеної інформації та ресурсів.

Системи управління конфігурацією (*Configuration Management*) - дозволяють автоматизувати процес управління конфігурацією інформаційних систем та мережі, включаючи контроль версій, конфігураційні файли, параметри безпеки та налаштування.

Системи контролю трафіку мережі (*Network Traffic Control*) - забезпечують контроль та моніторинг трафіку в мережі, дозволяючи виявляти та блокувати небажані дії, такі як атаки з зовнішньої мережі, шкідливі програми, вторгнення та інші загрози безпеці мережі.

Системи захисту кінцевих точок EPP (*Endpoint Protection Platforms*) та EDR (*Endpoint Detection and Response*) - ПЗ, що встановлюється на кінцевих точках (наприклад, на персональних комп'ютерах, ноутбуках, смартфонах) та забезпечує їх захист від шкідливого ПЗ та інших загроз, які можуть виникнути під час користування ІТ-ресурсами. Використання штучного інтелекту у системах

EPP/EDR дозволяє забезпечити більш точне і оперативне виявлення загроз, а також автоматизувати процес виявлення та реагування на інциденти. Наприклад, система на основі штучного інтелекту може аналізувати структуру файлів та порівнювати її зі структурами відомих шкідливих програм для виявлення загроз, які не були відомі раніше.

У зв'язку з цим, багато виробників ПЗ для кібернетичного захисту пропонують рішення які базуються на штучному інтелекті. Наприклад, такі компанії, як *IBM Security, Symantec, McAfee, Cisco, Palo Alto Networks ma Crowdstrike*, пропонують продукти, які використовують AI для виявлення та запобігання кібератакам.

Для організації, яка потребує широкого периметру кібернетичного захисту, популярні рішення від компаній *IBM Security, Symantec, Cisco Security, Palo Alto Networks* які мають широкий спектр функцій, включаючи виявлення загроз, ідентифікацію потенційних вразливостей та аналіз стану безпеки мережі. Для забезпечення кібернетичного захисту IoT-інфраструктури невеликої організації або окремого робочого місця може використовуватися ПЗ від компаній *CylancePROTECT, Darktrace* та *CrowdStrike*, які спеціалізуються на ефективному виявленні та блокуванні шкідливого ПЗ та інших загроз. Для забезпечення базового рівня кібернетичного захисту тільки окремого робочого місця можливо використати антивірусне ПЗ *Norton AntiVirus Plus, Bitdefender Antivirus Plus, Avast Free Antivirus Malwarebytes* тощо, яке використовує елементи AI для виявлення загроз.

Так, наприклад ПЗ *Darktrace* - використовує нейронні мережі для виявлення загроз та аномальних дій в мережах компаній, ПЗ *CylancePROTECT* використовує AI для ідентифікації та блокування шкідливого ПЗ та зловмисного коду, а ПЗ *CrowdStrike Falcon* використовує AI для розпізнавання та блокування загроз в реальному часі та надає аналітику поведінки загроз, що допомагає зрозуміти, які саме системи та джерела можуть бути уражені. Дане ПЗ забезпечує захист від різних видів загроз, включаючи зловмисний код, фішинг, ін’єкції, які можуть пошкодити комп'ютерну мережу. *CrowdStrike Falcon* складається з наступних модулів: *Falcon Prevent* - модуль захисту від загроз, який використовує AI та інші технології для ідентифікації ШПЗ та зловмисного коду, та забезпечує їх блокування перед тим, як вони можуть спричинити шкоду; *Falcon Insight* - модуль моніторингу та реагування на інциденти, який забезпечує збір даних про загрози та їх аналіз за допомогою машинного навчання, щоб швидко виявляти та реагувати на потенційні інциденти; *Falcon Discover* - модуль для виявлення небезпек в мережі, який використовує технології штучного інтелекту та машинного навчання для пошуку аномальних поведінок та дій у мережі; *Falcon OverWatch* - модуль моніторингу та реагування на інциденти, який забезпечує постійний контроль та аналіз мережі за допомогою експертів.

Модель штучного інтелекту *CrowdStrike Falcon* аналізує велику кількість даних у режимі реального часу для навчання. Ці дані включають інформацію про типові та нетипові патерни поведінки зловмисників, що дозволяє продукту виявляти нові кіберзагрози, навіть якщо вони раніше не були відомі. ПЗ *CrowdStrike Falcon* використовує алгоритми, які аналізують стандартну поведінку користувачів та систем, що дозволяє виявляти аномальну поведінку, що може свідчити про напад. Крім того, *CrowdStrike Falcon* має достатню масштабованість, що дозволяє використовувати його на окремих робочих місцях, а також на більш широкому рівні для захисту всієї мережі компанії. Завдяки технології штучного інтелекту, ПЗ забезпечує постійне відстеження активності у мережі, виявлення потенційних загроз та прийняття відповідних заходів для їх блокування.

Таким чином, штучний інтелект AI відіграє важливу роль у забезпеченні кібернетичного захисту та дозволяє аналізувати великі обсяги даних й виявляти потенційні загрози, а також швидко реагувати на нові види загроз та адаптуватися до змін в кіберпросторі.

Література

1. Хіммельманн Р. Штучний інтелект в кібербезпеці / Р. Хіммельманн // Cyber Defense Review. – 2018. – Т. 3, № 2. – С. 46-55.

2. Bhattacharyya, S., Kalita, J. K., & Sarker, R. A. (2021). Cybersecurity using machine learning: A review. ACM Computing Surveys. – 2021. 54(2), P. 1-37.

3. Кібербезпека та штучний інтелект: перспективи взаємодії та захисту від нових загроз: монографія / За ред. В. І. Мацука. – К.: Центр навчальної літератури, 2019. – 208 с.

4. Деркач О. Кібербезпека в умовах сучасних загроз: монографія / О. Деркач, І. Борисенко, І. Дідовець та ін. – К.: Наукова думка, 2020. – 456 с.

Вавіленкова А.І.
д.т.н., доцент,
Національна академія СБ України

СТРАТЕГІЇ ЗДІЙСНЕННЯ КІБЕРАТАК

Незважаючи на активне застосування таких методів соціальної інженерії, як фішинг, спамінг, тейлгейтинг, вейлінг, «серфінг через плече», «послуга за послугу», «сміттєвий дайвніг» та ін., а також існування величезної кількості зловмисного програмного забезпечення, зокрема, різноманітних видів комп’ютерних вірусів, SQL-ін’єкції, логічних бомби, зламів паролів, несанкціонованих точок доступу [1], всі вони є лише механізмами для реалізації того чи іншого виду кібератак. А для захисту та протидії кібератакам дуже

важливою на сьогоднішній день є тема дослідження безпосередніх стратегій здійснення кібератак, тобто дій, спрямованих на комп'ютер чи будь-який елемент комп'ютерної інформаційної системи з метою зміни, знищення, крадіжки даних, а також використання або нанесення шкоди мережі [2].

На сьогодні основним видом кібератак залишається DDoS – атака (відмова в обслуговуванні), що використовується для виведення з ладу та зламу обчислювальної техніки та здійснюється шляхом створення великої кількості запитів, спричиняючи перевантаження мережевого трафіка та порушення роботи сервера [3]. На відміну від Dos-атаки, яку досить просто можна зафіксувати та знешкодити, заблокувавши джерело, DDoS-атаку складно упередити, оскільки зловмисники використовують для збільшення об'єму трафіку мережу пов'язаних між собою машин (ботів). Кожним таким комп'ютером зловмисники можуть керувати віддалено, а у потрібний момент активізувати команду для початку відправлення запитів для атаки сервера. В результатів цього заповнюється канал зв'яку між сервісом, на який проводиться атака, та Інтернет-провайдером, після чого сервер перестає працювати.

Залежно від особливостей здійснення атак та вразливостей, на які вони спрямовані, розрізняють декілька основних стратегій здійснення DoS-атак.

Атака типу Ping of Death – використовує таку уразливість стеку протоколів TCP/IP, як фрагментація пакетів даних – на комп'ютер жертви надсилається фрагментований ICMP-пакет, розмір якого перевищує допустимий у протоколі, після чого комп'ютер жертви намагається відновити пакет, внаслідок чого функціонування операційної системи порушується. Для захисту від такого типу кібератак можна використовувати брандмауер для перевірки розміру фрагментованих пакетів [3].

Атака SYN-flooding – орієнтується на таку уразливість стеку протоколів TCP/IP, як «механізм потрійного рукостискання» - коли зловмисник відправляє занадто багато пакетів TCP SYN, створюючи таким чином потік запитів, на які комп'ютер жертви повинен відповісти комбінацією SYN+ACK, а зловмисник у свою чергу не завершує «потрійне рукостискання» та не надсилає пакети з відміткою ACK, на які очікує комп'ютер жертви, тобто з'єднання залишається у напіввідкритому стані. Щоб захистити систему від подібного типу DoS-атаки, можна збільшити розмір черги з'єднання та зменшити значення часу очікування з'єднання або використати брандмауер, що блокуватиме вхідні пакети SYN.

IP-Spoofing – атака типу «Man in the Middle», під час якої зловмисник відправляє модифікований IP – пакет з перевіреною IP-адресою джерела на хост жертви. Жертва приймає цей пакет, після чого трафік від хоста жертви надходить зловмиснику замість реальної достовірної адреси. Для захисту від IP-Spoofing можна використовувати списки доступу, якщо це зовнішній трафік.

ARP-Spoofing – ще один різновид атаки для реалізації стратегії «Man in the Middle», коли зловмисник пов'язує свою власну MAC-адресу з перевіреною IP-

адресою в мережі. Це стає можливим шляхом маніпулювання ARP-таблицею, тому коли хост-жертва надсилає пакет на перевірену IP-адресу у відповідності до записів ARP-таблиці, насправді пакет надсилається зловмиснику у мережі.

Основними методами захисту від DDoS-атак [4] є зменшення зон, доступних для атаки, що обмежує можливості зловмисника для атаки та забезпечує можливість централізованого захисту, зводячи до мінімуму кількість можливих точок для небезпеки та зосередження зусиль на її нейтралізації; забезпечення транзитного потенціалу та контроль за потужністю сервера; моніторинг типового та нетипового трафіка; розгортання брандмауерів для відбиття складних атак рівня додатків.

Література

1. Курс Cisco Курс мережевої академії Cisco Networking Academy «IT Essentials: PC Hardware and Software». [Електронне джерело]. URL: https://www.netacad.com

2. Закон України про основні засади забезпечення кібербезпеки України від 5 жовтня 2017 року № 2163-VIII. [Електронне джерело]. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

3. Вавіленкова А.І., Душкевич В.С., Лозниця Р.А. Види налаштувань безпеки компютера: Proceedings of the V International Scientific and Practical Conference «Formation of perceptions of the structure of scientific methodology», 30-31 січня, 2023, – Відень, Австрія: InterSci. – 2023. – С. 47–50.

4. Лісовська Ю.П. Кібербезпека: ризики та заходи. Кондор. 2019. 272 с.

Гордієнко С.Б.
к.т.н.,
Національна академія СБ України

ПИТАННЯ РЕАЛІЗАЦІЇ КОНЦЕПЦІЇ ЩОДО БЕЗПЕРЕРВНОСТІ ІНФОРМАЦІЙНО-КОМУНІКАТИВНИХ ТЕХНОЛОГІЙ В УМОВАХ ВОЄННОГО СТАНУ

З огляду на активну фазу військових дій та спрямованість держави агресора на знищення енергетичного сектору України, особливо актуальним постає питання забезпечення стійкості функціонування та безперервності інформаційних та комунікаційних технологій на об’єктах критичної інфраструктури держави.

Забезпечення стійкості та ефективного функціонування процесів на об’єктах критичної інфраструктури України в умовах активної військової агресії російської федерації, на сьогодні є пріоритетним завданням діяльності безпекового та оборонного сектору країни.

Для забезпечення стійкості життєво важливих процесів функціонування державних структур в умовах військового стану необхідний ефективний процес управління на постійній основі з огляду на ризик-орієнтований підхід [1].

Процеси забезпечення безперервності функціонування життєво важливих технологій мають вирішальне значення для безперервної роботи всіх видів бізнесу та сфери державного управління. Що важливо, ці процеси набувають все більшого значення, оскільки компанії та державні структури стають все більш залежними від технології ведення бізнесу.

За результатами аналізу фахівців різноманітних галузей інфраструктури держави на сьогодні все більше компаній, організацій та підприємств України у своїй діяльності схильні та спрямовують значні зусилля на забезпечення комплексного підходу до захисту, збереження та розвитку ресурсної бази і головних активів, а також зниження ризиків порушення інформаційної безпеки.

З урахування реалій сьогодення є нагальна потреба на державному рівні забезпечити ефективний процес управління, для забезпечення безперервності бізнес-процесів та належної стійкості щодо функціонування основних ресурсних можливостей організацій.

Питання розробки та реалізації концепції безперервності інформаційних та комунікаційних технологій на об’єктах критичної інфраструктури розглядається на всіх рівнях функціонування інформаційних систем з огляду на створення та ефективне функціонування системи управління безперервністю бізнесу (Business Continuity Management) – (BCM).

Безперервність бізнесу на сьогодні є концепцією з елементами, які орієнтовані на забезпечення стійкого та ефективного функціонування процесів на об’єктах критичної інфраструктури України в умовах активної військової агресії російської федерації: це – *витривалість, швидке відновлення та здатність ефективно реагувати на всі непередбачувані інциденти та катастрофи*.

Для збереження процесу функціонування бізнесу в умовах кризових ситуацій розроблено певний підхід до управління організацією, який сформулював міжнародні стандарти ISO/IEC 27031, ISO 22301.

Стандарт ISO/IEC 27031 напряму тісно пов'язаний зі стандартом системи менеджменту безперервності бізнесу (BCMS) – ISO 22301:2019, визнаним на міжнародному рівні таким, який дозволяє будь-якій компанії чи організації забезпечувати свою актуальність в сучасному бізнес-середовищі [2].

Цей стандарт може забезпечити основу для створення та використання ефективної системи безперервності бізнесу та всіх важливих процесів функціонування інформаційних та комунікаційних технологій на об’єктах критичної інфраструктури, дозволить організаціям забезпечувати їх ефективне функціонування, з огляду на рекомендації щодо підтримання безперервності процесів, надасть цінну інформацію, корисну для стратегічного планування, управління ризиками, ресурсами та активами.

В умовах воєнного стану дуже важливою є стійка позиція підприємств на ринку економічних відносин, здатність компаній, організацій та важливих об'єктів життєзабезпечення інфраструктури держави продовжувати працювати під час збоїв, які виникають внаслідок атак на критичну інфраструктуру країни.

Отже, якщо деструктивні спрямування на інфраструктуру держави в період військового стану не можуть бути забезпечені рекомендаціями раніше створених планів реагування на надзвичайні ситуації то є доцільним всім компаніям, організаціям та підприємствам застосувати всебічний процес забезпечення готовності управління безперервністю функціонування та стійкістю системи відповідно до міжнародних стандартів ISO/IEC 27031, ISO 22301 [3].

На жаль, досвід показує, що багато організацій все ж таки не мають плану безперервності бізнесу (BCP) та/або плану аварійного відновлення (Desaster Recovery Plan – DRP).

Це значить, що, не зважаючи на актуальність питання, більшість організацій і компаній не готові до ефективного відновлення в разі аварії, пошкоджень військового спрямування чи катастрофи.

Враховуючи перетин областей охоплення процесів BCP та DRP, економічно доцільно, щоб розробкою, тестуванням та впровадженням BCP та DRP займалася одна й та сама професійна команда та мати рекомендації та інформацію командам аварійного відновлення реагувати на збої та забезпечення організації дієвої допомоги у своєчасному відновленні процесів функціонування.

Стан безпекової стратегія критичної інфраструктури та критичних індустрій на сьогодні в нашій державі є вкрай несприятливим і за умов військової агресії та подальшої ескалації може привести до кризової ситуації в економічній діяльності та поглиблення кризи в гуманітарній сфері. І тому відбувається визначення опцій та розроблення антикризових планів спрямованих на найбільш дієві заходи, що лежать у військово-політичній площині [4].

Розробку та впровадження стратегій безпекового спрямування компаній та організацій слід починати заздалегідь, вже сьогодні, враховуючи сценарії припинення військових дій чи їх перехід у більш латентну фазу.

Стратегія безпекового спрямування об'єктів критичної інфраструктури та критичних галузей повинна відповідати наступним цілям: *безперервного функціонування; створення умов безпеки для персоналу та мінімізація ризиків; запобігання вторгненню в технологічні процеси, ресурси та активи зловмисників; стійкість комунікацій та енергозабезпечення; швидкого реагування на інциденти аварійного характеру*.

Подібні вимоги є базовими в низці міжнародних технічних стандартів, щодо забезпечення національної стійкості [5].

Згідно з даними вітчизняних та зарубіжних експертів, поточний стан більшості об'єктів економічної інфраструктури країни в теперішній і в довоєнний період, характеризується такими положеннями як:

1. Незадовільний рівень впровадження та застосування сучасних стандартів.

Негативною оцінкою і характеристикою об'єктів загальногосподарської діяльності та критичної інфраструктури є ігнорування стандартів безпеки. Більшість керівників відділів АСУ недостатньо обізнані зі стандартами і їх не використовують у своїй діяльності за виключенням сфери кібербезпеки.

2. Ризик-орієнтовані підходи до управлінських та технологічних рішень.

При управлінні безпекою функціонування індустріальних систем та критичної інфраструктури ризик-орієнтовані підходи є ключовими. В основу їх покладено принцип прийнятного ризику.

3. Стан системи управління виробничими ресурсами та активами.

В цій сфері багато компаній впровадили сучасні системи управління індустріальними процесами, виробничими активами що можна назвати найбільш прогресивним кроком.

Стійкість системи функціонування процесів державного рівня, економіки, господарювання та ведення бізнесу з різними формами власності та галузевої направленості набуває значного значення. На сьогодні надання дієвої допомоги створення сучасного механізму по ефективному забезпеченню цієї діяльності покладається на систему управління безперервністю бізнесу. Сьогодні є нагальна потреба в процесі, що забезпечує виживання та стійкість основної діяльності об'єктів критичної інфраструктури під час кризових ситуацій. Здатність організації відновлюватися після надзвичайних ситуацій, які призводять до припинення процесу функціонування напряму пов'язана зі ступенем планування безперервності бізнесу.

Література

1. Гладиш С. В., Кононович В. Г., Тардаскін М. Ф. Розподіл відповідальності щодо реагування та обробки інцидентів безпеки в інформаційно-телекомунікаційній мережі загального користування // Зв'язок. — 2007. — № 8. — С. 28–31.

2. Безперервність бізнесу // Банківська енциклопедія / С. Г. Арбузов, Ю. В. Колобов, В. І. Міщенко, С. В. Науменкова. – Київ : Центр наукових досліджень Національного банку України : Знання, 2011. – 504 с. – (Інституційні засади розвитку банківської системи України).

3. ISO/IEC 27031: 2011 року (Інформаційні технології. Методи забезпечення безпеки. Керівництво по створенню готовності інформаційно-комунікаційних технологій до забезпечення безперервності бізнесу).

4. ISO 22301:2019: Security and Resilience – Business Continuity Management Systems – Requirements

5. ISO 22313: 2012 «Соціальна безпека. Системи менеджменту безперервності бізнесу. Керівництво по застосуванню».

Грибенко Р.В.
Національний університет оборони України імені Івана Черняховського

МОНІТОРИНГ ІНФОРМАЦІЙНОГО ПРОСТОРУ В ІНТЕРЕСАХ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ У ВОЄННІЙ СФЕРІ

Законодавча база у системі національної безпеки України дозволяє окреслити основні функції держави, тобто функціональні складові, які спрямовані на забезпечення воєнної безпеки, а саме:

– моніторинг загрозливих ситуацій національній безпеці у воєнній сфері;

– прогнозування розвитку загрозливих ситуацій національній безпеці у воєнній сфері;

– вироблення і прийняття управлінських рішень щодо захисту суверенітету держави на основі чинного законодавства та міжнародного права, у тому числі шляхом застосування воєнної сили;

– підтримка бойової могутності (спроможності) воєнної організації держави (сектору безпеки і оборони) для стримування та відсічі агресії;

– ресурсне забезпечення сфери воєнної безпеки держави [1].

Для з'ясування пріоритетності зазначених функцій в реалізації військового будівництва в Україні важливою проблемою є оцінка рівня внеску виконання кожної із функцій в забезпечення воєнної безпеки держави, зокрема, функції моніторингу обстановки загрозливих ситуацій національній безпеці України у воєнній сфері.

Аналіз опублікованих робіт показує, що на сьогодні теорія воєнної безпеки є недосконалою, у ній бракує чітких формальних методів і методик для кількісних оцінок певних аспектів цієї сфери, зокрема і самого рівня воєнної безпеки для окремої держави. З цієї причини кількісна оцінка внеску, зокрема моніторингу виявлення кіберзагроз в забезпечення воєнної безпеки, є складним завданням, яке ще не вирішене.

Виходячи із зазначеного, метою тез доповіді є розгляд методичного підходу та оцінки внеску моніторингу, зокрема загрозливих ситуацій національній безпеці України у воєнній сфері, в забезпечення обороноздатності та воєнної безпеки держави [2].

Моніторинг загрозливих ситуацій воєнного характеру для держави є діяльність пов'язана з інформаційним забезпеченням усіх її (функцій) суб'єктів воєнної сфери. Зосередимо увагу лише на цій складовій. При цьому під поняттям моніторинг (від англ. monitor- контролюючий), зокрема стосовно воєнної сфери, слід розуміти безперервну розвідку (спостереження) реальних явищ і процесів та формування на цій основі інформації певного цільового спрямування в інтересах оборони держави.

Такий моніторинг можливо поділити на три основних різновиди:

повільний моніторинг кіберзагроз, як статистичне накопичення і аналіз

упродовж тривалого часу загрозливих для держави фактів воєнного характеру та оцінка на цій основі воєнно-політичної обстановки (режим мирного часу);

прискорений моніторинг кіберзагроз – те ж саме, але з введенням у певний момент часу режиму посиленого спостереження у загрозливому секторі географічного простору(режим мирного часу, стан загострення ситуації, початок кризи);

оперативний моніторинг – те ж саме, але з введенням у стані кризи режиму безперервного спостереження за діями реального противника для оцінки оперативної обстановки (режим особливого періоду, криза, воєнні дії).

Для інформаційного забезпечення стримування чи припинення агресивних дій противника шляхом застосування воєнної сили (а це необхідно, перш за все, для ефективних дій сил безпеки і оборони) найбільш важливим є оперативний моніторинг. Тому, у свою чергу, необхідно підкреслити, що рівень оперативного моніторингу визначається характеристиками військових систем, які призначені для безперервного спостереження за нерухомими та рухомими об’єктами противника [3].

Проведене оцінювання одночасно дозволило у кількісному вимірі показати важливість ролі наукового забезпечення у процесі створення (удосконалення) інформаційних систем військового призначення, зокрема військових системах. Так, наявність науково обґрунтованих вимог до таких систем дозволяє у 2 – 3 рази підвищити внесок у загальний рівень забезпечення воєнної безпеки держави у порівнянні із випадком формування вимог за відсутності науково-методичного апарату. Це підтверджує високу актуальність наукових досліджень, які спрямовані на розробку і удосконалення науково-методичного апарату обґрунтування вимог та відповідних методологічних основ не лише щодо зазначеного класу систем, але й до систем іншого призначення у сфері оборони держави.

Таким чином, наведені результати наукового дослідження підтверджують домінуючу роль та важливість моніторингу з виявлення кіберзагроз в забезпеченні обороноздатності держави та її воєнної безпеки, що вимагає пріоритетного розвитку в Україні моніторингових систем військового призначення та відповідних подальших досліджень.

Література

1. Cybersecurity a generic reference curriculum (2016). URL: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_10/1610-cybersecurity-curriculum.pdf.

2. National Cyber Security Strategy Good Practice Guide (2016). URL: https://www.enisa.europa.eu/publications/ncss-good-practice-guide.The U.S. Army in Multi-Domain Operations 2028.

3. TRADOC Pamphlet 525-3-1 (2018). URL: https://info.publicintelligence.net/USArmy-MultidomainOps2028.pdf.

Гулак Г.М.
д.т.н., доцент,
Національна академія СБ України
Отто Г.К.
аспірант,
Інститут проблем математичних
машин і систем НАН України

ЛАЗЕРНИЙ ВІБРОМЕТР ЯК ДЖЕРЕЛО ДОДАТКОВОЇ ІНФОРМАЦІЇ ПРО СИСТЕМУ КІБЕРЗАХИСТУ

Загально відомим є той факт, що добування інформації комбінованими методами, значно підвищуючи результативність кожного із складових методів, реалізує так званий синергетичний ефект.

В науково-практичних публікаціях достатньо глибоко проаналізовані ситуації щодо використання зловмисниками інсайдерської інформації стосовно побудови систем кібербезпеки [1], яка сприяє проведенню атак методами соціальної інженерії. Водночас питанням можливості та ефективності застосування спеціальних технічних засобів, зокрема, лазерних систем дистанційного вимірювання нановібрацій (ЛДВ) [2] приділено недостатньо уваги.

Класичний підхід ЛДВ полягає у використанні лазера, як джерела зондувального – та фотодіода, як приймача розсіяного об’єктом виміру випромінювання, яке містить дані про вібрацію у вигляді доплерівського розширення частотного спектру.

Спосіб, який використовує лазер, як джерело зондувального та приймач розсіяного випромінювання одночасно, засновується на інтерферометрії зворотного зв’язку (*Laser Feedback Interferometry* – LFI).

Теоретичні та експериментальні роботи з LFI, проаналізовані в статтях, що описують класичний підхід фіксації вібрацій, розглядають в якості носія інформації виключно випромінювання в резонаторі лазеру, яке фіксується фотодіодом, розташованим за «глухим» дзеркалом, рідше – виводиться напівпрозорим дзеркалом безпосередньо із резонатору.

Відмінно від існуючих підходів, в наших експериментах, в якості носія інформації використовується струм накачки. Не зважаючи на те що струм накачки містить корисну інформацію було відомо ще більше як сорок років тому, це питання ще й досі не досліджено кількісно.

Лазерні сенсори (лазерні допплерівські віброметри) застосовуються в багатьох галузях людської діяльності, де присутні коливання механічних об’єктів - в промисловості, медицині, наукових дослідженнях тощо. При цьому особливо чутливі лазерні сенсори можуть бути застосовані для діагностики надслабких акустичних коливань віддалених об’єктів, тобто, «лазерні мікрофони» є не чим

іншим, як особливо чутливими лазерними сенсорами, які після метрологічних тестувань можуть бути також використані для діагностики цивільних об'єктів.

При використанні в якості мембрани віддалених предметів можна отримати корисний сигнал досить гарної якості. Теоретичні дослідження доводять, що із усіх лазерних віброметрів найефективнішими є пристрої, що працюють за принципом LFI. Досвід розробки цих пристроїв доводить, що при їх застосуванні можна із великим відсотком розбірливості добути сигнал на відстані до 150 метрів (при використанні гарного предмета в якості мембрани).

Проблемою використання лазерних доплерівських віброметрів зазвичай є вибір об’єкта, що буде слугувати мембраною. Обраної мембрани визначить якість отриманої інформації.

При віддаленій реєстрації вібрацій від непідготовлених поверхонь якнайкраще підходять легкі предмети, що знаходяться якнайближче до джерела сигналу. Із предметів, що можуть розташовуватись на робочому столі – картонні, пінопластові, легкі пластикові вироби, тощо. Легкі ролети на вікнах, плакати на стінах також можуть бути використані в якості потенційних мішеней. Отже, для уникнення потенційного виливу інформації доцільним вважається використання щільних важких штор на вікнах, також можна використати на вікнах тонуючи плівки.

Література

1. Shkarlet, S. at al. (2019). The Model of Information Security Culture Level Estimation of Organization. Advances in Intelligent Systems and Computing, 1019, pp. 249–258.

2. Hulak, H., & Otto, G. (2020). Методи і моделі побудови інформаційних технологій дистанційного вимірювання нановібрацій . Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(8), 22-33. https://doi.org/10.28925/2663-4023.2020.8.2233

Гулак Г.М.
д.т.н., доцент,
Трофімов А.С.
Національна академія СБ України

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ СИСТЕМИ ДИСТАНЦІЙНОГО НАВЧАННЯ НА ОСНОВІ КОНЦЕПЦІЇ ПОВНОЇ НЕДОВІРИ

Актуальність дослідження обумовлена тим фактом, що відомі програмні платформи підтримки освітнього процесу в дистанційному режимі переважно забезпечують вирішення питань менеджменту цифровим навчальним

середовищем, при цьому лише частково відповідають на виклики і загрози з боку кіберпростору та потенційну можливість несумлінних дій з боку учасників освітнього процесу.

У рамках дослідження виконано аналіз та порівняння функцій захисту інформації сучасних навчальних платформ, на основі концепції повної недовіри «Zero Trust» [1] побудовано вдосконалену моделі загроз СДН, визначені основні напрями розвитку політики інформаційної безпеки на підставі вказаної концепції та уточнено архітектуру системи кіберзахисту інформаційних ресурсів СДН.

На підставі аналізу функцій навчальних платформ, а саме: Moodle, Blackboard, Canvas, Google Classroom, Khan Academy, які на поточний час використовуються закладами освіти, було визначено основні функції безпеки СДН, а саме: ідентифікація і автентифікація користувачів, контроль/управління доступом, криптографічний захист даних, моніторинг інцидентів та ведення журналу подій, політика конфіденційності, резервне копіювання, тестування/аудит/оновлення безпеки, політика надійних паролів.

Аналіз реалізацій визначених функцій безпеки показав, що жодна з перехованих систем не передбачає функцій і механізмів перевірки цілісності і автентичності ресурсів, а також їх авторства.

В якості вихідних даних для розробки моделі загроз СДН обрано запропоновану в [2] онтологічну модель освітнього процесу та ключове положення концепції повної недовіри, що вона стосується всіх без винятку учасників інформаційного обміну.

Модель загроз включає в себе: визначення ролей учасників освітнього процесу та їх повноважень в системі, несумлінні операції порушників кібербезпеки по відношенню до інформаційних ресурсів.

Базові елементи архітектури кіберзахисту СДН на основі концепції повної недовіри та вимог законодавства [3] зображені на рис.1.

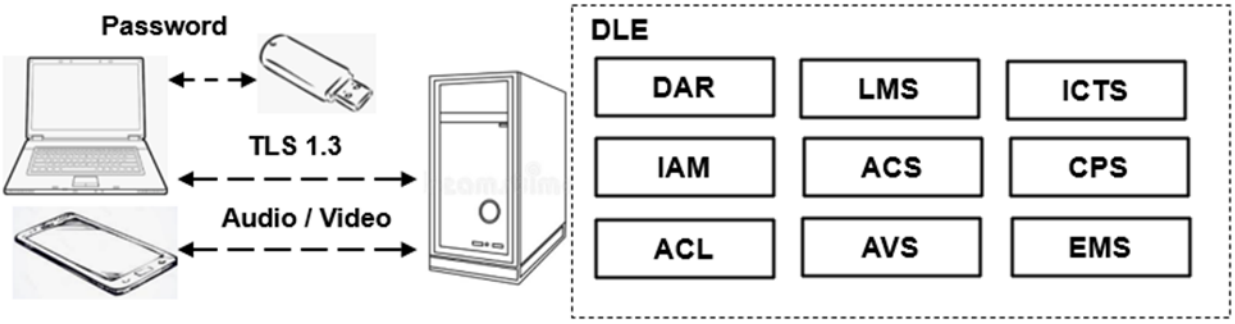


Рис. 1. Базові елементи архітектури кіберзахисту СДН

На рисунку використовуються наступні скорочення і позначення:
IAM –управління ідентифікацією та автентифікацією;
ACS –система управління доступом;
ACL –список контролю доступу;
AVS –антивірусна система;

CPS –система криптографічного захисту, яка забезпечує управління ключами, генерацію початкових паролів новим користувачам під час їх ініціалізації, формування кодів MAC та шифрування файлів;

DAR – база даних голосових еталонів користувачів СДН;

DLE – цифрове навчальне середовище;

EMS –система управління подіями, їх включаючи реєстрацію;

ICTS –система контролю цілісності та тестування системи захисту;

LMG – система підтримки навчального процесу;

TLS 1.3 – протокол захисту транспортного рівня (*transport layer security*).

З метою попередження фальсифікації інформаційних ресурсів, з урахуванням практик концепції повної недовіри, пропонується: створення спільного секретного (приватного) ключу k для певних учасників освітнього процесу, впровадження технології багатофакторної авторизації (в тому числі з використанням біометричних даних), підтвердження доступу в систему через додатковий канал. Спираючись на вказані механізми доцільно сформувати поетапну процедуру ідентифікації користувача, та інтегрувати її в політику інформаційної безпеки СДН.

Підсумовуючі викладене, можливо зазначити, що в рамках дослідження на основі концепції повної недовіри була розроблена модель загроз СДН, визначені практичні аспекти вдосконалення політики інформаційної безпеки з урахуванням вимог законодавства і зазначеної концепції, а також запропоновані механізми забезпечення захисту інформаційних ресурсів СДН.

Література

1. Michael Buckbee, «What Is Zero Trust? Architecture and Security Guide», [Електронний ресурс] 24.10.2019. URL: https://www.varonis.com/blog/what-is-zero-trust

2. Гулак Г.М. (2020) Методологічні засади побудови гарантоздатних захищених інформаційних систем дистанційного навчання закладів вищої освіти // Математичні машини і системи. 2020. № 4. С. 148–162.

3. Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах: Постанова Кабінету Міністрів України від 29.03.2006 р. N 373. URL: https://zakon.rada.gov.ua/laws/show/373-2006-п#Text

Гулак Г.М.
д.т.н., доцент,
Національна академія СБ України
Гулак Є.Г.
аспірант,
Корнієць В.А.
аспірант,
Інститут проблем математичних
машин і систем НАН України

БЕЗПЕКА ШИФРУВАННЯ КОРОТКИХ ПОВІДОМЛЕНЬ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Інформаційний обмін в інформаційно-комунікаційних системах (ІКС) об'єктів критичної інфраструктури, включаючи комплекси керування виконавчими механізмами, системи інформування про надзвичайні ситуації, промислові комп'ютеризовані системи пожежної безпеки і дистанційного контролю територій та об'єктів, інформаційно-діагностичні системи в технологіях IoT часто реалізується шляхом обміну короткими повідомленнями в мережах мобільного зв'язку.

На поточний час для швидкого обміну відносно короткими повідомленнями широко використовуються застосунки на мобільних платформах – месенджери [1]. Їх застосування не потребує швидкісних каналів зв'язку або оренди виділених IP-адрес, водночас механізми забезпечення безпеки приховані за завісою комерційного «ноу-хау». Це актуалізує питання підвищення кіберзахисту ІКС об'єктів критичної інфраструктури, в яких використовуються мобільні пристрої.

В переважної більшості наведених випадків існують потенційні загрози порушення конфіденційності чутливих даних, що може підвищувати ризики порушення сталого функціонування цих систем. Тому існує нагальна потреба забезпечення безпеки коротких повідомлень.

В [2] досліджено побудову ботнет на основі відео контейнерів для стеганографічного контенту на платформах SNS (Social Network Service). Показано, що створена схема може бути реалізована в додатку Telegram SNS.

В [3] запропоновано новий підхід для приховування факту відправлення коротких повідомлень на основі створення секретного IP-каналу.

Сучасний алгоритм блокового шифрування AES має високі якості і швидкодію. Водночас, в режимах ECB або CBC він потребує довжини повідомлення кратної 64 біт. З метою уникнення цього обмеження в [4] запропоновано його модифікацію, що придатна для шифрування повідомлень довжини кратної 32-бітам без розширення даних.

Підчас передачі по каналам зв’язку пакети даних можуть бути піддані атакам, внаслідок чого їх відхилить шифратор, а це може призведе до блокування функцій ІКС. Для уникнення подібної ситуації в [5] запропоновано метод на основі кодів сімейства Ріда-Соломона, який забезпечить доставку коротких важливих повідомлень при дотриманні балансу швидкості обслуговування і пропускної здатності мережі.

В [6] на основі криптосхеми Єль Гамаля запропоноване компактне асиметричне шифрування безпечне щодо атак з обраним шифрованим текстом.

Інформація щодо безпеки застосування асиметричних криптосистем для шифрування коротких повідомлень надана в дослідженні [7]. Проблемою асиметричних шифрів, як відмічене в [8], є небезпека тривалого застосування секретного ключа, у разі його компрометації існує загроза розшифрування всіх повідомлень, які перехоплені зловмисником раніше.

В рамках проведеного дослідження умов проведення атак на захищений мобільний інформаційний обмін шляхом розпізнавання поточного стану об’єкту критичної інфраструктури на основі статистики довжин шифрованих повідомлень (рисунок) зроблено висновок про потенційно високу вразливість таких систем та надано рекомендації щодо її подолання (рис. 1).

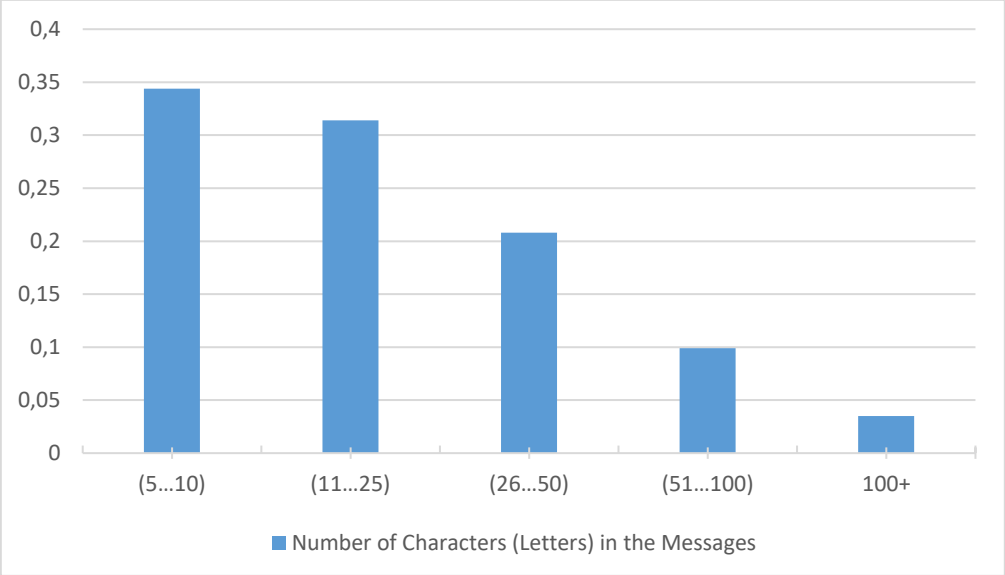


Рис.1. Розподіл довжин повідомлень в чатах WhatsApp

Загалом, підсумовуючи огляд систем кіберзахисту на мобільних пристроях можливо зробити висновок про недостатню увагу з боку розробників таких систем питанням блокування вразливості криптосистем, що обумовлена властивостями інформаційних потоків.

Література

1. Rosenfeld, A. et al. (2018) WhatsApp usage patterns and prediction of demographic characteristics without access to message content Sep. 27 2018 / Demographic Research 39, pp.647-670.

2. Kwak, M. Cho, Y. A (2021) Novel Video Steganography-Based Botnet Communication Model in Telegram SNS Messenger. Jan 2021 / Symmetry, Basel, 13 (1), 84, pp. 2-16.

3. Z. Trabelsi, et al., (2006) Traceroute Based IP Channel for Sending Hidden Short Messages, Proc. Advances in Information and Computer Security (IWSEC), October 2006. pp. 421–436.

4. Lu, E.H. Huang, K.T. Chiu, J.H. (2016) Word-Based AES Encryption Without Data Expansion. Jul. 2016 | Journal of Information Science and Engineering 32 (4), pp. 849-861.

5. Grushevsky, Y. L. et al. (2006) Adaptive RS Code for Message Delivery Over Encrypted Military Wireless Networks, MILCOM-2006 IEEE Military Communications conference, 2006, pp. 1-5.

6. Asbullah, M.A, Ariffin, M.K. (2012) A Proposed CCA-secure Encryption on an ElGamal Variant. 7th International Conference on Computing and Convergence Technology (ICCCT2012), pp. 499-503.

7. Bresson, E; Chevassut, O. Pointcheval, D. (2004) New security results on encrypted key exchange. 7th International Workshop on Theory and Practice in Public Key Cryptography 2004. Public Key Cryptography - PKC 2004, Proceedings 2947, pp.145-158.

8. B. Schneier, B. Hall (1997) An improved e-mail security protocol C. 13th Annual Computer Security Applications Conference 1997. 13th Annual Computer Security Applications Conference, Proceedings, pp. 227-230.

Гулак Г.М.
д.т.н., доцент, Національна академія СБ України
Скітер І.С.
к.ф.-м.н., доцент,
Гулак Є.Г.
аспірант, Інститут проблем математичних машин і систем НАН України
Цирканюк Д.А.
аспірантка, Київський університет імені Бориса Грінченка

БАЗОВІ ЗАСАДИ ПОБУДОВИ ЦЕНТРУ КІБЕРБЕЗПЕКИ ОБ`ЄКТІВ ЯДЕРНОЇ ЕНЕРГЕТИКИ

Галузь ядерної енергетики в умовах збройної агресії в Україні за суттю є становим хребтом економіки та найнебезпечнішим елементом критичної

інфраструктури. Технологічна складність цієї галузі, потенційні ризики виникнення нештатних ситуацій на об'єктах ядерної енергетики (ОЯЕ) внаслідок реалізації загроз техногенного, природного або антропогенного характеру, включаючи терористичні кібератаки на інформаційні інфраструктури, актуалізують завдання створення галузевого центру кібербезпеки (ГЦК).

Підвищення складності структури інформаційно-комунікаційних систем (ІКС) ОЯЕ, збільшення кількості видів та обсягів важливої інформації, яка циркулює в цих системах, а також постійне зростання потужності та різноманіття кібератак висувають особливі вимоги до побудови ВЦК який за архітектурою, апаратною і програмною платформами, рівнем професіоналізму персоналу, напрацьованими методиками реагування на кіберінциденти повинен відповідати викликам сучасності.

Збої програмної і апаратної платформ та спрямовані впливи на автоматизовані системи управління технологічними процесами здатні руйнувати або заблокувати інформаційні ресурси внаслідок чого ефективність функціонування обладнання ОЯЕ може бути суттєво знижена або створені передумови ситуацій, які матимуть катастрофічні наслідки.

Саме ГЦК повинен забезпечувати стале надійне функціонування інформаційних і технологічних систем ОЯЕ шляхом розвитку системи кібербезпеки та реалізації превентивних, блокуючих та нейтралізуючих організаційно-технічних заходів. В роботі запропонований системний підхід щодо визначення базових засад побудови ГЦК на основі врахування основних факторів, що впливають на стан кібербезпеки та на прийняття рішень щодо:

– визначення стратегічних і тактичних задач та функцій центру, їх регулярного уточнення;

– ідентифікації ресурсів, що підлягають захисту, та відстежування потенційних загроз безпеки, розробки і супроводженні моделей загроз безпеки і моделей порушника;

– формування вимог та параметрів безпеки ІКС ОЯЕ;

– тренінгів і навчань персоналу ОЯЕ, формування у персоналу культури кібербезпеки;

– реалізації організаційно-технічних заходів для оцінки рівня вразливостей та їх мінімізації в ІКС;

– надання дієвої допомоги персоналу ОЯЕ в випадках виникнення кіберінцидентів для блокування і локалізації загроз, ліквідації їх наслідків;

– участі спеціалістів центру у проведенні розслідувань випадків, які мали суттєві наслідки.

Пріоритетними завданнями наукових досліджень у сфері забезпечення кіберезпеки ОКІ є, створення моделі функціонування центру кібербезпеки та, забезпечення гарантоздатності автоматизованих систем ОЯЕ, як технологічної основи їх функціонування.

Актуальність і практична значущість визначеного завдання відмічена у доповіді на засіданні Президії НАН України [1], де звернута увага на необхідність забезпечення гарантоздатності автоматизованих систем ОЯЕ, в тому числі в частині забезпечення кібербезпеки об'єктів.

Щодо проблеми комп'ютерної безпеки ОЯЕ в роботі [2] зазначено, що рішення які були обрані системою безпеки на новозбудованих ядерних установках, призвели до зростання кіберзагроз для цих установок, а цілісність цифрових систем безпеки опинилася під загрозою. Огляд підходів ядерної промисловості до кібербезпеки з точки зору керівництва та проектування наведений в [3]. В роботі [4] розглянута проблема необхідності узагальнення проблем кіберзахисту на різних об'єктах критичної інфраструктури Німеччини та деяких інших країн.

В роботі [5] проведено аналіз факторів зниження ризику ядерних та радіаційних аварій на АЕС з урахуванням специфічних умов, пов'язаних з інформаційною безпекою в системі фізичного захисту атомних електростанцій.

В [6] основний акцент зроблено на комп'ютерну безпеку інформаційних та керуючих систем, важливих для ядерної безпеки. Розглядаючи аспекти безпеки, автори [7] звертають увагу на запобігання впливу методів соціальної інженерії, підвищення рівня культури інформаційної безпеки організації. Систематизація методів, моделей та основних підходів забезпечення кібербезпеки, виявлення кіберзагроз та їх класифікації представлена в [8].

Запропонована в роботі модель загроз ІКС ОЯЕ описує взаємодію системи захисту інформації із зовнішніми та внутрішніми факторами (рис.1).

На підставі проведеного аналізу були визначені наступні базові принципи побудови ГЦК: інтеграція, централізація, уніфікація, масштабованість, модульність, живучість.

Принципи інтеграції та консолідації доцільно реалізовувати відносно розрізнених масивів даних про ОЯЕ. Принцип централізації реалізується шляхом використання для всіх підсистем автоматизованої системи управління єдиних метаданих та нормативно-довідкової інформації.

Рис.1. Модель реалізації загроз інформаційній системі об'єкту ядерної енергетики

Принцип уніфікації реалізується в частині єдиної інформаційно-комунікаційної системи для всіх структур та форматів даних. Принцип масштабованості реалізується через можливість поетапної розробки і впровадження без принципової заміни технічної платформи. Принцип модульності реалізується через побудову ЦКБ як сукупності модулів реалізації окремих функцій і завдань, що забезпечує гнучкість підсистем і системи в цілому під необхідну структуру управління безпекою.

Принцип живучості реалізується через забезпечення безперебійної роботи, отримання достовірних результатів, захист від несанкціонованих дій.

Створення центру кібербезпеки ОЯЕ повинно підняти на якісно новий рівень стан безпеки підприємств галузі, а також координації заходів щодо розгортання системи безпеки для інформаційної інфраструктури на ОЯЕ.

Література

1. Носовський, А. В. (2021). Науково-технічний супровід робіт з подолання наслідків чорнобильської катастрофи. *Вісник Національної академії наук України*, (7), С. 32–36.

2. Park, J. K., Suh, Y. S., & Park, C. (2016). Implementation of cyber security for safety systems of nuclear facilities. *Progress in Nuclear Energy*, *88*, pp. 88–94.

3. Poresky, C., Andreades, C., Kendrick, J., & Peterson, P. (2017). *Cyber Security in Nuclear Power Plants: Insights for Advanced Nuclear Technologies.* (UCBTH-17-001). CA.

4. Berg, H.-P. (2017). Cybersecurity of critical infrastructures such as nuclear facilities. *ENERGETIKA, 63*(4), pp. 141–145.

5. Погосов, О. Ю., Дерев'янко, О. В. (2017). Фізичний захист АЕС та інформаційна безпека як необхідні умови зниження ризиків ядерних і радіаційних аварій. *Ядерна та радіаційна безпека, 3*(75), С.50–55.

6. Чумак, Д. В., Клевцов, О. Л. (2015). Комп'ютерна безпека на ядерних об'єктах в Україні: області взаємодії між ядерною безпекою та захищеністю. *Ядерна та радіаційна безпека, 3*(67), С.60–64.

7. Shkarlet, S. at al. (2019). The Model of Information Security Culture Level Estimation of Organization. *Advances in Intelligent Systems and Computing, 1019*, pp. 249–258.

8. Литвинов, В. В. та ін. (2018). Захист корпоративних мереж від атак з використанням контент-аналізу глобального інформаційного простору. *Технічні науки та технології, 1*(11), С.115–130.

9.*Computer security at nuclear facilities: reference manual: technical guidance.* (2011). International Atomic Energy Agency.

Гуменюк І.В.
к.т.н.,
Охрімчук В.В.
к.т.н.,
Кошева І.Г.
Житомирський військовий інститут імені С. П. Корольова

ОСОБЛИВОСТІ АНТИУКРАЇНСЬКОГО КІБЕРВПЛИВУ НА ОБ'ЄКТИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВНОГО СЕКТОРУ

Агресія росії в кіберпросторі розпочалася ще задовго до 2014 року, однак триває й досі. Перед початком агресії проти України було розгорнуто декілька успішних кампаній кібершпигунства. Перші кібератаки на інформаційні системи приватних підприємств та державних установ України були зафіксовані ще під час масових протестів наприкінці 2013 року, у той час більше 22 підприємств та державних установ України були заражені комп'ютерним хробаком, який потім отримав назву "Uroboros". Головною метою його було викрадення інформації, в тому числі персональних даних та паролів доступу до інформаційних ресурсів.

Проте у відкриту (активну) фазу війни в кіберпросторі росія перейшла в травні 2014 року під час президентських виборів, коли російські хакери вивели з ладу інформаційну систему Центральної виборчої комісії України "Вибори". Згодом у липні 2014 року офіційний веб-портал Президента України зазнав потужної DDoS-атаки, результатом чого інформаційний ресурс декілька годин був

недоступним, прес-служба глави держави була змушена розповсюджувати інформацію через інформагентства.

З того часу кібератаки стали більш масштабними, охоплювали енергетичну сферу та державні фінансові установи. Зокрема дії росії проти України стали першим випадком успішної кібератаки на цивільний об'єкт критичної інфраструктури. В ніч на 23 грудня 2015 року російськими хакерами було проведено успішну атаку на внутрішню мережу "Прикарпаття обленерго", було вимкнено близько 30 підстанцій, унаслідок чого близько 230 тисяч мешканців на декілька годин залишилися без світла. Нападники змогли отримати доступ до корпоративної мережі компанії завдяки вдалому зараженню комп'ютера одного із співробітників троянським шкідливим програмним забезпеченням "BlackEnergy". Ще одну атаку на енергетичну сферу було здійснено 18 грудня 2016 року на підстанції "Північна" в Києві. У результаті її реалізації протягом 2 годин через збій в автоматиці управління більшість споживачів північної частини правого берега Києва та прилеглих районів області залишилися без струму. Іншу масштабну кібератаку, під час якої постраждали сайти Міністерства фінансів, Держказначейства, Пенсійного фонду, було здійснено в грудні 2016 року, внаслідок якої було знищено частину інформації, а також виведено з ладу обладнання. У зв'язку з цим сталися затримки з бюджетними виплатами на сотні мільйонів гривень. Для виведення з ладу серверів державних фінансових установ зловмисники використовували "KillDisk" (програма для знищення файлів з комп'ютерів/серверів), а також троянську програму "BlackEnergy", ту саму, що і в атаці на "Прикарпаттяобленерго". Але наймасштабнішою атакою, яку на собі відчув кожен українець, вважається атака з використанням вірусу "NotPetya". Вона відбулася 27 червня 2017 року, було заражено близько 12 тисяч персональних комп'ютерів, більшість із яких належала приватним українським організаціям, а також Уряду, банкам, державним енергетичним компаніям, київському аеропорту та метрополітену. Від атак постраждала значна кількість приватних компаній, торгові мережі (METRO Cash&Carry, Novus, Fozzy, Епіцентр, Рост тощо), телеком-оператори (Київстар, Vodafone, Lifecell), мережі заправних станцій (WOG, KLO), транспортні та енергетичні компанії.

Не виключенням є військова сфера. За словами екс-командувача Головного управління зв'язку та інформаційних систем Генерального штабу Збройних Сил України генерал-лейтенанта Володимира Рапка починаючи з 2014 року, зафіксовано інтенсивне збільшення кількості кібератак різного ступеня складності, направлених на порушення функціонування інформаційно-комунікаційних систем Збройних Сил України. Як правило, застосовувалися DDoS атаки на системи й розповсюдження шкідливого програмного забезпечення.

Наприклад, одним із пристроїв кібербезпеки було зафіксовано DDoS атаки на веб-сайт Міністерства оборони України – більше 6 тисяч звернень до сайту на секунду. За своєю географією найбільше атак відбувається з території росії, але

також можуть використовуватись майданчики союзних нам країн для її проведення, що ускладнює остаточну ідентифікацію.

Від початку війни тенденція на зростання кількості кібератак зберігається. Так, у ІІІ кварталі 2022 за допомогою засобів Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки було опрацьовано 24 млрд. подій. Кількість зареєстрованих та опрацьованих кіберінцидентів зросла – від 64 до 115.

У ІІІ кварталі 2022 року фіксується істотне зростання активності хакерських груп щодо розповсюдження шкідливого програмного забезпечення, серед якого є як програми, що викрадають дані, так і ті, які спрямовані на знищення даних. Порівняно зі статистичними даними за ІІ квартал 2022 року, кількість кіберінцидентів з високим рівнем критичності зросла на 128%.

Порівняно з І та ІІ кварталами, у ІІІ кварталі 2022 року кількість критичних подій кіберінцидентів, джерелом яких є IP-адреси росії, зросла у 35 разів. Також, порівняно з ІІ кварталом 2022 року, майже вдвічі зросла кількість детектованих подій ІБ, пов’язаних із активним скануванням, джерелом яких є IP-адреси росії.

Проаналізувавши дії росії в кіберпросторі, можливо виділити ряд принципових особливостей їх організації та проведення. Вплив на критичну інформаційну інфраструктуру здебільшого має перманентний характер. Кіберпростір використовується росією як для проведення кібератак на Україну, так і проведення інформаційних операцій. Завжди спостерігається активізація дій росії в кіберпросторі в період важливих подій, політичних чи економічних змін у країні. Крім того відбуваються збільшення кіберінцидентів перед початком бойових дій. Тож можна вважати, що кібератаки тісно пов’язані з проведенням військових, інформаційних операцій чи політичних кроків. Так, наприклад, більше ніж за місяць до повномасштабного вторгнення на територію України в середині січня росія провела масштабну кібератаку на понад 20 українські урядові установи, намагаючись знизити здатність країни протистояти майбутньому воєнному нападу з боку москви. Серед головних цілей ворожих хакерів – шпіонаж (отримання розвідданих щодо логістики, озброєння, планів та операцій Сил безпеки та оборони), спроби виведення з ладу об’єктів критичної інформаційної інфраструктури, позбавлення доступу громадян до державних послуг та сервісів, банківського обслуговування тощо. А також – інформаційно-психологічні операції та дезінформаційні “вкиди” з метою підриву довіри до спроможностей органів державної влади, Сил безпеки та оборони, поширення панічних настроїв серед населення. За атрибуцією абсолютна більшість кіберінцидентів пов’язана з хакерськими угрупуваннями, що фінансуються урядом росії.

Таким чином кіберінциденти та кібератаки мають негативне місце у забезпечення кібербезпеки та національної безпеки держави у тому числі. При цьому для росії як у збройній немає правил, так і в кібервійні вона не дотримується їх. Саме тому, врахування особливостей проведення росією кіберрозвідки, здійснення кібервливу на об’єкти критичної інфраструктури, базову підготовку з питань

кібергігієни військово- та держслужбовцями України є одним із ключових факторів досягнення інформаційної ті кіберпереваги над противником.

Дмитренко Ю.П.
к.ю.н., професор,
Національна академія СБ України
Дмитренко Е.С.
д.ю.н., професор,
Київський національний економічний університет імені Вадима Гетьмана

ВИКОРИСТАННЯ OSINTу У ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ: ОРГАНІЗАЦІЙНІ, КАДРОВІ ТА ФІНАНСОВІ ПИТАННЯ

Розвідка на основі аналізу відкритих джерел інформації (OSINT) є невідємною частиною діяльності розвідувальних органів європейських країн. Характерною особливістю застосування цього методу є поєднання OSINT з іншими видами розвідки та використання різних методів добування інформації, що значно підвищує ефективність та результативність процесу прийняття управлінських рішень. Розвідувальна діяльність із використанням відкритих джерел збільшує можливості спеціальних служб, але в її роботі є чотири критичні компоненти, на які необхідно звертати увагу при роботі: джерела, програмне забезпечення, послуги та неупереджений аналіз. Їх комплексна цінність завжди зіставляється з якістю розвідувальної інформації. Насамперед, варто зазначити, що кількість джерел інформації та її обєми в OSINT є незрівнянно вищими, ніж у результаті її отримання оперативним шляхом, що вимагає застосування високотехнологічних спеціальних автоматизованих комплексів обробки інформації та розробки відповідного інноваційного програмного забезпечення. Розвиток інформаційних технологій, збільшення інформаційних потоків зумовили зростання ролі OSINT у розвідувальній діяльності спеціальних служб. Аналіз відкритих джерел інформації проводиться практично всіма спеціальними службами, однак організована ця діяльність у різних країнах по-різному. Найбільшу складність у процесі розвідувальної діяльності на основі аналізу відкритих джерел інформації зумовлюють широкі можливості проведення спеціальних операцій щодо дезінформації [1]. Збір інформації з відкритих джерел нині є досить ефективним, він широко використовується для характеристики одного з напрямів діяльності більшості спеціальних служб світу. Також є значна кількість спеціальних досліджень, присвячених розробці новітнього інструментарію пошуку розвідувальної інформації в мережі Інтернет. Розвідка в компютерних мережах охоплює процедури збору й обробки інформації, які

проводяться з метою підтримки прийняття рішень у сфері забезпечення національних інтересів, виключно з відкритих джерел [1].

Основоположником терміна OSINT «розвідка з відкритих джерел» (Open Source INTelligence – OSINT) вважається розвідувальне співтовариство США, яке почало активне його використання ще з лютого 1941 р. (створення Інформаційної служби закордонного віщання – Foreign Broadcast Information Service — FBIS) [2]. Найширше використання «OSINT» також здобули у США. Можна навести перелік організацій які користуються цим методом: Рада із захисту відкритих джерел (DOSC); Командування розвідки і безпеки ЗС США (INSCOM); Служба розвідувальної інформації Департаменту сухопутних військ (DA IIS); Національна розвідка центру відкритих джерел (DNI OSC); Академія відкритих джерел; Департамент передових систем (ASD); ФБР; Дослідницька служба бібліотеки Конгресу (Congressional Research Service). США використовує інформацію, отриману за допомогою «OSINT», в більшій мірі для планування бойових дій, організації та проведення військових операцій, запобігання терористичним актам [3]. На думку аналітиків розвідки США найбільшою проблемою методу «OSINT» на даний момент вважають неперевірені джерела інформації, провокуючі ресурси, де найбільший ризик недостовірної інформації. Для отримання найбільш актуальної та якісної інформації користувач повинен обробити великий масив з різних джерел, узагальнити їх так, як вимагає мета та завдання дослідження. У США сформована розгалужена мережа центрів і пунктів, що ведуть OSINT-розвідку та надають відомості більш ніж 7 тис. споживачам розвідувальних даних. І це не що інше, як результат скоординованих дій законодавчої і виконавчої влади, спрямованих на проведення цілеспрямованої політики в галузі забезпечення національної безпеки. Подібні структури є на всіх рівнях. За результатами різних експертних оцінок, американські розвідувальні служби з відкритих джерел добувають від 35 % до 95 % розвідданих. Частка витрат OSINT у розвідувальному бюджеті США складає лише 1 % [4].

Ізраїль також ефективно використовує «OSINT», в першу чергу для аналізу військової спроможності противника. В структурі військової розвідки існує окремий спеціальний підрозділ для аналізу відкритих джерел інформації «Hatsaf», який збирає інформацію лише для військових цілей. У Великобританії за допомогою «OSINT» цивільні журналісти служби BBC Monitoring здійснюють первинний збір інформації, яка в подальшому потрапляє до співробітників спецслужб для її використання за конкретними напрямами досліджень[3].

Як приклад інтенсивності та оптимальності організації OSINT можна розглянути Бельгію. Спеціальної нормативної основи, яка регламентує діяльність OSINT, на загальнодержавному рівні в Бельгії не існує. Разом із тим відомчими нормативними актами, які мають обмежений доступ створено відповідний підрозділ, який організаційно входить до складу Штабу Оборони Бельгії — Головної служби розвідки та безпеки (Service Général du Renseignement et de la

Sécurité /SGRS/). Напрями діяльності та завдання підрозділу OSINT визначаються в плані збору інформації, який розробляється на підставі щорічного головного плану розвідки (затверджується урядом) та пріоритетних розвідувальних завдань. На підставі згаданого плану збору інформації підрозділ OSINT розробляє тематику огляду міжнародної преси, передплату газет, спеціалізованих та періодичних видань, передплату на доступ до спеціалізованих баз даних, тематику та спрямованість моніторингу оперативних новин. Крім цього, тематика огляду преси та моніторингу новин може змінюватись та доповнюватись (корегуватись) протягом року відповідно до розвитку обстановки у світі. Підрозділ розвідки з відкритих джерел має загальну чисельність всього 7 осіб. Щорічно отримує та готує доповіді на більше 1500 різноманітних запитів на інформацію; Бюджет підрозділу OSINT на рік становить близько 650 000 євро на доступ до спеціалізованих баз даних. Ця сума не враховує передплату на газети, журнали та інші періодичні видання. Як одну з основних баз даних інформації підрозділ OSINT використовує FACTIVA, доступ до якої за рік коштує 25 000 євро. Раніше підрозділ використовував французьку Lexis Nexis, яка оцінюється як менш спроможна порівняно з FACTIVA [1].

Зважаючи на міжнародний досвід використання «OSINT», для отримання якісної та актуальної інформації необхідно не лише опрацьовувати велику кількість джерел інформації, а обробляти її, аналізувати, перевіряти та знаходити підтвердження досліджуваних фактів, подій та явищ, адже багато інформації створюється саме для дезінформації, проведення ІПСО.

Ще у листопаді 1941 року в м. Портланд (штат Орегон) була розгорнена перша станція моніторингу. Після початку Другої світової війни FBMS була передана в підпорядкування одному з трьох департаментів МО США (Department of Defense), а саме – Department of the Army (DA). 1947 року FBMS була переіменована у Foreign Broadcast Information Service (FBIS) і введена в структуру ЦРУ (CIA). До моменту поглинання служби в її підпорядкуванні знаходилося 19 станцій моніторингу, розгорнутих у різних країнах світу. Їх співробітниками були не тільки громадяни США, але й місцеві жителі (носії мови). Частина матеріалів переводилася відразу на місцях, інша відправлялася в центральний офіс в м. Рестон (штат Вірджинія). Основними споживачами підготовлюваних службою документів були понад 700 абонентів Розвідувального співтовариства (Intelligence Community), урядові і правоохоронні органи, а також різні відомства федерального та місцевого рівнів [4]. Події 11 вересня 2001 року спонукали керівництво США переглянути роль відкритих джерел в структурі інформаційно-аналітичної діяльності ключових державних органів; 2004 рік ознаменувався для американської розвідки початком нового етапу масштабного реформування. Цього року Джордж Буш підписав закон «Про реформування розвідки та протидію терористичній загрозі» (Intelligence Reform and Terrorism Prevention Act of 2004), що містить вказівки про включення OSINT-розвідки як повноцінного і

рівноправного виду в діяльність Розвідувального співтовариства, а також про формування національного центру розвідки на основі аналізу відкритих джерел [5].

Дослідження цього питання дає підстави дійти висновку, що проведення розвідки на основі аналізу відкритих джерел інформації є базовою складовою у діяльності розвідувальних органів провідних країн світу. Особливістю застосування зазначеного методу є поєднання OSINT з іншими видами розвідки та використання різних методів добування інформації, що в значній мірі підвищує ефективність та якість процесу прийняття управлінських рішень. Організація розвідувальної діяльності із використанням відкритих джерел значно збільшує стартові та потенційні можливості спецслужб, в роботі яких є чотири ключові складові, на які необхідно звернути увагу: джерела, програмне забезпечення, послуги та аналіз. Їх цінність завжди співвідноситься з якістю розвідувальної інформації. Насамперед, варто зазначити, що кількість джерел інформації та їх обсяги в OSINT є незрівнянно вищими, ніж у результаті її отримання оперативним шляхом, що вимагає застосування потужних спеціальних автоматизованих комплексів обробки інформації та розробки ефективного програмного забезпечення. В ході ведення сучасної високотехнологічної гібридної війни, слід враховувати, що отримання інформації з різних джерел (в тому числі, і з відомих видань) не гарантує її достовірності, а навпаки: з одного боку може бути загрозою при проведенні ворогом інформаційно-психологічної інформації, а з іншого - при веденні розвідувальної діяльності використовувати відкриті джерела та їх широке використання для проведення спеціальних заходів дезінформації противника.

Література

1. Бурба В.В. Організаційно-правові засади використання розвідки з відкритих джерел інформації (OSINT) в діяльності розвідувальних служб європейських країн. Юридичний бюлетень. випуск 11. Ч. 1. 2019. С. 11-19 DOI https://doi.org/10.32850/2414-4207.2019.11-1.01.

2. Open Source Intelligence. FMI 2-22.9. December 2006. Federation of American Scientists. URL: http://www.fas.org/irp/doddir/army/fmi2-22-9.pdf.

3. Серватовський А. В., Онищенко Ю. М., Макаренко П. В. Міжнародний досвід використання OSINT. Актуальні питання протидії кіберзлочинності та торгівлі людьми. Харків, 2018. С. 379- 381.

4. Електронна енциклопедія Wikipedia. Англомовна версія [Електронний ресурс]. Режим доступу:http://en.wikipedia.org/wiki/ United_States_Intelligence_ Community.

5. Кожушко О.О. Розвідка відкритих джерел інформації (OSINT) у розвідувальній практиці США. Київ: Інститут міжнародних відносин НАУ. С.68-74.

Дмитрук Н.Ю.
Національна академія СБ України

ПРОБЛЕМИ ПРОТИДІЇ КІБЕРНЕТИЧНИМ АТАКАМ рф НА ОБ'ЄКТИ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Актуальність цієї теми полягає в тому, що кібернетичні атаки стають все більш складними та суттєвою загрозою для критичної інформаційної інфраструктури різних держав, у тому числі й України. Російська Федерація, як відомо, активно використовує кібернетичні технології для здійснення кібернетичних атак на об'єкти критичної інформаційної інфраструктури, що може призвести до серйозних наслідків для національної безпеки та економіки країни.

З цієї причини, ефективні заходи протидії кібернетичним атакам Російської Федерації на об'єкти критичної інформаційної інфраструктури є надзвичайно важливими для забезпечення безпеки держави та її громадян. Розвиток таких заходів, які враховують специфіку кібернетичних загроз та потенційні наслідки, є необхідним для запобігання можливим атакам та забезпечення стійкої роботи критичної інформаційної інфраструктури країни [1].

Метою даної теми є розробка та вдосконалення ефективних заходів протидії кібернетичним атакам Російської Федерації на об'єкти критичної інформаційної інфраструктури. Основна мета полягає в забезпеченні безпеки національної інформаційної інфраструктури, яка є життєво важливою для функціонування економіки, соціальних та державних структур країни.

Зараз кібернетичні атаки Російської Федерації на об'єкти критичної інформаційної інфраструктури стали серйозною загрозою для безпеки країн світу, в тому числі і для України.

Для ефективної протидії таким атакам, необхідно розробити і впровадити відповідні заходи, серед яких можуть бути наступні:

1. Підвищення свідомості громадян та фахівців щодо кібернетичних загроз та методів захисту від них.
2. Підвищення рівня кібербезпеки на різних рівнях - від індивідуальних користувачів до великих корпорацій та державних органів.
3. Розробка та впровадження високоефективних технічних засобів захисту від кібернетичних атак, включаючи системи виявлення та реагування на атаки.
4. Підвищення рівня кібербезпеки в області критичної інформаційної інфраструктури, такої як енергетика, транспорт, банківська система, забезпечення яких є важливим для функціонування держави та суспільства.
5. Запровадження міжнародного співробітництва та обміну інформацією з метою ефективного захисту від кібернетичних загроз, включаючи спільні дослідження, тренінги та вправи.

6. Розробка та впровадження ефективних правових механізмів, що регулюють дії у сфері кібербезпеки та кібернетичної війни.

Кібербезпека є ключовою складовою безпеки держави [2]. Російська Федерація використовує кібернетичні атаки як ефективний інструмент у своїй геополітичній стратегії. Критична інформаційна інфраструктура є особливо вразливою до кібернетичних загроз. Кібератаки можуть призвести до серйозних наслідків, таких як втрата конфіденційної інформації, порушення роботи енергетичних систем, транспорту, фінансових і банківських установ, медичних закладів та інших критичних об'єктів. Ефективна протидія кібернетичним атакам Російської Федерації на об'єкти критичної інформаційної інфраструктури потребує розробки та впровадження новітніх технологій та заходів кібербезпеки, які забезпечать захист від різних видів кібернетичних загроз. До таких заходів можуть відноситись: розробка та впровадження ефективної системи виявлення та протидії кібернетичним атакам, забезпечення захисту мережі та системи керування критичної інформаційної інфраструктури, підвищення кваліфікації фахівців з кібербезпеки, створення механізмів взаємодії між державними та приватними секторами з метою забезпечення кібербезпеки. Важливо також вдосконалювати національну правову базу з кібербезпеки та забезпечувати виконання законодавства в цій сфері, забезпечувати міжнародну співпрацю з країнами-партнерами.

Підвищення культури кібербезпеки серед населення та бізнес-середовища є однією з ключових складових ефективної протидії кібернетичним атакам. Необхідно розвивати свідомість про кібербезпеку, надавати інформаційну підтримку та навчання з цієї теми, а також залучати громадськість до допомоги у виявленні та протидії кіберзагрозам.

Забезпечення кібербезпеки має бути комплексним та системним підходом, який враховує технічні, організаційні, кадрові та правові аспекти. Для досягнення максимальної ефективності необхідно планувати та розробляти стратегії кібербезпеки, які враховують специфіку кожного конкретного об'єкту критичної інформаційної інфраструктури [3].

Розробка та впровадження заходів протидії кібернетичним атакам на об'єкти критичної інформаційної інфраструктури є важливою складовою національної безпеки та є відповідальністю держави. Успішність таких заходів залежить від залучення ресурсів, виконання спеціальних програм та стратегій, які враховують специфіку кібернетичних загроз та потенційні наслідки для національної безпеки.

Висновок. Отже, кібербезпека є надзвичайно важливою темою в наш час, оскільки кібернетичні загрози стають все більш складними та небезпечними. Російська Федерація відома своїми агресивними кібернетичними діями проти інших країн, що може призвести до серйозних наслідків для критичної інформаційної інфраструктури. Розвиток ефективних заходів протидії кібернетичним атакам Російської Федерації на об'єкти критичної інформаційної

інфраструктури є надзвичайно важливим завданням для забезпечення національної кібербезпеки. Для досягнення цієї мети необхідно розробляти та впроваджувати ефективні заходи захисту, які будуть враховувати новітні кібернетичні загрози та забезпечувати стійкість критичної інформаційної інфраструктури від кібернетичних атак. Важливим аспектом є також розробка механізмів моніторингу та виявлення кібернетичних загроз, що дозволить своєчасно виявляти та реагувати на кібернетичні атаки. Підвищення кваліфікації фахівців з кібербезпеки також є важливим елементом у забезпеченні ефективного захисту критичної інформаційної інфраструктури. Тільки за допомогою поєднання різноманітних заходів можна досягти високого рівня кібербезпеки та захистити важливу інформацію від кібернетичних загроз.

Література

1. Абрамов В. І., Зюзя О. В. Удосконалена базова модель міждержавного протиборства з урахуванням сучасних тенденцій російсько-української війни. [URL.: http://www.dy.nayka.com.ua/].

2. Про критичну інфраструктуру Документ 1882-IX, чинний, поточна редакція – Редакція від 05.12.2022, підстава – 2684-IX [URL.: https://zakon.rada.gov.ua/].

3. ЗАКОН УКРАЇНИ Про національну безпеку України [URL.: https://ips.ligazakon.net/].

Загика М.В.
Національна академія СБ України

КІБЕРЗАХИСТ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: ПОШУК ПРОБЛЕМ ТА ШЛЯХІВ ЇХ ВИРІШЕННЯ

Кінцевою метою хакерів, як правило є збагачення. Відрізняються тільки шляхи досягнення кінцевої мети: шифрування даних на кінцевих пристроях користувачів з метою вимагання коштів за розшифрування, фішинг, викрадення баз даних з персональними або будь-якими іншими даними, за які можна отримати кошти тощо. Однак, ситуація в українському кіберпросторі дещо інша. Кількість кібератак та кіберінцидентів із початком повномасштабного вторгнення різко зросла. Крім того, кібератаки часто передують або ж корелюють із кінетичними атаками ворога. Стає зрозуміло, що за більшістю кібератак стоять російські спецслужби та хактивісти, що працюють на уряд російської федерації, адже більшість атак було спрямовано на державний сектор та сектор безпеки і оборони [1-3].

Метою російської федерації є українська інформаційна інфраструктура: її знищення чи отримання доступу до українських державних інформаційних ресурсів. Варто розуміти, що кібератаки можуть бути допоміжним інструментом за допомогою якого ворог проводить його інформаційно-психологічні операції з метою створення панічних настроїв та поширення пропаганди й дезінформації. Свідченням цього можуть бути розсилання інформаційних повідомлень із шкідливим програмним забезпеченням, в тому числі із скомпрометованих електронних скриньок органів державної влади, – збільшення кібератак на засоби масової інформації [4-6]. Але, варто розуміти, що кібератаки становлять серйозну загрозу інформаційній безпеці держави. Атаки на логістичний сектор та державні інформаційні ресурси, ресурси органів державної влади, телекомунікаційну сферу – можуть спричинити не просто панічні настрої, а ускладнити функціонування та взаємодію між суб'єктами важливими для функціонування держави [7].

З початком повномасштабного вторгнення на армію та державу почали посилено працювати об'єкти критичної інфраструктури, а отже стали пріоритетною ціллю для ворога, в тому числі й у кіберпросторі. Захист таких об'єктів у кіберпросторі є складовою національної безпеки держави. Однак, наразі лише розпочато процес формування реєстру об'єктів критичної інфраструктури, категоризацію об'єктів критичної інфраструктури у секторах і досить тривалий період займе процес реалізації усіх вимог з організації заходів безпеки на цих об'єктах. Одним із напрямків забезпечення безпеки об'єкта критичної інфраструктури є його кіберзахист.

На сьогодні основними суб'єктами національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України. Кожен із цих суб'єктів виконує свої завдання із забезпечення кібербезпеки держави. Зрозуміло, що ці структури взаємодіють та обмінюються інформацією щодо кіберзагроз між собою, а в певних випадках і з міжнародними партнерами. Однак, процес захисту об'єктів критичної інфраструктури лише розпочався, що стосується як законодавчої частини, так і реалізації заходів вже на фізичному та технічному рівнях.

Вже в умовах воєнного стану під триваючими кінетичними та кібернетичними атаками різко збільшилась кількість об'єктів, яким необхідно забезпечити кіберзахист. Процес побудови захисту об'єктів критичної інфраструктури вже в умовах воєнного стану вимагає швидких дій, що також може чинити певний негативний вплив, оскільки для кожного об'єкту необхідно створити індивідуальний комплекс заходів, що вимагає більше часу, ніж розробка типових стандартних рекомендацій чи положень для усіх об'єктів загалом. Треба також зазначити, що відповідно до постанови Кабінету Міністрів України від 9 жовтня 2020 року № 1109 «Деякі питання об'єктів критичної інфраструктури» до

об’єктів критичної інфраструктури може бути віднесено установу як державної, так і приватної форм власності. Разом з тим, для приватних структур наразі відсутній обов’язковий механізм моніторингу та інформування основних суб’єктів національної системи кібербезпеки про кіберінциденти. Також, в Україні є лише Урядова команда реагування на комп’ютерні надзвичайні події CERT-UA, галузеві команди чи ті, які функціонували б при якійсь бізнес структурі – відсутні. Крім того, CERT-UA опрацьовує лише певну частину кіберінцидентів у державному секторі і ті запити приватних установ, що були ними ініційовані. Тобто, повномасштабної статистики щодо кіберзагроз наразі немає.

Ще однією проблемою стає нестача профільних фахівців у сфері кіберзахисту. Це стосується і об’єктів критичної інфраструктури, яким необхідні такі фахівці для забезпечення підтримки кібербезпеки та швидкої реакції у разі кіберзагрози на об’єкті, так і основних суб’єктів національної системи кібербезпеки, оскільки на них теж збільшується відповідне навантаження.

Отже, для ефективного кіберзахисту об’єктів критичної інфраструктури: швидкого реагування та запобігання кіберзагрозам, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем об’єктів можна запропонувати такі шляхи вирішення проблем:

- удосконалення механізмів взаємодії та обміну інформацією про кіберзагрози між основними суб’єктами національної системи кібербезпеки;
- створювати навчальних програм та курсів для підготовки кадрів у сфері кіберзахисту, а також, системне напрацювання та підвищення рівня знань, вмінь та практичних навичок фахівців з кіберзахисту;
- створення регіональних та галузевих центрів та команд реагування на кіберінциденти та кіберзагрози;
- залучення міжнародних партнерів для підготовки українських фахівців.

Література

1. У ніч повномасштабного вторгнення рф ворог хотів знищити весь кіберзахист України, – СБУ: веб-сайт. URL: https://ssu.gov.ua/novyny/u-nich-povnomasshtabnoho-vtorhnennia-rf-voroh-khotiv-znyshchyty-ves-kiberzakhyst-ukrainy-sbu-video (дата звернення: 18.03.2023).

2. Former Conti ransomware gang members helped target Ukraine, Google says: веб-сайт. URL: https://www.theverge.com/2022/9/7/23341045/former-conti-ransomware-gang-target-ukraine-google (дата звернення: 18.03.2023).

3. «Позбавити українців інформації». У Держспецзв’язку прокоментували кібератаку на Укрінформ: веб-сайт. URL: https://biz.nv.ua/ukr/tech/kiberataka-na-ukrinform-u-derzhspeczv-yazku-nazvali-naslidki-novini-ukrajini-50298355.html (дата звернення: 19.03.2023).

4. Держспецзв’язку: вороги атакують електронні пошти військових: веб-сайт. URL: https://ms.detector.media/manipulyatsii/post/29036/2022-02-25-derzhspetszvyazku-vorogy-atakuyut-elektronni-poshty-viyskovykh/ (дата звернення: 19.03.2023).

5. «Бійтесь і чекайте гіршого»: хакери атакували урядові сайти та «Дію» : веб-сайт. URL: https://www.pravda.com.ua/news/2022/01/14/7320353/(дата звернення: 18.03.2023).

6. Довідкова інформація з питань діяльності CERT-UA за фактами впливу на стан кібербезпеки у 2022 році: Computer Emergency Response Team of Ukraine: веб-сайт. URL: https://cert.gov.ua/article/37121 (дата звернення: 16.06.2022).

7. Статистика кібератак на українську критичну інформаційну інфраструктуру: 15–22 березня: Державна служба спеціального зв’язку та захисту інформації України: веб-сайт. URL: https://cip.gov.ua/ua/news/statistika-kiberatak-na-ukrayi nsku-kritichnu-informaciinu-infrastrukturu-15-22-bereznya (дата звернення: 20.03.2023).

Іванів В.І.
Національний університет оборони України імені Івана Черняховського

АНАЛІЗ УМОВ, ЯКІ ФОРМУЮТЬ ПОЯВУ КІБЕРЗАГРОЗ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ СИСТЕМІ ВІЙСЬК (СИЛ)

У сучасному суспільстві кібератаки стають частішими та мають тенденцію чинити все значніший і триваліший вплив на економіку країни, незаперечним є той факт, що надійний захист від кібератак активно впливає на стан економічної, політичної, соціальної, оборонної та інших складових національної безпеки держави [1].

Очевидним є той факт, що порушення функціонування об’єктів критичної інфраструктури держави може призвести до розвитку надзвичайних ситуацій, пов’язаних із загибеллю людей, екологічними катастрофами, заподіянням великого матеріального, фінансового, економічного збитку або великомасштабними порушеннями життєдіяльності міст та населених пунктів. У цих умовах надзвичайно важливу роль відіграє забезпечення безпеки, у тому числі і кібербезпеки об’єктів критичної інфраструктури держави.

Враховуючи зазначене вище, метою тез є визначення основних факторів, що впливають на стан кібербезпеки об’єктів критичної інфраструктури.

Проведений аналіз існуючих систем захисту інформації, дає змогу визначити основні складові частини системи кіберзахисту інформаційно-комунікаційних систем об’єктів критичної інфраструктури:нормативно-правова; організаційна; технічна; підготовка, перепідготовка та підвищення кваліфікації відповідних

фахівців. Кожна із приведених вище складових частин, так чи інакше, впливає на стан кібербезпеки інформаційно-комунікаційних системи військ (сил).

Інформаційно-комунікаційна система військ (сил) зазвичай являються об'єктом захисту, як цілісне утворення. В той же час, їх складові елементи: обслуговуючий персонал, математичне, програмне, технічне, інформаційне забезпечення тощо можливо розглядати, як окремі об'єкти захисту від кіберзагроз.

Кіберзагрози для інформаційно-комунікаційна система військ (сил) можуть виходити з різних джерел: навмисних, ненавмисних, природних.

Джерела кібератак для інформаційних систем об'єктів критичної інфраструктури можуть знаходитись як ззовні (зовнішній порушник) так і зсередини.

Проте на практиці використання такого обладнання дає змогу побудувати мережевий міст на відстань лише до 10 кілометрів, за умови прямого бачення. Та навіть такі технічні характеристики дають змогу виявити деякі критичні вразливості в даному обладнанні та використати їх для реалізації кібернетичних атак зокрема впровадження атаки всередині (інсайдерства) [2].

Використання стандартних даних для адміністрування такого пристрою, дає можливість зловмиснику здійснити підключення з будь якої точки, яка знаходить ся в радіусі дії даного телекомунікаційного обладнання, тим самим отримати доступ до мережі, стати його повноправним клієнтом або просто переконфігурувати обладнання з метою виведення зі строю лінії прив'язки.

Сценарій кібервпливу, зводиться до того, що підключитися до такого мережевого мосту в радіусі дії такої антени, тобто в неконтрольованій зоні, це лише питання декількох хвилин. А результати такого підключення, в залежності від того, яка інформація передається по мосту можуть бути непередбачуваними.

В даний момент інформаційно-комунікаційна система ЗС України надає всі послуги для обміну інформацією в внутрішній мережі. Проте особливості побудови інформаційно-комунікаційних систем відкривають для зловмисників ряд вразливостей за допомогою яких чутлива інформація може потрапити до них. Можемо виділити такі аспекти, а точніше пробіли в безпеці важливої інформації.

Для контролю за обміном повідомленнями та документами в ЗС України розгорнуто поштові сервери та систему електронного документообігу. Дані сервіси контролюється підрозділами по забезпеченню кібернетичної безпеки, тобто виток інформації з такого серверу чи системи зведений до мінімуму. Проте користувачам не завжди до вподоби використання даних сервісів і вони наполегливо користуються сторонніми поштовиками та файловими обмінниками. Результатом цього є втрата гігабайтів інформації, що були передані таким способом.

Викрадення та аналіз такої інформації здійснюється зловмисниками з метою отримання розвід-даних, а в деяких випадках така інформація використовується, для публікації в ЗМІ, з метою компрометації Збройних Сил України, дестабілізації

ситуації в підрозділах та є доказом безвідповідальності користувачів інформаційно-комунікаційної системи ЗС України.

Варто зауважити, що інформаційно-комунікаційної системи ЗС України функціонують та виконують завдання за призначенням, проте через безвідповідальність деяких користувачів, точками входу до інформаційно-комунікаційної системи може стати необачно підключений до АРМ пристрій для виходу в Інтернет.

Відповідно проведеного аналізу, на стан забезпечення кібербезпеки інформаційно-комунікаційної системи об’єкта критичної інфраструктури можуть впливають такі фактори: наявність необхідної та достатньої нормативно-правової бази з питань забезпечення кібербезпеки інформаційно-комунікаційної системи об’єктів критичної інфраструктури; наявність джерел кіберзагроз, їх можливості, тип, вид, мета, мотиви, зацікавленість у здійсненні кібератак; наявність вразливостей у системах кіберзахисту, які можуть використовуватися при здійсненні кібератак; наявність чи відсутність сприятливих умов для реалізації кіберзагроз; привабливість активів, на які власне і спрямовуються кібератаки.

Таким чином, кібербезпека є невід'ємною складовою інформаційної безпеки. Водночас інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки, яка характеризує стан захищеності національних інтересів в інформаційній сфері від зовнішніх та внутрішніх загроз і являє собою сукупність інформаційно-психологічної та інформаційно-технологічної безпеки держави.

Література

1. Зелена книга з питань захисту критичної інфраструктури в Україні. Аналітична доповідь. – К.: НІСД, 2015. – 35 с.

2. Інституційне забезпечення державної комунікативної політики: досвід країн Європи. Аналітична доповідь. – К.: НІСД, 2014. – 40 с.

Козюра В.Д.
к.т.н., доцент,
Решетніков О.В.
Національна академія Служби безпеки України

УПРАВЛІННЯ ЖИТТЄВИМ ЦИКЛОМ КІБЕРАТАКИ

Як визначає Oxford Dictionaries «парадигма – це певний набір концепцій або шаблонів мислення, включаючи теорії, методи дослідження, постулати і стандарти, відповідно до яких здійснюються наступні побудови, узагальнення та експерименти».

Відносно забезпечення кібербезпеки сучасних інформаційно-телекомунікаційних систем, що експлуатуються в організаціях критичної інфраструктури України, то на думку провідних західних фахівців в сфері кіберзахисту інвестувати слід в першу чергу в управління життєвим циклом кіберзагроз, що дозволить організаціям адекватно реагувати на кібератаки в залежності від стадії їх розвитку. У звіті найбільшої американської IT-компанії Verizon Communications вказується, що з усіх кібератак, здійснених в 2015 р, 84% залишили докази в журналах, які автоматично ведуться на робочих станціях і серверах. А це означає, що за допомогою відповідних програмних інструментів захисту та аналітичної роботи фахівців кібератаки можна було нейтралізувати на досить ранніх стадіях розвитку і запобігти нанесеним збиткам.

До основних стадій життєвого циклу кібератаки відносяться:

1) зовнішня розвідка об'єкта кібератаки;
2) сканування вразливостей об'єкта кібератаки;
3) доступ на об'єкт кібератаки і підвищення привілеїв порушника;
4) проникнення в систему і організація витоку інформації;
5) «тилове забезпечення» тривалого перебування на об'єкті кібератаки;
6) «штурм» - виведення з ладу апаратних засобів об'єкта кібератаки;
7) обфускація (маскування) ворожої діяльності.

Виходячи з парадигми необхідності управління життєвим циклом кібератак, можна визначити такі етапи цього процесу.

Перший етап – збір даних комп'ютерної криміналістики. До того моменту, як загроза проявить весь свій функціонал, деякі її прояви можна спостерігати в IT-середовищі. Загрози можуть реалізовуватися через такі домени IT-інфраструктури: User Domain, Workstation Domain, LAN Domain, LAN-to-WAN Domain, Remote Access Domain, WAN Domain і System / Application Domain. Тому, чим більше IT-інфраструктури організація спостерігає, тим більше загроз вона може виявити.

На даній стадії слід звернути увагу на наступні моменти:

– організація повинна зібрати дані про ефективність моніторингу безпеки та всіх тривожних сигналах;

– збір log-журналів і машинних даних (це може забезпечити глибоке уявлення про те, що фактично відбувається в мережі, що захищається, на рівні окремого користувача або застосування);

– збір даних низькорівневих сенсорів (такі сенсори, як сенсори мережі і кінцевих точок, збирають більш низкорівневу інформацію, яка стане корисною, якщо журнали недоступні).

Другий етап – виявлення загроз, реалізується після того, як організація встановлює процедуру виявлення кібератак, завдяки чому атаки можна виявити досить рано. Це досягається двома способами:

1) пошукова аналітика, коли IT-фахівці організації переглядають звіти і виявляють будь-які відомі або зареєстровані виключення з мережевих і антивірусних засобів безпеки;

2) машинна аналітика, виконувана виключно апаратно-програмними засобами. Розвиток в останні роки теорії і практики штучного інтелекту показує, що програмне забезпечення має можливості машинного навчання, а це, в свою чергу, дозволяє автономне сканувати великі обсяги даних і надавати фахівцям короткі і наочні результати для подальшого аналізу. Машинне навчання дозволяє спростити процес виявлення загроз, оскільки воно автоматизовано і постійно вивчає нові загрози самостійно.

Третій етап – класифікація (розпізнавання) виявлених загроз, які оцінюються з метою виявлення їх потенційної небезпеки, терміновості вирішення і способів їх нейтралізації. Ця стадія чутлива до часу, оскільки виявлена загроза може реалізуватися швидше, ніж очікувалося.

Тут вже штучний інтелект не завжди допомагає і вимагає великих затрат ручної праці і часу. На цьому етапі помилкові спрацьовування є серйозною проблемою, і їх необхідно ідентифікувати, щоб організація не використовувала ресурси по відношенню до неіснуючих загроз. Неефективне розпізнавання може привести до пропуску справжніх загроз і включенню помилкових. Таким чином, реальні загрози можуть бути пропущеними.

Четвертий етап – розслідування інцидентів. Загрози, віднесені до категорії актуальних, повинні бути повністю розслідувані, щоб визначити, чи є вони причиною інциденту в області кібербезпеки.

Цей етап вимагає постійного доступу до даних комп'ютерної криміналістики і відомостям про багато загрози. В основному він автоматизований, і це спрощує процес пошуку певної загрози серед мільйонів відомих. На цьому етапі також розглядається будь-який потенційний збиток, який загроза могла заподіяти організації, перш ніж була ідентифікована засобами безпеки.

П'ятий етап – нейтралізація кібератаки. Тут застосовуються відповідні заходи для усунення або зменшення впливу виявленої загрози на організацію. Організації прагнуть досягти цього етапу якомога швидше, оскільки загрози можуть завдати непоправної шкоди за короткий період часу.

Цей процес автоматизований, щоб забезпечити більш високу пропускну здатність видалення загроз, а також полегшити обмін інформацією та співробітництво між відділами в організації.

Шостий етап - відновлення, яке наступає тільки після того, як організація переконається, що виявлені загрози були нейтралізовані і будь-які ризики, з якими вона стикається, знаходяться під контролем. Мета цього етапу – повернути організацію в стан, в якому вона перебувала до атаки. Відновлення сильно залежить від типу програмного забезпечення або служби, які виявилися пошкодженими. Зміни, які могли бути внесені під час інциденту з кібератакою або

під час реагування, потрібно відстежувати. Ці два процеси можуть призвести до небажаних конфігурацій або дій, вжитих для того, щоб або поставити під загрозу систему, або запобігти її подальшому пошкодженню. Вкрай важливо, щоб системи були приведені саме в той стан, в якому вони перебували до моменту здійснення атаки. Існують засоби автоматичного відновлення, які можуть автоматично повертати системи в стан, в якому була зроблена резервна копія. Слід діяти обачно, щоб гарантувати відсутність старих або появу нових вразливостей для порушників.

Лашин Я.О.
н.с.,
Кульчицький О.С.
н.с.,
Сівоха І.М.
н.с.,
Національний університет оборони України імені Івана Черняховського

ПРОТИДІЯ КІБЕРНЕТИЧНИМ АТАКАМ рф НА ІНФОРМАЦІЙНІ РЕСУРСИ УКРАЇНИ

У сучасному світі інформаційні технології відіграють дуже важливу роль у різних сферах життя. Інформаційні ресурси стали невід'ємною частиною життя суспільства, вони забезпечують швидкий доступ до інформації, підвищують продуктивність та зручність взаємодії між людьми та організаціями. Проте зі зростанням значущості інформаційних технологій з'являється загроза кібернетичних атак, які можуть завдати значних шкідливих наслідків. Особливо гостро ця проблема стоїть перед Україною, яка є об'єктом кібернетичних атак з боку російської федерації (рф).

Кібернетичні загрози для України є однією з найбільш актуальних проблем. Зростання кількості кіберінцидентів та кібератак спрямованих проти України, може говорити про те, що рф активно використовує цей метод для ведення війни проти України в кіберпросторі. За висновком експертів, кібернетичні атаки рф спрямовані на наступні об'єкти:

- господарсько-промислові об'єкти;
- системи зв'язку;
- банки та фінансові установи;
- системи управління критичними інфраструктурними об'єктами;
- державні установи.

Кібернетичні атаки рф можуть мати різні форми та мету. Найбільш поширеними формами є:

– фішингові атаки;
– атаки на веб-сайти та веб-додатки;
– DDoS-атаки;
– атаки на мережі та інформаційні системи;
– крадіжка даних та кібершпигунство.

Крім того, рф може використовувати кібернетичні атаки для дестабілізації ситуації в Україні та створення хаосу.

Заходи протидії кібернетичним атакам рф на інформаційні ресурси України.

Для ефективної протидії кібернетичним атакам рф на інформаційні ресурси України необхідно вживати наступні заходи:

1. Підвищення кваліфікації фахівців з кібербезпеки

Для ефективної протидії кібернетичним загрозам необхідно підвищувати кваліфікацію фахівців з кібербезпеки. Необхідно навчати фахівців відповідальної поведінки в мережі Інтернет та застосуванню сучасних технологій кібербезпеки.

2. Зміцнення співпраці з іншими країнами

Україна повинна співпрацювати з іншими країнами в боротьбі з кібернетичними загрозами. Необхідно обмінюватися досвідом та інформацією з іншими країнами щодо кібербезпеки та спільно працювати над покращенням захисту в кіберпросторі. З урахуванням того, що кібербезпека є міжнародною проблемою, важливо підтримувати міжнародну співпрацю в цій сфері. Україна повинна підтримувати співпрацю з міжнародними організаціями, такими як НАТО, ОБСЄ, ЄС та іншими, з метою обміну досвідом та розв’язанню проблем кібербезпеки. Також важливо розробити спільні стандарти та протоколи з міжнародними партнерами, які дозволять створити єдиний кіберпростір та сприяти підвищенню ефективності боротьби з кіберзагрозами.

3. Створення державної стратегії кібербезпеки

Необхідно створити державну стратегію кібербезпеки, яка передбачатиме заходи щодо захисту інформаційних ресурсів та кіберпростору країни. Важливо, щоб ця стратегія була розроблена на національному рівні та враховувала специфіку країни та її інформаційної інфраструктури.

4. Посилення законодавства

Необхідно посилити законодавство у сфері кібербезпеки, щоб забезпечити ефективний захист інформаційних ресурсів країни від кібератак. Важливо встановити відповідальність за кіберзлочини та передбачити належну відповідальність злочинців.

5. Підвищення рівня громадської обізнаності

Оскільки кібербезпека є проблемою не тільки для державних органів, а й для приватних осіб, важливо підвищити рівень громадської обізнаності щодо кібербезпеки та захисту від кібератак. Необхідно проводити кампанії з освіти громадян про загрози, які існують в кіберпросторі, а також про заходи, які можна вжити для їх запобігання.

6. Зміцнення кібербезпеки

Зміцнення кібербезпеки є кінцевим кроком у боротьбі з кібернетичними загрозами. Україна повинна розвивати та вдосконалювати свої системи захисту від кіберзагроз та створювати нові. Необхідно забезпечити захист критично важливих інфраструктурних об'єктів, які мають важливе значення для функціонування держави.

Кібербезпека є важливим питанням для держави в умовах війни та постійно зростаючими кіберзагрозами. Україна, як і інші країни, повинна приділяти значну увагу захисту своїх інформаційних ресурсів від кібератак. Для досягнення цієї мети необхідно вживати комплексних заходів, таких як розробка та впровадження захисних технологій, співпраця з іншими країнами, створення державної стратегії кібербезпеки, посилення законодавства та підвищення рівня громадської обізнаності. Україна має підтримувати тісні контакти з іншими країнами, обмінюватися досвідом та інформацією про кібербезпеку, а також спільно розробляти та впроваджувати заходи протидії кібератакам.

Крім того, важливо зазначити, що кібербезпека є динамічним поняттям, яке постійно розвивається. Тому Україна повинна відстежувати нові тенденції та інновації у сфері кібербезпеки та постійно вдосконалювати свої засоби захисту від кібератак. Лише за умови виконання цих заходів Україна може захистити свої інформаційні ресурси від кіберзагроз та забезпечити стабільну роботу інформаційних систем в умовах війни.

Література

1. Баловсяк Н. Чи має Росія кібернетичну суперзброю? - Український тиждень. Український тиждень. URL: https://tyzhden.ua/chy-maie-rosiia-kibernetychnu-superzbroiu/ (дата звернення: 20.03.2023).

2. Петровський Д. Росія посилить свої кібератаки на Україну та її союзників: названо час. Новини України - останні новини України сьогодні - УНІАН. URL: https://www.unian.ua/science/rosiya-posilit-svoji-kiberataki-na-ukrajinu-ta-jiji-soyuznikiv-microsoft-12067638.html (дата звернення: 20.03.2023).

3. Поляковська Т. Росія здійснила масштабну кібератаку на українські веб-ресурси. Новини України - останні новини України сьогодні - УНІАН. URL: https://www.unian.ua/techno/rosiya-zdiysnila-masshtabnu-kiberataku-na-ukrajinski-veb-resursi-12156906.html (дата звернення: 20.03.2023).

4. Interfax-Ukraine. Низка українських інформаційних ресурсів зазнала кібератаки - Держспецзв'язку. Інтерфакс-Україна. URL: https://interfax.com.ua/news/telecom/893494.html (дата звернення: 20.03.2023).

5. Ukrinform. На низку державних ресурсів відбувається кібератака. Укрінформ - актуальні новини України та світу. URL: https://www.ukrinform.ua/rubric-technology/3683610-na-nizku-derzavnih-resursiv-vidbuvaetsa-kiberataka.html (дата звернення: 20.03.2023).

6. Ukrinform. Росія здійснює на Україну понад 10 кібератак за добу – СБУ. Укрінформ - актуальні новини України та світу. URL: https://www.ukrinform.ua/rubric-ato/3676108-rosia-zdijsnue-na-ukrainu-ponad-10-kiberatak-za-dobu-sbu.html (дата звернення: 20.03.2023).

7. Ukrinform. Рф здійснює кібератаку на українську судову систему. Укрінформ - актуальні новини України та світу. URL: https://www.ukrinform.ua/rubric-technology/3683198-rf-zdijsnue-kiberataku-na-ukrainsku-sudovu-sistemu.html (дата звернення: 20.03.2023).

Макаров Я.І.
Національний університет оборони України імені Івана Черняховського

АНАЛІЗ ТЕРМІНОЛОГІЧНИХ ПІДХОДІВ ЩОДО ВИЗНАЧЕННЯ КІБЕРЗАГРОЗ ДЕРЖАВІ У ВОЄННІЙ СФЕРІ

Кібербезпека все частіше стає ефективним інструментом для досягнення мети щодо несилового контролю та управління, як об’єктами з критичною інформаційною інфраструктурою держави, що може піддатися такому впливу, так і окремо взятими громадянами, їх об’єднаннями. Вони відкривають можливості досягнення політичних цілей, змін легітимних урядів, а також здійснення деструктивних змін в усіх сферах життєдіяльності суспільства і держави (економічній, енергетичній, духовній тощо), взяття під контроль і навіть поневолення цілих народів і країн практично без застосування військової сили в класичному її розумінні [1].

Взагалі, на сьогодні, практично всі більш-менш розвинені держави вже зіткнулися з кіберзагрозами та необхідністю формувати системи кібербезпеки та кібероборони. Тенденція перенесення дій у воєнних конфліктах до нового бойового середовища – кіберпростору ще більше загострило ці проблеми. Це спонукало провідні країни світу до запровадження першочергових заходів зі створення спеціальних структур і підрозділів для дій у кіберпросторі.

Спираючись на світовий досвід можна стверджувати, що процес забезпечення кібербезпеки, перш за все, передбачає протидію деструктивним впливам у цій сфері. Для цього потребує створення й організації потужна підсистема кіберзахисту. Не менш важливими складовими системи забезпечення кібербезпеки мають виступати і підсистеми кіберрозвідки та кібервпливу.

Кіберзагроза – явище, дія, умова, фактор, що становить небезпеку для інформації, інфраструктури та суб’єктів управління, а також порядку управління ними, порушення властивостей одного або декількох з яких може призвести до порушення процесу управління [2].

У сформульованому вище відомому визначенні кіберзагрози не охоплюються усі аспекти досліджуваного явища. Також у ньому не розкривається сутність самого поняття загрози, а тому визначення кіберзагрози потребує подальшого уточнення. Так, при формулюванні нового й більш повного визначення обов'язково слід враховувати те, що кібернетичні загрози впливають на:

процеси управління в системі державного управління та її інституцій шляхом здійснення цілеспрямованих деструктивних кібернетичних впливів на технічні системи, які використовуються для його реалізації та соціум;

ступінь готовності населення й особового складу військових формувань до оборони держави за умов погіршення іміджу оборонної сфери держави та її представників при цілеспрямованому інформаційно-психологічного впливі на вказані категорії;

процеси знецінення національних культурних цінностей і традицій, людської й національної гідності шляхом поширення в засобах масової інформації та мережі Інтернет невластивих тій чи іншій державі культурних цінностей, культу насильства, жорстокості, порнографії;

темпи послаблення суспільно-політичної, міжетнічної та міжконфесійної єдності суспільства;

процеси розголошення інформації, яка становить державну та іншу передбачену законодавством таємницю, а також конфіденційної інформації, що є власністю приватного сектору економіки;

зародження у суспільній та в індивідуальній свідомості населення різноманітних негативних уявлень, за рахунок застосування спеціальних засобів кібернетичного впливу;

темпи зростання пропаганди сепаратизму за етнічною, мовною, релігійною та іншими ознаками за рахунок використання засобів масової інформації, а також Інтернет.

При цьому також слід враховувати те, що перелік об'єктів та суб'єктів впливу кіберзагроз постійно змінюється й доповнюється, оскільки в сучасних умовах досить динамічно змінюються форми та способи протиборства, стрімко модернізуються сили і засоби досягнення цілей, швидко розвиваються, вдосконалюються і впроваджуються високі технології в усіх сферах життєдіяльності людства. Слід зауважити на тому, що наведені вище кібернетичні загрози відносяться до загроз кібербезпеці у соціотехнічній сфері, оскільки переважна їх більшість націлена на соціум або його окремі складові, а також на технічні засоби управління та комунікацій. Це пояснюється тим, що на сучасному етапі розвитку інформаційних технологій чітко виокремити суто технічну або суто соціальну систему досить проблематично, адже будь-яка соціальна система для свого функціонування використовує технічні засоби комунікацій, обробки інформації тощо, а будь-яка технічна – тією чи іншою мірою контролюється та управляється соціумом.

Таким чином, аналіз підходів щодо визначення кіберзагроз державі у воєнній сфері дозволяє зробити висновок, що в цілому визначення даної категорії не суперечать одне одному та за своїм змістом є достатньо схожим одне з одним. Однак для відображення сутності досліджуваної категорії з огляду на предметну галузь, доцільно скористатися тлумаченням де стверджується, що "загроза інтересам безпеки – це готовність (наміри та можливість) одного із суб'єктів політики завдати шкоду життєво важливим інтересам іншому суб'єкту".

Література

1. Ризики та можливості примирення в українському суспільстві. Аналітична доповідь. – К.: НІСД, 2017. – 22 с.

2. Ризикогенні фактори соціальної напруженості в Україні. Аналітична доповідь. – К.: НІСД, 2017. – 14 с.

Малейчик М.П.
Національна академія СБ України

ПРОБЛЕМИ ПРОТИДІЇ КІБЕРНЕТИЧНИМ АТАКАМ рф НА ОБ'ЄКТИ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Україна вже зіткнулася з кількома серйозними кібернетичними атаками з боку рф на об'єкти критичної інформаційної інфраструктури, такі як енергетика, транспорт та фінансова система. Щоб забезпечити ефективну протидію таким атакам, необхідно вжити наступних заходів:

Підвищити кваліфікацію та компетентність кадрів у сфері кібербезпеки. Необхідно забезпечити постійну підготовку фахівців з кібербезпеки та забезпечити їхнє постійне навчання та вдосконалення навичок, щоб вони могли ефективно протидіяти кібернетичним атакам.

Розробити та впровадити систему моніторингу та виявлення кібератак на об'єкти критичної інформаційної інфраструктури. Необхідно забезпечити постійний моніторинг системи та вчасне виявлення кібератак, щоб забезпечити швидку реакцію на них.

Забезпечити захист критично важливих інформаційних систем від кібернетичних атак. Необхідно вжити заходів забезпечення кібербезпеки, таких як шифрування, аутентифікація, контроль доступу та захист від вірусів та шкідливих програм.

Встановити процедури реагування на кібератаки та реалізувати плани дій у випадку їхнього виникнення. Необхідно розробити та впровадити плани дій, щоб ефективно реагувати на кібератаки та забезпечити швидке відновлення роботи інформаційних систем.

Кібернетичні атаки на об'єкти критичної інформаційної інфраструктури є серйозною загрозою для національної безпеки і стабільності країни. Російська Федерація відома своїми спробами провести кібернетичні атаки на інші держави, включаючи Україну та інші країни Європи. На жаль, немає ніякого універсального рішення для протидії кібернетичним атакам, але існують деякі кроки, які можуть бути вжиті для зменшення ризиків.

Одним з головних кроків для протидії кібернетичним атакам є забезпечення належного рівня кібербезпеки в об'єктах критичної інформаційної інфраструктури. Це означає, що організації мають приділяти особливу увагу захисту своєї мережевої інфраструктури від кібернетичних загроз. Для цього можна використовувати різні технології, такі як мережеві брандмауери, інтрудер-детектори та інші заходи.

Також важливо забезпечити належний рівень кібербезпеки в галузях, які забезпечують критичну інфраструктуру, таких як енергетика, транспорт, комунікації тощо. Це означає, що організації мають працювати з правительством та регуляторами, щоб встановити стандарти кібербезпеки та забезпечити їх дотримання.

Протидія кібернетичним атакам рф на об'єкти критичної інформаційної інфраструктури є важливим завданням для багатьох країн світу. Основні проблеми, які потрібно вирішувати для ефективної протидії кібернетичним атакам, включають наступні:

Виявлення інцидентів: Однією з головних проблем у боротьбі з кібернетичними атаками є швидкість виявлення інцидентів. Чим швидше виявляється атака, тим швидше можуть бути прийняті заходи для її ліквідації.

Розробка відповідних заходів безпеки: Для ефективного захисту критичної інформаційної інфраструктури потрібно розробити відповідні заходи безпеки. Це може включати в себе налагодження захисту від різних видів кібератак, регулярні оновлення програмного забезпечення та апаратного забезпечення, а також створення запобіжників та обмежень доступу до інформації.

Підвищення кваліфікації персоналу: Важливим фактором є кваліфікація персоналу, який займається захистом критичної інформаційної інфраструктури. Вони повинні бути готові реагувати на кібернетичні загрози і знати, як взаємодіяти зі спеціалізованими службами безпеки та правоохоронними органами.

Міжнародне співробітництво: Важливо встановити міжнародні зв'язки і співробітництво між країнами для ефективного боротьби з кібернетичними загрозами.

Отже, протидія кібернетичним атакам рф на об'єкти критичної інформаційної інфраструктури вимагає вирішення кількох важливих проблем, таких як виявлення інцидентів, розробка заходів безпеки, підвищення кваліфікації персоналу та міжнародне співробітництво. Вирішення цих проблем може сприяти

ефективному захисту критичної інформаційної інфраструктури від кібернетичних атак.

Мельник Д.С.
к.ю.н.,доцент, п.н.с.,
Національна академія СБ України

СУЧАСНІ КІБЕРЗАГРОЗИ БЕЗПЕЦІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ В УМОВАХ ВІЙСЬКОВОЇ АГРЕСІЇ рф

Акції кібервпливу в сучасних умовах стали невід'ємною складовою гібридної агресії рф проти України. Наша країна вже тривалий час є полігоном для хакерських експериментів російських спецслужб, диверсій і терактів проти об'єктів вітчизняної критичної інфраструктури (далі – ОКІ). Шкідливі вірусні програми («Bad Rabbit», «Black Energy», «Locky», «Petya», «Not Petya», «WannaCry» та ін.) спершу були апробовані в Україні, а потім застосовані проти критичної інфраструктури країн Заходу.

Україна упродовж 2014-2022 років зазнала безпрецедентної кількості кібератак на інформаційні ресурси ОКІ – підприємств життєзабезпечення, енергетичної, транспортної сфери, державних фінансових установ, органів, які гарантують безпеку, оборону, захист від надзвичайних ситуацій тощо. Безпосереднього кібервпливу зазнали інформаційні системи та мережі на ОКІ.

Перша визнана успішною кібератака на енергетичну систему України з виведенням її із ладу сталася ще у грудні 2015 року, коли російським хакерам із використанням троянської програми «BlackEnergy» вдалося атакувати комп'ютерні системи управління низки енергопостачальних компаній [1].

Чергова кібератака сталась вночі з 16 на 17 грудня 2016 року. На понад годину була виведена з ладу підстанція «Північна» енергокомпанії «Укренерго», без струму залишились споживачі північної частини правого берега м. Києва та низки районів області [2]. Упродовж травня – липня 2017 року комп'ютерні системи КМ України, «Укренерго», «Київенерго», операторів зв'язку, «Укрзалізниці», аеропорта «Бориспіль», низки державних фінустанов та комерційних структур в Україні зазнали масованої атаки вірусу «WannaCry» та мережевого черв'яка «Petya» [3].

Вже у січні 2018 року хакери зламали сервер Головного теруправління юстиції в Одеській області, а у квітні - сайт Міненерговуглепрому України. У квітні – травні 2019 року правоохоронцями фіксувалися кібератаки з рф на сервер ЦВК України. В листопаді 2019 року командою «CERT-UA» були заблоковані 11 DDoS-атак на веб-ресурси Офісу Президента України.

На початку травня 2020 року командою «CERT-UA» були заблоковані 9 DDoS-атак на веб-ресурси Офісу Президента України. У серпні 2020 року НКЦК при РНБО України повідомив про підготовку хакерським угрупованням «Armageddon» кібератаки на інформресурси органів влади та ОКІ напередодні Дня незалежності України. У вересні 2020 року хакери зламали сайт НПУ.

Надалі правоохоронці в листопаді 2021 року викрили протиправну діяльність хакерського угруповування «Armagedon», учасники якого з 2014 року здійснили понад 5 тис. кібератак на державні інформресурси України. Вони використовували власні вірусні програми і намагалися «заразити» понад 1,5 тис. урядових комп'ютерних систем, встановити контроль над ОКІ [4].

У минулому році вищевказані прояви продовжили мати місце та ще більше актуалізувалися перед початком повномасштабної військової агресії рф проти України. 15.02.2022 лютого хакери здійснили потужну DDOS-атаку на веб-сайти органів державної влади, державних банківських установ та портал «Дія». Експерти з питань цифрової трансформації визначили дестабілізацію та сіяння хаосу всередині України в якості мети атаки, яку було здійснено з різних країн [5].

З початку повномасштабного військового вторгнення 24.02.2022 рф посилила здійснення гібридної агресії проти України у кіберпросторі, яка включає реалізацію концепції інформаційного протиборства, базованої на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій. Протягом минулого року експертами неодноразово фіксувалися системні кібератаки на інформаційні ресурси ОКІ та органів державної влади й військового управління, що часто були синхронізовані з ракетно-бомбовими ударами ЗС рф й переслідували єдину мету – дестабілізацію та виведення з ладу військової та цивільної критичної інфраструктури України.

За останні роки в Україні не були зафіксовані атаки кібертерористів

безпосередньо на ОКІ. Однак електронні платіжні системи та криптовалюти активно використовуються для забезпечення функціонування каналів фінансування терористичної, диверсійної та сепаратистської діяльності в Україні та поза її межами [6].

Висока анонімність та віддаленість доступу кібератак сприяє їх широкому застосуванню проти України. Технічний рівень реалізації кібератак на ОКІ постійно зростає, вдосконалюються і розробляються нові інструменти й механізми вчинення. Набуває глобального масштабу використання кіберпростору терористичними організаціями. Міжнародні хакерські угруповання все частіше залучаються іноземними спецслужбами до реалізації акцій кібервпливу.

Необхідність захисту ОКІ в сучасних умовах зумовлює низка серйозних загроз національній безпеці, перелік яких визначений у Стратегії національної безпеки України, затвердженій Указом Президента України від 14.09.2020 № 392/2020, та доповнюється положеннями Стратегії кібербезпеки України, затвердженої Указом Президента України від 26.08.2021 № 447/2021. Серед них:

продовження рф гібридної війни проти України шляхом системного застосування воєнних, кібернетичних, інформаційно-психологічних, політичних і економічних засобів; продовження спецслужбами іноземних держав, насамперед рф, розвідувально-підривної діяльності проти України у кіберпросторі шляхом вчинення тривалих, складних і прихованих кібератак; комп‘ютерний тероризм та комп‘ютерна злочинність; посилення загроз для критичної інфраструктури, пов‘язаних з погіршенням її технічного стану, відсутністю інвестицій в її оновлення та розвиток, несанкціонованим втручанням у її функціонування, триваючими бойовими діями, тимчасовою окупацією частини території України; кібератаки рф на інформаційно-комунікаційні системи державних органів України та ОКІ; використання ресурсів ОКІ для фінансування тероризму, сепаратизму та розповсюдження зброї масового знищення тощо.

В умовах збройної агресії сусідньої держави та тривалого ведення нею

гібридної війни проти України наявна в державі ситуація вимагає перегляду засад діяльності всієї системи забезпечення національної безпеки України, спрямованої на захист її критичної інфраструктури. Відповідно потребують перегляду й засади забезпечення безпеки критичної інформаційної інфраструктури України.

Зокрема, перед уповноваженими державними органами постають нові завдання: протидія терористичним та іншим загрозам національній критичній інфраструктурі; організація належного захисту цієї інфраструктури, забезпечення стійкості функціонування її систем і елементів, запобігання вчиненню терактів і диверсій, у т.ч. кібернетичних, виникненню надзвичайних ситуацій на ОКІ, припинення іншого незаконного втручання у діяльність систем життєзабезпечення; упередження, стримування і недопущення настання тяжких наслідків тощо.

Разом з тим, на переконання фахівців, подальшу діяльність за цим напрямом необхідно зосереджувати не лише на постійному протистоянні противнику, але й створювати відповідні умови та адміністративні режими, за яких його підривні дії будуть неефективними.

Важливою передумовою такого підходу до організації дієвої системи забезпечення національної безпеки та захисту національних інтересів, яка зможе забезпечити ефективне функціонування системи захисту критичної інфраструктури, є запровадження в державі та постійне удосконалення контррозвідувального режиму, передбаченого Концепцією забезпечення контррозвідувального режиму в Україні, затвердженої Указом Президента України від 06.10.2017 № 310/2017.

Також потребує неухильного виконання Концепція створення державної системи захисту критичної інфраструктури України, схвалена розпорядженням КМ України 06.12.2017 № 1009 р., спрямована на створення в державі системи управління безпекою критичної інфраструктури та забезпечення стабільного

функціонування в рамках забезпечення національної системи стійкості (Указ Президента України від 27.09.2021 № 479/2021), і місця кожного державного органу у системі виявлення і нейтралізації загроз об'єктам, що мають стратегічне значення для безпеки держави.

Окрім цього, необхідно законодавчо визначити поняття кібертероризму та прийняти національну Стратегію захисту критичної інфраструктури, реалізація яких дозволить створити в державі ефективну систему захисту ОКІ, координації та управління силами і засобами забезпечення її безпеки.

З урахуванням актуальних загроз і сучасних методів ведення гібридної війни проти України актуальним є посилення відповідальності за вчинення кібератак, диверсій та інших суміжних з ними протиправних дій на шкоду національній критичній інфраструктурі. З цією метою необхідно опрацювати питання щодо необхідності внесення відповідних змін до КК України.

Актуальними є організаційні й технічні заходи захисту інформаційних ресурсів ОКІ: поширення серед органів державної влади та ОКІ індикаторів актуальних кіберзагроз, рекомендацій та інструментів реагування із використанням платформи MISP-UA; забезпечення цілодобового моніторингу стану мережевої інфраструктури державних органів, ОКІ шляхом їх підключення до системи управління подіями інформаційної безпеки SIEM; розгортання ефективної системи моніторингу, здатної виявляти шкідливу активність, яка не детектується антивірусним програмним забезпеченням, на пристроях користувачів інформаційних ресурсів державних органів та ОКІ.

Література

1. Міненерговугілля оприлюднило звіт про російську кібератаку на обленерго. URL: http://mpe.kmu.gov.ua/minugol/control/uk/publish/article?art_id=245086886&cat.

2. В Укренерго пояснили масштабний збій в енергосистемі під Києвом кібератаками URL: http://economics.unian.ua/energetics/1689781-v-ukrenergo-poyasnili-masshtabniyzbiy-v- energosistemi-pid-kievom-kiber-atakami.html. (дата звернення:10.03.2018).

3. Ще один фронт. Як Україна відповідає на виклики, що постали у віртуальному просторі. URL: http://tyzhden.ua/publication/183407. (дата звернення:10.03.2018).

4. В Україні викрили хакерів ФСБ, які здійснили понад 5 тисяч кібератак на держоргани. URL: https://ord-ua.com/2021/11/04/v-ukraini-vikrili-hakeriv-fsb-jaki-zdijsnili-ponad-5-tisjach-kiberatak-na-derzhorgani/. (дата звернення:05.12.2021).

5. Демедюк С. Державна система кіберзахисту спрацювала на «відмінно», реагуючи на останню кібератаку, яка була здійснена стосовно державних вебресурсів та банківської системи. URL: https://www.rnbo.gov.ua/ua/Diialnist/5263.html. (дата звернення:12.03.2022).

6. В СБУ назвали перевод криптовалют основным механизмом финансирования ОРДЛО. URL: https://antikor.com.ua/articles/220214-vordlo. (дата звернення:10.03.2018).

Мєшков В.І.
аспірант,
Корнієнко В.І.
д.т.н., професор,
Національний технічний університет «Дніпровська політехніка»

РОЗРОБКА ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ ІНТЕЛЕКТУАЛЬНОГО МОНІТОРИНГУ ТРАФІКУ КОМП'ЮТЕРНОЇ МЕРЕЖІ ДЛЯ СИСТЕМ ВИЯВЛЕННЯ АТАК

Зі зростанням кількості підключених до мережі пристроїв та об'єму передаваних по мережі даних, зростає й ризик виникнення різних загроз для безпеки мережі. Атаки на комп'ютерні мережі (КМ) можуть завдати значної шкоди, включаючи втрату даних, недоступність сервісів та інші наслідки. У зв'язку з цим, важливо мати ефективну систему виявлення та запобігання атакам на мережу.

Інтелектуальний моніторинг трафіку (ІМТ) КМ є одним з ефективних засобів виявлення потенційних загроз для безпеки мережі. Він дозволяє виявляти небезпечний трафік та сприяє вчасному реагуванню на можливі атаки.

Інформаційна технологія ІМТ КМ для систем виявлення атак (СВА) – це комплексний підхід до моніторингу трафіку в комп'ютерних мережах з метою виявлення потенційно шкідливої активності. Ця технологія використовується для підвищення безпеки мережі, виявлення атак, ідентифікації порушників та забезпечення безпеки даних.

СВА можуть використовувати різні методи моніторингу, такі як сигнатурний аналіз, аналіз використання портів та протоколів, поведінковий аналіз та інші. Інформаційна технологія ІМТ КМ може використовувати ці методи, а також машинне навчання, штучний інтелект та інші технології для автоматичного виявлення аномалій в трафіку.

Застосування цієї технології може допомогти забезпечити безпеку мережі, зменшити ризик витоку конфіденційної інформації та зменшити кількість часу, потрібного для виявлення і реагування на атаки. Однак важливо пам'ятати, що жодна система не є повністю безпечною, тому інформаційна технологія ІМТ КМ повинна бути використана як частина комплексної стратегії забезпечення безпеки мережі.

До алгоритму інформаційної технології ІМТ КМ для СВА можуть бути

включені наступні кроки:

1. Зібрати дані про трафік мережі: отримати доступ до мережевого трафіку і зберігати дані про нього в реальному часі.

2. Обробити отримані дані: виконати аналіз отриманого трафіку і виокремити ключові параметри, такі як IP-адреса, порти, протоколи, розмір пакетів тощо.

3. Використати методи виявлення аномалій: використовуючи методи машинного навчання, статистичні методи та інші алгоритми, провести аналіз виокремлених параметрів трафіку для виявлення аномальної поведінки.

4. Підтвердити аномалії: для підтвердження аномальної поведінки провести додатковий аналіз, щоб переконатися, що виявлені аномалії є потенційно шкідливими.

5. Прийняти рішення про заходи безпеки: на основі результатів аналізу прийняти рішення про вжиття заходів для захисту мережі, наприклад, заблокувати доступ для аномальних джерел, повідомити про це відповідні служби безпеки тощо.

6. Записати результати: зберегти результати аналізу для подальшого використання та аудиту безпеки мережі.

Це базовий алгоритм, інформаційна технологія ІМТ КМ може включати додаткові кроки для забезпечення безпеки мережі. Важливо звернути увагу на те, що цей алгоритм може бути адаптований до потреб конкретної мережі і СВА.

ІМТ КМ для СВА може використовувати різні методи і технології, щоб ефективно виявляти потенційні загрози безпеці мережі:

– машинне навчання: використання алгоритмів машинного навчання дозволяє створити моделі, які можуть виявляти аномальні поведінки та навіть передбачати майбутні атаки. Це дає можливість швидко реагувати на можливі загрози та забезпечити безпеку мережі.

– аналіз потоку даних: аналіз потоку даних дає змогу проводити моніторинг трафіку в режимі реального часу та реагувати на потенційні атаки з мінімальним часом затримки. Цей метод дає можливість виявляти аномалії, які не виявляються іншими методами.

– аналіз поведінки: використання методів аналізу поведінки дає змогу виявляти аномальні патерни поведінки в мережі. Наприклад, атаки, які зазвичай виконуються крок за кроком, можуть бути виявлені, якщо аналізувати потік даних на основі цих патернів.

– система виявлення Інтранет-атак: ця система виявляє внутрішні атаки на мережу, такі як атаки від зловмисників з фізичним доступом до комп’ютерів у мережі. Система виконує моніторинг трафіку в мережі та виявляє аномальну активність, яка може свідчити про внутрішню атаку.

– аналіз мережевого трафіку з використанням інструментів: існує багато різних інструментів, які можуть допомогти в аналізі мережевого трафіку. Наприклад, Wireshark, tcpdump та інші. Ці інструменти дають змогу виконувати

моніторинг трафіку та відстежувати пакети, які можуть свідчити про можливі загрози безпеці мережі.

– IDS системи: IDS використовуються для моніторингу мережевої активності з метою виявлення можливих загроз безпеці мережі. Ці системи використовують сигнатурний аналіз, створення правил та аналіз поведінки для виявлення загроз.

– IDS на основі машинного навчання: IDS на основі машинного навчання використовують навчання без учителя для виявлення аномальної активності в мережі. Ці системи можуть використовувати алгоритми кластеризації та зменшення розмірності даних для виявлення потенційних загроз.

– системи превентивного контролю: системи превентивного контролю використовуються для захисту мережі від потенційних атак. Ці системи включають брандмауери, IPS (системи запобігання вторгненням) та інші інструменти, які дозволяють контролювати трафік в мережі та блокувати потенційні загрози.

Ці методи можуть використовуватися окремо або у поєднанні один з одним для забезпечення ефективного моніторингу та виявлення потенційних загроз безпеці мережі.

ІМТ КМ для СВА є ефективним інструментом для забезпечення безпеки мережі. Проте, цей підхід також має свої недоліки, а саме:

– великий обсяг даних: обсяг даних, який генерується в мережі, може бути дуже великим, що може ускладнити аналіз трафіку.

– помилкові спрацювання: інтелектуальні системи моніторингу можуть виявляти помилкові аномалії та вказувати на потенційні загрози, які не є такими.

– специфіка мережі: системи моніторингу можуть не підходити для деяких мереж через специфічні характеристики трафіку.

– недостатня точність: системи моніторингу можуть мати недостатню точність у виявленні аномалій, якщо зловмисники використовують нові та невідому техніку атак.

ІМТ КМ для СВА дозволяє виявляти різноманітні загрози для безпеки мережі, серед яких можна виділити наступні: атаки типу DDoS, вторгнення у мережу, віруси та шкідливі програми, фішингові атаки, крадіжка даних, викрадення облікових записів, перехоплення трафіку, спам-атаки, створення ботнету, сканування портів, виток інформації (табл.1).

Таблиця 1

Заходи ІМТ

Тип атаки	**Опис**	**Заходи ІМТ**
DDoS-атаки	Спроба перевантаження мережі для заборони доступу до неї	Виявлення великої кількості запитів з одного IP-адреси
Вторгненн	Спроба отримати	Виявлення підозрілих

Тип атаки	Опис	Заходи ІМТ
я	несанкціонований доступ до мережі	запитів та несподіваних дій
Віруси та шкідливі програми	Поширення шкідливих програм для завдання шкоди	Виявлення джерела та способу передачі шкідливого коду
Фішингові атаки	Намагання отримати конфіденційну інформацію через шахрайські методи	Виявлення підозрілих запитів та переходів на сторінки
Крадіжка даних	Спроба отримати конфіденційну інформацію шляхом викрадення даних	Виявлення підозрілих запитів та спостереження за передачею даних
Спам-атаки	Розсилка непотрібної інформації через мережу	Виявлення великої кількості повідомлень з однаковим вмістом
Створення ботнету	Створення мережі зі заражених комп'ютерів для здійснення атак	Виявлення підозрілих запитів та спостереження за використанням ресурсів
Сканування портів	Спроба знайти вразливості у мережі через сканування портів	Виявлення великої кількості запитів на різні порти мережі
Виток інформації	Спроба передати конфіденційну інформацію з мережі	Спостереження за передачею даних та виявлення підозрілих запитів

Ці заходи інтелектуального моніторингу можуть допомогти виявляти потенційні загрози та захищати мережу від атак. Однак, слід мати на увазі, що заходи протидії атакам повинні бути комплексними та орієнтованими на конкретну мережу, оскільки кожна мережа має свої особливості та потенційні вразливості.

Література

1. Шаповаленко О.Д., Кліменкова Н.А. Застосування інтелектуального аналізу даних для виявлення мережевого вторгнення. // Інформаційні технології в освіті, науці і техніці. / ЧДТУ – 2022. URL: https://er.chdtu.edu.ua/bitstream/ChSTU/4258/1/Збірник_тез_ІТОНТ_2022.pdf (дата звернення: 04.03.2023).

2. Мєшков В.І., Віролайнен В.О. Аналіз сучасних систем виявлення та запобігання вторгнень в інформаційно-телекомунікаційних системах // НТУУ «КПІ ім. І. Сікорського». – 2015. URL: https://ela.kpi.ua/bitstream/ 123456789/17609/1/meshkov.pdf. (дата звернення: 04.03.2023).

3. Корнієнко В.І, Герасіна О.В., Тимофєєв Д.С., Сафаров О.О., Ковальова Ю.В. Ідентифікація та прогнозування самоподібного трафіку інформаційно-комунікаційних мереж для систем виявлення атак. Information Technology: Computer Science, Software Engineering and Cyber Security, 1, 20–29, doi: https://doi.org/10.32782/IT/2022-1-4

4. Лазаренко С.В. Особливості функціонування систем виявлення атак на автоматизовані системи. Сучасний захист інформації. 2015. No 1. С. 33-40.

Назаренко О.Л.
Національна академія СБ України

ДО ПИТАННЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФРАСТРУКТУРИ ТА ІНФОРМАЦІЇ У КІБЕРПРОСТОРІ В КОНТЕКСТІ МІЖНАРОДНОЇ БЕЗПЕКИ

Кіберзагрози зростають і з мірою розвитку кіберпростору – з боку як державних, так і недержавних суб'єктів, зокрема, кіберзлочинців.

Наприклад, під час пандемії Covid-19, зі сплеском діджиталізації кількість шкідливих електронних повідомлень у спробі скористатися зростаючою цифровою залежністю зросла на 600% [1].

Використання комп'ютерної пропаганди у світі поширилося – зокрема, операцій кібервпливу та поширення дезінформації – як державними, так і недержавними суб'єктами [2].

Зростання геополітичної напруженості з приводу безпеки інформаційно-комунікаційних технологій (ІКТ) також спонукало держави посилити контроль над ланцюгами передачі ІКТ [3].

Кібератаки часто відбуваються нижче порогу збройного конфлікту. Наприклад, одне з найбільших в історії порушень кібербезпеки – хакерську атаку Solar Winds, яку у 2020р. зазнав уряд США, скоріше можна назвати актом шпіонажу, ніж війни. Цей випадок став результатом вразливості ланцюга постачання, яка залишила беззахисними багато компаній та урядів у всьому світі [4].

Інтернет не є абстракцією – він пов'язаний з інфраструктурою з фізичною географічною прив'язкою, хоча при цьому він нібито не обмежений кордонами. Деякі держави, зокрема Китай, запровадив поняття кіберсуверенітету [5].

Примітно, що до більш закритої системи Інтернету також рухається ЄС – цифрового та технологічного суверенітету. Так, у 2020р. ЄС з метою розширення хмарних та інформаційних послуг започаткував проект зі створення європейської хмарної системи (GAIA-X), захищеної законами ЄС про інформацію [6]. Також у 2020р. Європейський суд скасував угоду Privacy Shield про обмін даними між ЄС і США – зокрема, через занепокоєння практикою стеження американських

розвідслужб і законами ЄС про захист інформації. Маються на увазі санкції проти китайських високотехнологічних компаній (зокрема, Huawei і ByteDance, власника TikTok) і спроби переконати союзників не використовувати китайське обладнання в телекомунікаційних мережах [6].

США не бачать потреби в новому міжнародному регулюванні кібербезпеки і технічного захисту систем ІКТ, оскільки вважають, що чинне міжнародне гуманітарне право вже поширюється на кіберпростір в умовах збройного конфлікту. Натомість вони виступають за ухвалення державами добровільних і необов'язкових норм, спрямованих на забезпечення безпеки інфраструктури та інформації у мирний час. Резолюція, внесена США, призвела до створення нової групи урядових експертів – Group of Governmental Experts, (GGE) з просування відповідальної поведінки держав у кіберпросторі в контексті міжнародної безпеки (GGE on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security).

Література

1. Baig, A. The Covid-19 recovery will be digital: A plan for the first 90 days, McKinsey Digital. URL: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-covid-19-recovery-will-be-digital-a-plan-for-the-first-90-days (дата звернення 17.03.2023).

2. How Can We Stem the Tide of Digital Propaganda? URL: https://www.cigionline.org/articles/how-can-we-stem-the-tide-of-digital-propaganda/?utm_source=google_ads&utm_medium=grant&gclid=EAIaIQobChMIndPNy7qX_gIVfQWiAx29gQHcEAAYASAAEgLRvfD_BwE (дата звернення 17.03.2023).

3. Про оцінку кіберсили держав і міжнародні рейтинги. URL: https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf (дата звернення 17.03.2023).

4. Paul K. «What we know–and still don't–about the worst-ever US Government cyber-attack», The Guardian, URL: https://www.theguardian.com/technology/2020/dec/15/orion-hack-solar-winds-explained-us-treasury-commerce-department. (дата звернення 17.03.2023).

5. Graham M. «Geography/internet: Ethereal alternate dimensions of cyberspace or grounded augmented realities?», Geographical Journal, vol.179, no.2 (June 2013), c.177-182.

6. Williams R.D. «Beyond Huawei and TikTok: Untangling US concerns over Chinese tech companies and digital security» URL: https://www.brookings.edu/research/beyond-huawei-and-tiktok-untangling-us-concerns-over-chinese-tech-companies-and-digital-security/ (дата звернення 17.03.2023).

Олексієнко К.О.
Національна академія СБ України

ПРОБЛЕМИ ПРОТИДІЇ КІБЕРНЕТИЧНИМ АТАКАМ рф НА ОБ'ЄКТИ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Дослідження проблеми протидії кібернетичним атакам рф у наш час є особливо актуальною темою. На жаль, ворог не залишає спроб нашкодити нашій державі на усіх можливих фронтах, одним з яких є інформаційний простір.Незмінним чином, гібридна агресія Російської Федерації щодо України в кіберпросторі є однією з основних загроз кібербезпеці країни. Кібератаки з боку росії націлені головним чином на інформаційно-комунікаційні системи державних установ України та на об'єкти критичної інформаційної інфраструктури .Вдалі атаки рф на об'єкти критичної інформаційної інфраструктури становлять серйозну загрозу для кібербезпеки України. Російські кібератаки здійснюються з метою виведення з ладу інформаційно-комунікаційних систем державних органів та об'єктів критичної інфраструктури(об'єктами критичної інформаційної інфраструктури є підприємства та установи (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), продовольство, охорона здоров'я, комунальне господарство, що є стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення, виведення з ладу або руйнування яких може мати вплив на національну безпеку і оборону, природне середовище, призвести до значних матеріальних та фінансових збитків, людських жертв), отримання прихованого доступу і контролю, здійснення розвідувальної та розвідувально-підривної діяльності. Ці атаки можуть мати серйозні наслідки, такі як порушення функціонування важливих інфраструктурних систем, втрата чутливої інформації та перешкоджання звичайним діям органів влади та громадськості. У зв'язку з цим, забезпечення кібербезпеки об'єктів критичної інфраструктури є надзвичайно важливим завданням для України. Лише протягом першого півріччя 2020 року Служба безпеки України нейтралізувала понад 300 кібератак і кіберінцидентів на об'єкти критичної інфраструктури.[2] До цих кібератак були причетні майже 20 хакерських угруповань, які також викрито і знешкоджено спецслужбою. Значну частину хакерів напряму контролювали з рф. Їх метою було завдання шкоди українським державним органам і підприємствам оборонно-промислового комплексу. Також згідно з повідомленнями Служби безпеки України, з моменту розпочаття повномасштабного вторгнення Росії, було виявлено та нейтралізовано понад 120 потужних кібератак на ресурси державних органів та військового управління України, а також на ІТ-системи об'єктів критичної інфраструктури, операторів зв'язку та ЗМІ.[1]

Отже, давайте розглянемо більш детально, деякі з проблем протидії кібернетичним атакам ворога на об’єкти критичної інфраструктури та певні способи їх вирішення:

Недостатня обізнаність з кібербезпекою

-Це дійсно серйозна проблема, оскільки недостатня обізнаність з кібербезпекою може призвести до порушення безпеки інформації та вразливості інформаційних систем до кібератак. Багато компаній та установ недооцінюють ризики кібербезпеки і не розуміють необхідність відповідних заходів захисту. Тому надзвичайно важливо проводити регулярну підвищення обізнаності з кібербезпекою серед персоналу інформаційних систем, а також регулярно аудитувати системи на вразливість і вживати відповідні заходи щодо їх захисту.

Недостатня координація між установами

-Так, недостатня координація між установами може стати перешкодою в протидії кібератакам на об’єкти критичної інформаційної інфраструктури. Це може бути пов'язано з розбіжностями в методах та стратегіях захисту, відсутністю обміну інформацією та координації дій між різними установами. Для забезпечення успішної протидії кібератакам необхідно розробляти та впроваджувати механізми співпраці та обміну інформацією між установами, а також проводити регулярні тренування та навчання співробітників установ з питань кібербезпеки.

Недостатнє фінансування та забезпечення ресурсами

-Для ефективного захисту від кібератак необхідне значне фінансування на розробку та впровадження новітніх технологій кібербезпеки, а також забезпечення достатньої кількості та якості людських ресурсів, які зможуть забезпечити захист інформаційних систем від потенційних загроз. Недостатній рівень фінансування та забезпечення ресурсами може призвести до недостатнього рівня захисту та зростання ризиків кібератак на об’єкти критичної інформаційної інфраструктури. Тому, вирішення цієї проблеми вимагає прийняття необхідних заходів для забезпечення належного рівня фінансування та ресурсів для забезпечення кібербезпеки.

Відсутність законодавчої бази

-Недостатня законодавча база та відсутність відповідальності за кібератаки може створювати небезпеку та підштовхувати зловмисників до здійснення кібератак. Для ефективної протидії кіберзлочинності необхідно мати належну законодавчу базу та відповідну її реалізацію, що включає в себе визначення видів кіберзлочинів, механізми виявлення та розслідування кібератак, а також встановлення відповідальності за кіберзлочинні дії та механізми їх покарання. До прикладу важливим кроком стало затвердження у 2016 році Стратегії кібербезпеки України. За роки реалізації попередньої Стратегії кібербезпеки України, затвердженої Указом Президента України від 15.03.16 р № 96, було докладено зусиль до становлення та розвитку національної системи кібербезпеки.[3] Важливим етапом її інституалізації стало прийняття Закону України “Про основні

засади забезпечення кібербезпеки України, який визначив правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері

кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.[4]

Результат покращення системи захисту можна буде побачити, якщо кожний елемент, який становить проблему, буде вирішено. Це дозволить нам підвищити ефективність заходів протидії атакам на об'єкти критичної інформаційної інфраструктури та забезпечити надійний захист нашої інформаційної безпеки в кіберпросторі.

Література

1.За час війни кількість хакерських атак в Україні зросла втричі. URL: https://www.ukrinform.ua/rubric-technology/3447656-za-cas-vijni-kilkist-hakerskih-atak-vukraini-zrosla-vtrici.htm

2. За півроку СБУ нейтралізувала 300 кібератак на об'єкти критичної інфраструктури URL: https://ssu.gov.ua/novyny/za-pivroku-sbu-neitralizuvala-300-kiberatak-na-obiekty-krytychnoi-infrastruktury

3.Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України від 26.08.21 р. № 447. URL: https://www.president.gov.ua/documents/4472021-40013 (дата звернення: 17.03.2023)

4. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163–19#Text

Пітиляк Д.В.
Білоус І.І.
Бондаренко І.Д.
к.ю.н.,
Національна академія СБ України

ЛЮДСЬКИЙ ФАКТОР ЯК ВРАЗЛИВІСТЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИ ЗАСТОСУВАННІ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Актуальність теми полягає в тому, що у сучасному світі зростаюча кількість кібератак, де інформаційні технології стали неодмінною складовою нашого життя, які здійснюються через соціальну інженерію, вказує на те, що хакери визнають цей метод ефективним для вторгнення в інформаційні системи та отримання

незаконного доступу до конфіденційної інформації. Однак, у більшості випадків, люди сприйнятливі до атак соціальної інженерії, тому що вони часто є найслабшою ланкою в ланцюжку безпеки, їх можна легко обдурити або змусити маніпулювати, щоб вони розкрили конфіденційну інформацію або вжили дій, які можуть поставити під загрозу безпеку. Обізнаність і освіта можуть значною мірою допомогти запобігти таким типам атак, і організації повинні вживати заходів, щоб гарантувати, що їхні співробітники усвідомлюють ризики та готові відповідним чином реагувати, щоб не призвести до серйозних проблем з безпекою інформації. Розглянути способи захисту від соціальної інженерії та рекомендації щодо збереження конфіденційної інформації в безпеці.

Поняття соціальної інженерії та його сутність. Соціальна інженерія — це техніка, з використанням інформаційно-комунікаційних технологій яку застосовують кіберзлочинці для маніпулювання особами, яка використовує вразливі місця людини, такі як довіра, страх або цікавість, для отримання несанкціонованого доступу до інформації або систем, щоб вони розголошували конфіденційну інформацію або виконували дії, які можуть поставити під загрозу безпеку інформаційних систем організації.

Існує багато різних методів соціальної інженерії, які використовуються залежно від мети та контексту. Деякі з найбільш поширених сьогодні методів соціальної інженерії включають:

- фішінг (Phishing) – масове розсилання електронної пошти великій групі адресатів. Ознайомлення з електронними листами спонукає їх до, наприклад, відкриття вкладення листа, переходу за посиланням на веб-сторінку. Його метою є виманювання у довірливого або неуважного персоналу комп’ютерної системи персональних даних;
- фармінг (Pharming) – перенаправлення користувачів на шахрайські сайти для отримання їх логіну та паролю. Це досягається завдяки розповсюдженню електронної пошти серед користувачів, наприклад, соціальних мереж, онлайн-банкінгу, поштових веб-сервісів;
- прітекстінг (Pretexting) – отримання інформації або спонукання до вчинення певних дій обманом на основі заздалегідь складеного сценарію або створення фіктивної ситуації. Застосовується через телефон та потребує проведення попередніх досліджень для входження в довіру;
- смішінг (Smishing) – отримання інформації шляхом масового розсилання SMS повідомлень з посиланням на веб-ресурси або з реквізитами організацій (наприклад, фінансових). Внаслідок цього здійснюються відповідні дії, наприклад, дзвінок до банку для перевірки стану рахунку з зазначенням конфіденційних даних: номеру картки, терміну дії;
- вішінг (Vishing) – отримання інформації шляхом входження в довіру під час розмови через IP-телефон. При цьому в порушення конфіденційності здійснюється завдяки викладенню прохання у повідомленні зателефонувати на

певний міський номер. Наприклад, вести номер карти, паролі, PIN-коди, коди доступу або іншу інформацію;

- вейлінг (Whaling) – надсилання листа електронної пошти представнику керівництва організації, що спонукає його до обов'язкового перегляду та відповіді на отриманий лист;

Ці методи можна використовувати окремо або в поєднанні один з одним.

Ознаки які допомагають виявити соціальну інженерію**.** Ознаки, виявлення соціальної інженерії:

- недостовірна або підроблена адреса відправника;
- неочікувані повідомлення про проблеми з безпекою;
- неочікувані запити про конфіденційну інформацію;
- тривожні повідомлення;
- вимоги негайної дії;
- надмірні подарунки або пропозиції;
- незнайомі запити на зустріч або спілкування;

Ці ознаки не завжди свідчать про соціальну інженерію, але можуть служити попередженням для того, щоб бути пильним і уважним.

Як протидіяти атакам соціальної інженерії**.** Способи захисту від соціальної інженерії:

- ставтеся з підозрою до небажаних повідомлень: будьте обережні з електронними листами, текстовими повідомленнями або телефонними дзвінками від людей чи організацій, яких ви не знаєте, або які здаються занадто гарними, щоб бути правдою;
- перевірте особу відправника: завжди перевіряйте особу особи, яка зв'язується з вами, перш ніж надавати будь-яку конфіденційну інформацію. Це можна зробити, передзвонивши в організацію за відомим номером телефону або перевіривши адресу електронної пошти на наявність орфографічних помилок;
- підтримуйте своє програмне забезпечення в актуальному стані: переконайтеся, що операційна система вашого комп'ютера, веб-браузер та інше програмне забезпечення оновлюються останніми виправленнями безпеки, щоб зменшити ризик використання;
- використовуйте надійні паролі: використовуйте надійні унікальні паролі для всіх своїх облікових записів в Інтернеті та вмикайте двофакторну автентифікацію, коли це можливо;
- навчіться: дізнайтеся більше про соціальну інженерію та про те, як розпізнавати та уникати таких типів атак. Будьте в курсі останніх тенденцій атак соціальної інженерії;

Рекомендацій щодо збереження конфіденційної інформації:

- використовуйте шифрування: зашифруйте свої дані за допомогою надійних алгоритмів шифрування, щоб запобігти несанкціонованому доступу;

- обмежити доступ: обмежити доступ до конфіденційної інформації лише тим, хто її потребує. Використовуйте елементи керування доступом і дозволи користувача, щоб переконатися, що лише авторизовані особи мають доступ до конфіденційної інформації;
- захистіть свою мережу: використовуйте брандмауери, системи виявлення вторгнень та інші засоби безпеки, щоб захистити свою мережу від зовнішніх загроз;
- використовуйте захищені канали зв'язку: використовуйте захищені канали зв'язку, як-от зашифровану електронну пошту або безпечні програми обміну повідомленнями, щоб надсилати й отримувати конфіденційну інформацію;
- навчіть своїх співробітників: навчіть своїх співробітників важливості збереження конфіденційної інформації та надайте їм інструменти та ресурси, необхідні для цього;

Висновки. Підсумовуючи, застосування соціальної інженерії стає все більш популярним методом атак на інформаційну безпеку. Загалом, забезпечення безпеки інформації є надзвичайно важливим у нашому сучасному світі, де технології займають все більш вагому роль. Розуміння того, як соціальна інженерія працює, може допомогти уникнути викрадення конфіденційної інформації та інших проблем з безпекою даних. Отже, необхідно вивчати та застосовувати методи захисту від соціальної інженерії та забезпечувати належний рівень свідомості та уважності серед користувачів інформаційних технологій. Соціальна інженерія — явище, якому можна протистояти, якщо дотримуватися нехитрих правил і зберігати пильність.

Література

1. Смалько О.А., Захист інформаційних ресурсів: *Монографія.* - *Кам'янецьПодільський:* ПП Буйницький О. А., 2011., С. 704.

2. Хартфілд Р. Лукас Г., Виявлення атак семантичної соціальної інженерії з найслабшими посилання: Впровадження та емпірична оцінка системи сенсора людини як безпеки . *Комп'ютери та безпека*, 2018., т. 76, С. 101-127.

3. Рєзнік Ю.М., Соціально-гуманітарні технології управління. *Специфика та можливості застосування*., 2010., С. 91-105.

4. Мутон Ф., Лінен Л., Венте Х., Приклади атак соціальної інженерії, шаблони та сценарії , *Комп'ютери та безпека*, 2016., т. 59, С. 186-209,

5. Енгебретсон П., Основи хакерства та тестування на проникнення. *Тестування на проникнення стало простим*, 2013., С. 54-81.

Піштова Ю.С.
Жевелєва І.С.
к.ю.н., доцент
Національна академія СБ України

ПРОБЛЕМИ ВИЗНАЧЕННЯ ПОНЯТТЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ТЕОРІЇ ТА НА ПРАКТИЦІ

Зміни, що відбулись в останні роки у суспільному житті в цілому та у сфері економічної конкуренції зокрема призвели до значного зростання обсягів інформації. Поряд з останнім зросла і швидкість зміни інформації. За таких умов сформувалась ситуація, за якої виник розрив між кількістю інформації, що характеризує сучасне буття і спроможністю її засвоїти та ефективно використати. У зв'язку з чим виникла проблема інформаційної дезорієнтації та поширенню дезінформації, яка значним чином ускладнила прийняття об'єктивних рішень та можливість формування адекватної поведінки. Окрім того, широкого поширення набули інформаційні і комунікаційні технології, змістом яких стало формування інформаційного ресурсу та його збереженням, передача інформації, надання різного роду інформаційних послуг [1].

Сучасний стан захищеності прав і законних інтересів людини, суспільства й держави в інформаційній сфері України свідчить про недостатній рівень правового регулювання й забезпечення інформаційної безпеки. Так, непоодинокими є випадки порушення чи безпідставного обмеження вказаних прав та інтересів, у нормах, що регулюють інформаційні відносини, у правовому забезпеченні інформаційної безпеки існує чимало суперечностей, лакун і колізій, а деякі відносини у цій сфері взагалі не врегульовані. Убачається, що все це зумовлене, насамперед, слабким теоретичним обґрунтуванням підгалузі правового забезпечення інформаційної безпеки та іншими системними прорахунками. Однією із фундаментальних категорій національної безпеки держави є категорія інформаційної безпеки, але при цьому, у Законі України «Про національну безпеку України», який є основним орієнтиром забезпечення національної безпеки України, вказано, що державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, безпеки критичної інфраструктури, кібербезпеки України та на інші її напрями, відсутнє визначення поняття інформаційної безпеки [1]. У зв'язку з цим є потреба у визначенні даного поняття.

Поняття «інформаційна безпека» зустрічається і у Законі України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки», де остання визначається як стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через:

неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [2].

Проте, слід враховувати, що даний правовий акт розроблявся і був прийнятий до початку явних проявів гібридної війни та повномасштабного вторгнення, а також реалізації європейського курсу України, і по-друге, на наше переконання даному підходу притаманний однобічний підхід до забезпечення інформаційної безпеки, який не зовсім доречний у сфері економічної конкуренції.

Проект Закону «Про внесення змін до деяких законодавчих актів України щодо забезпечення національної інформаційної безпеки та права на доступ до достовірної інформації» [3], в якому пропонується доповнити Закон України «Про національну безпеку України» визначенням «інформаційна безпека» значною мірою повторює зазначене вище поняття «інформаційна безпека», проте дещо розширює спектр негативного впливу, зокрема вже згадується інформаційно-психологічний вплив. Проте, як і в попередньому, воно займає більш оборонний характер, дещо нівелюючи активні заходи забезпечення інформаційної безпеки України.

Як правило, у науці інформаційну безпеку України визначають як стан, за якого в умовах дії реальних та потенційних загроз забезпечується самозбереження, сталий і прогресивний розвиток інформаційної сфери, зокрема захищеність інформаційної інфраструктури, інформаційного простору, інформаційних ресурсів, інформаційних процесів та їх суб’єктів, а також досягнення відповідних національних цілей та реалізація національних інтересів в інформаційній сфері. При цьому забезпечення інформаційної безпеки держави, на нашу думку, це постійний процес діяльності компетентних органів, спрямований на запобігання, протидію загрозам інформаційній сфері, застосування активних заходів інформаційного впливу, а також сукупність умов такої діяльності, які реалізуються і здатні контролюватися тривалий час [4, с. 88].

В основу даного підходу покладено принцип, відповідно до якого основною метою забезпечення інформаційної безпеки є створення безпечного інформаційного середовища. А для цього захищати національні інтереси й цінності, виходячи з виявлення загроз і намірів противника, замало. Даний підхід передбачає також протидію та активні контрзаходи у процесі забезпечення інформаційної безпеки держави.

Разом з тим, відмічаємо, що контекстний аналіз вживання законодавця поняття «безпека інформації» дає підстави тлумачити його як стан захищеності інформації в системі. Відповідно, «захист інформації» – це діяльність із забезпечення вказаного стану захищеності. Захист інформації як складова діяльності із забезпечення безпеки інформації та інформаційної безпеки є одним із

засобів захисту прав і законних інтересів людини, суспільства, держави в інформаційній сфері [4, с. 89].

Таким чином, вважаємо за доцільне, з метою чіткого системного врегулювання питань протидії інформаційному екстремізму, що забезпечило б захист законних інтересів людини від негативних інформаційних впливів, суспільної моралі та держави, а також задля усунення колізій і прогалин законодавства закріпити поняття інформаційної безпеки в Законі України «Про національну безпеку». Вважаємо, що закріплення даного поняття сприятиме захисту прав та інтересів держави і громадян в інформаційній сфері.

Література

1. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. Відомості Верховної Ради. 2018, № 31, ст.241. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 17.03.2023).

2. Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 09.01.2007 № 537-V. URL: https://zakon.rada.gov.ua/laws/show/537-16#Text (дата звернення: 17.03.2023).

3. Про внесення змін до деяких законодавчих актів України щодо забезпечення національної інформаційної безпеки та права на доступ до достовірної інформації: проект Закону України від 20.01.2020. URL: https://detector.media/infospace/article/174057/2020-01-21-porivnyalna-tablytsya-do-proiektu-zakonu-ukrainy-pro-vnesennya-zmin-do-deyakykh-zakonodavchykh-aktiv-ukrainy-shchodo-zabezpechennya-natsionalnoi-informatsiynoi-bezpeky-ta-prava-na-dostup-do-dostovirnoi-informatsii/ (дата звернення 17.03.2023).

4. Довгань О.Д., Ткачук Т.Ю. Концептуальні засади законодавчого забезпечення інформаційної безпеки України. *Інформація і право*. № 1(28). 2019. С. 86-99.

Полонська О.І.
Національна академія СБ України

ЩОДО ОСОБЛИВОСТЕЙ ФУНКЦІОНУВАНЯ ПУБЛІЧНИХ ЕЛЕКТРОННИХ РЕЄСТРІВ В УМОВАХ ВОЄННОГО СТАНУ

Правові засади створення та функціонування публічних електронних реєстрів (далі – ПЕР) встановлені Законом України «Про публічні електронні реєстри» [1]. Інформація, що міститься в ПЕР, відповідно до закону, може мати в тому числі і гриф «з обмеженим доступом». З метою адаптації до викликів і загроз спричинених повномасштабною збройною агресією рф проти України введенням

правового режиму воєнного стану [2] нормативні вимоги до організації роботи реєстрів та баз даних зазнавали чималих змін.

Першочерговим кроком статтю 38 Закону України «Про публічні електронні реєстри» доповнено положеннями про заборону функціонування державних реєстрів, що зберігаються на хмарних ресурсах (дата-центрах) на тимчасово непідконтрольних територіях України, територіях держав-агресорів, підсанкційних держав, та на територіях, що мають митний або воєнний союз з зазначеними державами [3].

На період дії воєнного стану визначено перелік додаткових заходів, що мають на меті забезпечення безперебійного належного функціонування ПЕР, як то зупинення, обмеження, невідкладне блокування доступу користувачів в порядку і на умовах встановлених законодавством, в тому числі і на територіях де ведуться активні бойові, з переліку затвердженого Міністерством з питань реінтеграції тимчасово окупованих територій. Також, на період дії воєнного стану і протягом 6 місяців після його закінчення встановлена можливість володільцем ПЕР укладати договори про тимчасове адміністрування хмарних сервісів [4] з іноземними юридичними особами. Важливим аспектом у цьому контексті є виважений вибір провайдера, який забезпечує високий рівень захисту даних та відповідає вимогам законодавства України.

Загрози військового (фізичного) та кібернетичного характеру на державні інформаційні ресурси у період збройної агресії рф набули критичного кількісного показника. З метою відновлення відомостей Державних електронних інформаційних ресурсів (після пошкодження або знищення, в тому числі внаслідок кіберінцидентів та кібератак), їх безперебійного і належного функціонування, вони підлягають обов'язковому резервному копіюванню в Національному центрі резервування [5]. Усі факти зовнішнього злочинного впливу на об'єкти ПЕР мають бути зафіксовані і належним чином задокументовані.

Наразі державні інституції та громадські організації і спілки, зокрема Міністерство закордонних справ України, Антикорупційний штаб, ГУР Міністерства оборони України з початком війни здійснюють роботу щодо ведення реєстрів військових злочинів/злочинців рф на території України. З метою фіксації і належного документування злочинів Прокуратурою України створено єдиний ресурс warcrimes.gov.ua. Також, розшуком і фіксацією протиправних діянь військових рф на території України займаються і фахівці OSINT. Видається, що прийняття відповідних нормативно-правових актів з метою налагодження взаємодії і створення Єдиного реєстру військових злочинів рф на території України допоможе оптимізувати дану роботу.

Щодо об'єктів ПЕР, слід зауважити, що нормативне регулювання відповідних реєстрів і баз даних періодично актуалізується. Зокрема, Закон України «Про Єдиний державний демографічний реєстр та документи, що підтверджують

громадянство України, посвідчують особу чи її спеціальний статус» доповнено положенням, що враховують вимоги Закону України «Про соціальний і правовий захист осіб, стосовно яких встановлено факт позбавлення особистої свободи внаслідок збройної агресії проти України, та членів їх сімей». Звертає на себе увагу той факт, що даний закон даючи перелік уповноважених суб'єктів не визначає володільця, а лише вказує розпорядника – центральний орган виконавчої влади, що реалізує державну політику в сферах міграції (Державна міграційна служба), а в ст.4 лиш згадується Кабінет Міністрів України, який встановлює порядок ведення зазначеного реєстру. Також, ст.11 закріплює безоплатне отримання Державним комітетом статистики України відомостей або інших персональних даних про особу з ЄДДРУ для використання у статистичних цілях. Ідентичне положення містить і ст.5 ЗУ «Про Єдиний державний реєстр призовників, військовозобов'язаних та резервістів». Вбачається, що варто внести уточнення щодо необхідності проведення дії із знеособлення персональних даних, які передаються.

Серед найважливіших і найактуальніших кроків нормативно-правового характеру у сфері ПЕР, враховуючи сумну статистику щодо кількості втрат не лише військовослужбовців але й цивільного населення, кількості осіб, котрі вважаються безвісно відсутніми і оголошеними померлими, а також тих, що зазнали травм та ушкоджень внаслідок військових дій країни-агресора, є прийняття Закону України «Про державну реєстрацію геномної інформації людини». Даним законом визначено правові вимоги, основні засади і порядок обробки геномної інформації фізичних осіб.

Значної кількості змін та доповнень зазнали нормативно-правові акти з питання обліку і реєстрації внутрішньо переміщених осіб та переселенців. Разом з цим, варто відмітити і той факт, що з метою надання різного роду соціальних пільг громадянам України з боку іноземних міжнародних організацій, благодійних і волонтерських фондів проводиться масштабна обробка персональних даних фізичних осіб, що потребує відповідного контролю національних уповноважених державних інституцій.

В умовах воєнного стану своєчасні зміни нормативно-правових актів та оптимізація процесів функціонування публічних електронних реєстрів мають вирішальне значення для забезпечення ефективності державного управління та надання громадянам послуг в режимі онлайн. Особлива увага нормотворців має приділятися виробленню дієвих механізмів захисту інформації з обмеженим доступом (в тому числі персональних даних фізичних осіб) та забезпеченню конфіденційності інформації в рамках єдиної інформаційно-комунікаційної системи країни. Слід зауважити і на необхідності розробки та впровадження нових технологій, сучасних конструкцій технічного захисту об'єктів критичної інфраструктури і для забезпеченням безперебійної роботи ПЕР у надзвичайних ситуаціях.

Література
1. Про публічні електронні реєстри: Закон України від 18.11.2021 р. №1907-IX. URL: https://zakon.rada.gov.ua/laws/card/1907-20
2. Про введення воєнного стану в Україні // Указ Президента України від 24.02.2022 р. №64/2022. URL: https://zakon.rada.gov.ua/show/64/2022
3. Про внесення змін до деяких законів України щодо забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів // Закон України від 15.03.2022 р. №2130-XI. URL: https://zakon.rada.gov.ua/laws/show/2130-20#Text
4. Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану // Постанова Кабінету Міністрів України від 12.03.2022 р. №263. URL: https://zakon.rada.gov.ua/laws/show/263-2022-n#Text
5. Про хмарні послуги // Закон України від 17.02.2022 р. №2075-IX. URL: https://zakon.rada.gov.ua/laws/show/2075-20#Text
6. Про реалізацію експериментального проекту щодо функціонування Національного центру резервування державних інформаційних ресурсів // Постанова Кабінету Міністрів України від 08.02.2021 р. № 94. URL: https://zakon.rada.gov.ua/laws/show/94-2021n#n15

Полотай О.І.
к.т.н., доцент,
Львівський державний університет безпеки життєдіяльності

КОМП'ЮТЕРНА КРИМІНАЛІСТИКА ЯК ОДИН З ІНСТРУМЕНТІВ ПРОТИДІЇ ТА РОЗСЛІДУВАННЯ ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Комп'ютерна криміналістика є прикладною наукою про розкриття і розслідування злочинів, пов'язаних з комп'ютерної інформацією, про методи отримання та дослідження доказів, що мають форму комп'ютерної інформації (так званих цифрових доказів), про що застосовуються для цього технічні засоби, такі як SIEM-системи та інструменти з відкритим вихідним кодом [1].

- Комп'ютерна криміналістика вирішує такі завдання [3]:

– розроблення тактики оперативно-розшукових заходів та слідчих дій, пов'язаних з комп'ютерною інформацією;

– створення методів, апаратних та програмних інструментів для збирання та дослідження доказів комп'ютерних злочинів;

– встановлення криміналістичних характеристик правопорушень, пов'язаних із комп'ютерною інформацією.

- Проблеми, що стоять перед експертами з комп'ютерної криміналістики,

можна розбити на три основні категорії: технічні та адміністративні [5].

- Технічні питання.
- Шифрування — Зашифровані дані можуть бути неможливо переглянути без правильної клавіші або пароля. Екзаменатори повинні враховувати, що ключ або пароль можуть зберігатися в іншому місці на комп'ютері або на іншому комп'ютері, до якого підозрюваний має доступ.
- Збільшення простору зберігання даних — носії зберігають все більшу кількість даних, що для експерта означає, що для їх аналізу комп'ютери повинні мати достатню потужність обробки та доступну ємність для зберігання даних, щоб ефективно працювати з пошуком та аналізом великої кількості даних.
- Нові технології — Обчислювальна техніка — це напрям, що постійно розвивається, де завжди з'являються нові апаратні засоби, програмне забезпечення та операційні системи. Жоден комп'ютерний експертно-криміналістичний експерт не може бути експертом у всіх областях, хоча з них часто можна очікувати аналізу того, що вони раніше не зустрічали.
- Адміністративні питання.
- Прийняті стандарти. В комп'ютерній криміналістиці є безліч стандартів і правил, деякі з яких, здається, є загальноприйнятими. Причини цього включають: установи, що встановлюють стандарти, прив'язані до окремих законодавчих актів; стандарти спрямовані як на правоохоронну, так і на комерційну криміналістику, але не на обох.
- Придатний для практики. У багатьох юрисдикціях немає кваліфікаційного органу для перевірки компетенції та цілісності професійних комп'ютерних судових експертів. У таких випадках кожен може представити себе як комп'ютерний судово-медичний експерт, який може призвести до комп'ютерної криміналістичної експертизи сумнівної якості та негативного уявлення про професію в цілому.
- Одним з основних складових комп'ютерної криміналістики є збір даних порушника інформаційної безпеки, тобто процес пошуку цифрових слідів і візуалізації відповідної інформації для людини із цифрових пристроїв і їх периферійного обладнання і носіїв.
- Розрізняють два типи збору даних:
- 1. Збір нелетючих даних, тобто таких, що залишаються незмінними коли система вимикається або знеструмлюється. Ці дані зазвичай отримують із звичайних файлів жорстких дисків, а також із файлів підкачки, невикористаних місць кластерів диску, незайнятого простору диска.
- 2. Збір летючих даних, тобто даних, які визначаються як дані працюючого комп'ютеру, що можуть бути втрачені при його виключенні.
- Також у розслідуванні комп'ютерних злочинів важливу роль відіграють SIEM-системи, оскільки в разі інциденту вони здатні надати всю необхідну доказову базу, придатну як для внутрішніх розслідувань, так і для суду [1].

- При оперуванні цифровими доказами необхідно дотримуватися таких принципів [4]:

– процеси збирання і збереження цифрових доказів не повинні порушувати цілісність цих доказів;

– особи, які проводять криміналістичну оцінку цифрових доказів, повинні бути фахівцями в цій області;

– процеси вилучення, оцінки, зберігання або передачі цифрових доказів повинні бути задокументовані, збережені і доступні для перегляду.

Поряд з загальнонауковими комп'ютерна криміналістика застосовує і спеціальні методи дослідження, властиві тільки їй. Назвемо деякі з цих методів:

– Створення і застосування спеціалізованих криміналістичних інформаційних систем; перенастроювання і використання в своїх цілях систем подвійного призначення.

– Використання з метою виявлення або дослідження доказів публічних пошукових систем (таких як «Google»), а також пошукових систем спеціального призначення.

– Створення віртуальної особистості для цілей проведення з її допомогою ОРЗ і агентурної роботи.

– Збір «хеш» функцій відомих файлів для відділення їх від файлів, з тримають оригінальну призначену для користувача або модифіковану інформацію.

– Архівування повного вмісту носіїв для цілей повного розслідування можливих інцидентів.

– Емуляція мережевих сервісів для дослідження поведінки підозрілих програм в лабораторних умовах.

Загальнонаукові та спеціальні методи комп'ютерної криміналістики повинні використовуватися в боротьбі зі злочинністю в наступних формах.

1. Виробництво (впровадження) комп'ютерно-технічних експертиз. Крім цих експертиз IT спеціалісти повинні залучатися до інших видів експертизи.

2. Участь фахівців у проведенні слідчих дій, що мають відношення до комп'ютерної інформації, - обшуку, виїмки, огляду місця події і т.д.

3. Участь фахівця в проведенні ОРЗ. Найбільш затребуване в обговорюваній області захід - зняття інформації з технічних каналів зв'язку - проводиться не просто «за участю», а тільки самим фахівцем.

4. Участь фахівця в судовому засіданні. Ця форма, передбачена КПК, стала активно використовуватися лише при розгляді справ по комп'ютерним злочинам.

5. Постачання оперативних працівників і слідчих технічними засобами, які ті можуть використовувати в роботі самостійно, без участі фахівця.

6. Навчання користувачів і технічних фахівців підприємств (тобто потенційних потерпілих) методам первинної фіксації цифрових доказів, їх оберігання від знищення.

Отже, комп'ютерна криміналістика, якщо враховувати всі вище описані питання, дає змогу оперативно виявляти порушників інформаційної безпеки та запобігати здійснення комп’ютерних злочинів, які посягають на інформаційну безпеку в майбутньому.

Література

1. Полотай О., Довганик С. SIEM-системи, як елемент аналізу та управління подіями CSOC // Автоматизація та комп’ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку, 16-22 березня 2020, Черкаси, ЧНУ, С. 60-61.

2. Полотай О.І. Комп’ютерна криміналістика: основні завдання та проблеми. Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення: матеріали Міжнародної наукової інтернет-конференції. – Тернопіль. вип. 68. 2022. – С. 29-30.

3. Полотай О.І. *Роль комп’ютерної криміналістики у забезпеченні інформаційної безпеки.* Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення: матеріали Міжнародної наукової інтернет-конференції. – Тернопіль. вип. 67. 2021. – С. 41-43.

4. Федотов Н.Н. Форензика – компьютерная криминалистика – М.: Юридический Мир, 2007. – 432 с.

5. Центр кібербезпеки та комп’ютерної криміналістики. [Електронний ресурс]. Режим доступу з https://csdfc.org/vvedennya-v-komp-yuternu-kriminalistiku

Приходько І.М.
Національна академія СБ України

ЩОДО ОКРЕМИХ АСПЕКТІВ ЗАБЕЗПЕЧЕННЯ ВЛАСНОЇ БЕЗПЕКИ В ХОДІ ПОШУКОВИХ ЗАХОДІВ В МЕРЕЖІ ІНТЕРНЕТ

Реалії останнього десятиріччя, які сформувалися як у площині загальносвітового вибухового розвитку соціальних медіа, так і у площині новітньої української історії, нерозривно пов’язаної із протидією триваючій російській агресії, надали технології здобування інформації з загальнодоступних джерел або розвідки з відкритих джерел (англ. Open Sours Intelligence, акронім - OSINT) статус загальновизнаного й одного з найбільш затребуваних інструментів не тільки вітчизняних спеціальних служб та безпекових структур, але й комерційних установ, громадських об’єднань і навіть приватних осіб. Тематика OSINT стала настільки популярною, що годі й намагатися перерахувати публікації, посібники, методичні рекомендації присвячені його організації, алгоритмам та спеціальному інструментарію. Разом з цим в практичних питаннях

підготовки до проведення такої розвідки залишаються певні аспекти, які потребують додаткового висвітлення та опрацювання.

Насамперед, мова йде про взаємопов'язані безпеку та технічне забезпечення відповідних пошукових (розвідувальних) заходів. Загальновідомим є принцип використання у таких заходах (або у підготовці їх проведення) не персоніфікованих технічних пристроїв. І якщо з мобільними терміналами, які використовуються для реєстрації легендованих акаунтів у соціальних мережах чи пошуку об'єктів оперативної зацікавленості у спеціальних телефонних сервісах «Truecaller», «Getcontact» все більш менш зрозуміло – для відповідних задач достатньо знайти телефон з «нульовим» чи «динамічним» IMEI або придбати на радіоринку найдешевший вживаний смартфон «no-name», то з ПЕОМ ситуація набагато складніша. Цілком зрозуміло, що ані особиста машина, яка використовуються розвідником та членами його сім'ї для побутових цілей, ані робоча, на якій постійно обробляється службова інформація (хоча б і без обмеження доступу), напряму для таких цілей використовуватися не може. Розвіднику необхідно виходити з аксіоми, що в процесі активного або «чутливого» для супротивника OSINT ця машина неодмінно буде піддаватися хакерським атакам чи впливу розповсюдженого в мережі шкідливого програмного забезпечення (далі – ШПЗ). При цьому звичайні засоби захисту, насамперед антивірусні програми, а також різноманітні антитрекери, приховувачі цифрового «відбитку» комп'ютера чи його реальної IP-адреси переоцінювати не варто (особливо безкоштовні) – вони не завжди здатні перешкодити професійним хакерським втручанням. В свою чергу результативне втручання загрожує деанонімізацією особи розвідника, розкриттям об'єктів його оперативної зацікавленості, нанесенням шкоди відповідному обладнанню та створеним базам даних (впритул до їх знищення), компрометацією усієї структури, яка здійснює OSINT чи конкретних його напрямків, а також в окремих випадках здатне створити постійний канал прихованого витоку інформації щодо заходів розвідника та його колег.

Водночас, придбання спеціально для цілей OSINT певної кількості окремих ПЕОМ, та ще й з високими технічними характеристиками (з урахуванням роботи з великими обсягами даних мінімальні вимоги, наприклад до процесору, це 8-ядерний intel I5 8-го покоління, до обсягів оперативної пам'яті – 16 Gb) є певною проблемою, особливо для бюджетних організацій. До того ж за необхідності роботи за машиною декільком розвідникам постають питання збереження конфіденційності напрямків пошукових заходів кожного з них, певних особистих налаштувань, необхідності перед кожним сеансом OSINT тривалий час пересвідчуватися у налаштуваннях безпеки тощо.

Виходом з цієї ситуації може стати створення та використання на базі визначених ПЕОМ т.зв. «віртуальних машин», тобто штучно створених за допомогою спеціального програмного забезпечення (наприклад, VirtualBOX)

віртуальних образів комп'ютерів, які емулюють роботу основної системи використовуючи частину її ресурсів. Робота віртуальних машин практично не впливає на роботу основного комп'ютера, вони підтримують роботу усіх відомих операційних систем (в тому числі рекомендованих для заходів OSINT Linux-подібних), дозволяють встановлювати нові програми та зберігати файли, здійснювати пошук у соцмережах, працювати із документами, електронними листами тощо. На основному ПЕОМ можна створювати декілька віртуальних машин, можна переносити образ віртуальної машини з одного комп'ютера на інший, зберігати його у хмарних сховищах, а також клонувати його. Певні операції дозволяють у разі необхідності «відкочуватися» до збережених налаштувань машини, знищувати усі дані або навіть саму віртуальну машину після закінчення сеансу роботи та інше. Через те, що віртуальна операційна система за стандартних налаштувань не має доступу до основної системи, ШПЗ з неї не може попасти до основного ПЕОМ. Таким чином віртуальна машина дозволяє відкривати підозрілі файли та переглядати підозрілі посилання. На віртуальні машини можна встановити унікальне програмне забезпечення для збереження анонімності у мережі, яке не можна встановити на звичайний ПЕОМ, наприклад, операційну систему Whonix. Також віртуальна машина дозволяє запускати одразу декілька різних операційних систем, що у багатьох випадках є дуже корисною опцією.

Не можна стверджувати, що використання віртуальних машин надає абсолютну безпеку роботи в Інтернеті. Як і будь-який інший суто програмний продукт вони мають певні вразливості і історія знає окремі випадки, коли потужним хакерським угрупованням вдавалося ці вразливості відшукати. Проте, застосування цього інструменту реально дозволяє у рази підвищити безпеку роботи у мережі та рівень захисту власної інформації. У поєднанні із гнучкістю самого продукту та його здатністю нівелювати вищезазначені складнощі і застереження в організації OSINT це виводить його опанування на на майже обов'язковий для кожного професійного розвідника рівень.

Руденко М.І.
Власова С.М.
Національна академія Служби безпеки України

ОСОБЛИВОСТІ ЗАХИСТУ ВІД СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ ЯК СКЛАДОВОЇ КІБЕРАТАКИ

Соціальна інженерія – це мистецтво маніпулювання людьми шляхом виконання дій або розкриття конфіденційної інформації, на додаток до технічного знищення баз даних. Це явище набуло розвитку як в Україні, так і в інших країнах.

Соціальна інженерія базується на досить простих психологічних характеристиках людини, таких як: принцип взаємності («ти мені – я тобі»), принцип соціальної перевірки (ви оцінюєте свою поведінку в контексті поведінки більшість), повага до влади (ви довірятимете лікарю та поліції більше, ніж звичайній людині). Усі ці правила стосуються «офлайнового» шахрайства, але вони мають свої особливості, коли вчиняються онлайн.

Є багато методик, які підпадають під загальний термін соціальної інженерії у сфері кібербезпеки. Серед найвідоміших методик – спам та фішинг. Спам – це масове розповсюдження небажаних листів. Найчастіше спам – це лист електронної пошти, який відправляється одразу на велику кількість адрес, але він також може бути отриманий через миттєві повідомлення SMS та соціальні мережі. Фішинг – це форма кібератаки, під час якої злочинець намагається отримати довіру до жертви для виманювання таємної інформації. У кожному ланцюжку безпеки ми майже зазвичай є найслабшою ланкою, оскільки чутливі до різноманітних видів шахрайства. Методи соціальної інженерії користуються цією вразливістю людей щоб обманом неволити жертв, розкрити конфіденційну інформацію [1].

Особливості захисту від соціальної інженерії. Заходи захисту від соціальної інженерії включає наступні етапи:

1. Регулярне навчання з кібербезпеки усіх працівників включно з топ-менеджментом та IT-спеціалістів.

2. Впровадження заходів безпеки, які попереджають про можливі випадки зловживань, а також сповіщають про виявлення спаму та фішингу.

3. Створення політики безпеки з чітким планом дій, які співробітники повинні будуть вжити, якщо виявляти ознаки соціальної інженерії.

4. Застосування рішення для централізованого керування корпоративною мережею для надання повного огляду мережі всіх рішень безпеки та подій для виявлення та нейтралізації потенційних загроз.

Протидія соціальній інженерії схожа на внутрішню боротьбу з людською суттю. Потрібно усвідомлювати, що ніякі технічні заходи захисту інформації практично не допоможуть вберегти від соціального інжинірингу. Пов'язано це з тим, що соціальні інженери користуються слабкостями не технічних засобів, а як говорилося, людського фактору. У зв'язку з цим, єдиний спосіб протистояти соціальним інженерам – це постійна і правильна робота з персоналом.

Для того, щоб створити методику навчання персоналу, яка буде працювати, потрібно зрозуміти, чому люди вразливі для атак. Для виявлення цих тенденцій, необхідно звернути на них увагу завдяки дискусії – цим можна допомогти співробітникам зрозуміти, як соціальний інженер спроможний маніпулювати людьми.

Основна роль щодо боротьби з загрозами соціальної інженерії покладається на організацію, де працює персонал. Організація відповідає за те, щоб попередити

співробітників, наскільки серйозною може бути публікація «непублічної» інформації. Добре продумана інформаційна політика безпеки разом з гідним навчанням і тренуваннями покращать розуміння співробітників про належну роботу з корпоративною інформацією [2].

Навчання безпеки в межах політики організації по захисту інформації повинно проводитися для всіх співробітників без винятку, а не лише для співробітників, у яких є електронний або фізичний доступ до інформаційних активів організації. В умовах нашого часу майже все, чим займаються співробітники, пов'язане з обробкою інформації. Саме через це політика безпеки організації повинна поширюватися по всьому підприємству, незалежно від статусу співробітників.

Головною метою будь-якої навчальної програми є необхідність переосмислення співробітниками своєї поведінки і відносини, мотивування їх бажанням оборонити і зберегти інформацію організації. Хорошою мотивацією є демонстрація винагороди за участь не самої організації, а конкретних співробітників.

Інформація стає більш важливою у сучасному світі. Тому на теперішній час особливості захисту від соціальної інженерії як складової кібератаки щзалежать від наявного інформаційно-психологічного впливу на свідомість особи.

Інформаційно - психологічний вплив (ІПВ) – це вплив на свідомість особи і населення задля внесення змін у їх поведінку та (або) світогляд. Звідси виникає необхідність у забезпеченні інформаційно-психологічної безпеки.

Інформаційно-психологічна безпека особи (у вузькому розумінні) – це стан захищеності психіки людини від негативного впливу, який здійснюється шляхом упровадження деструктивної інформації у свідомість і (або) у підсвідомість людини, що призводить до неадекватного сприйняття нею дійсності. Особливо актуальним забезпечення інформаційно-психологічної безпеки в Україні стало у зв’язку з агресією росії проти України, коли гостро постало питання із підтримки частиною населення територіальної цілісності України, підтримання на високому рівні морального бойового духу військовослужбовців, сил АТО.

Застосування інформаційно-психологічного впливу та забезпечення інформаційно-психологічної безпеки неможливе без детального розгляду його теорії та методів реалізації.

Науковці зробили висновок, що використання інформаційної війни є спробою отримати перевагу над конкурентом або противником завдяки використанню власних або блокування інших інформаційних ресурсів. Вони довели, що інформаційна війна може вестися у фізичній, інформаційній і когнітивній області – це показує, що інформаційне протиборство може включати як традиційне фізичне знищення інформаційних ресурсів противника, так і виконання дій, направлених на людський розум [3].

Дослідники виявили, що одним із найбільш перспективних підходів до розуміння інформаційної війни на локальному рівні є гібридні моделі, які використовують моделі визначеного інформаційного простору та моделі соціальної мережі. Дана гібридна модель включає в себе організаційні та когнітивні моделі. У даній моделі інформація зменшується і перетворюється у вузлах та із затримкою через обмеження зв'язку між вузлами. Така модель може об'єднати аналіз соціальних мереж для оцінки аспектів комунікації та ієрархії, із переконанням мереж, для оцінки аспектів індивідуальної обробки інформації. Тобто в них використовують соціальні мережі для того, щоб зробити переконання мережі динамічними.

Наукові розробки із питання інформаційного протиборства є досить поширеними та грунтовними. Проте, існує проблема у побудові формальної моделі інформаційно-психологічного впливу. Тому отримані результати дозволять більш чіткіше визначити власне функцію та процес інформаційно-психологічного впливу. Це допоможе розробити нові кращі або покращити наявні методи захисту від нього, дозволить створити ефективні методи контрдій під час атаки.

У якості висновку слід зазначити, що основним недоліком у сфері запобігання негативним проявам соціальної інженерії є відсутність системної роботи щодо її виявлення та подолання, наявність лише декларативних положень у стратегіях (іншими вони і не можуть бути, що зрозуміло) та відсутність прийнятих законодавчих та підзаконних актів на їх конкретизацію та розвиток, низький рівень проінформованості населення щодо можливих загроз соціальної інженерії, а також високу латентність злочинів у цій сфері, що унеможливлює виявлення та притягнення до відповідальності усіх винних осіб.

Література

1. ELAKPI Наукова періодика Information Technology and Security. *Ukrainian research papers collection 2019. Information Technology and Security*, 2019.,Vol. 7, Iss. 2 (13), веб сайт URL: https://ela.kpi.ua/handle/123456789/33885 (дата звернення 14.03.2023).

2. Цуркан О. Методи протидії використанню соціальної інженерії. *Information Technology and Security*. 2019., Vol. 7, Iss. 2 (13). С. 161–170., веб – сайт URL:https://ela.kpi.ua/handle/123456789/33885 (дата звернення 13.02.2023).

3. Ткачук Л.М., Вишньовський В.В. Соціальна інженерія як засіб впливу на людську свідомість. веб – сайт URL: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/20485/4049.pdf (дата звернення 14.03.2023)

Сімоненко О.О.
викладач Національної академії Служби безпеки України

РОЛЬ КІБЕРБЕЗПЕКИ У ПОВСЯКДЕННОМУ ЖИТТІ І ЗАХИСТІ ПРИВАТНИХ ДАНИХ В МЕРЕЖІ ІНТЕРНЕТ

На сучасному етапі новітніх інформаційних та комунікаційних технологій в усіх сферах життєдіяльності людини актуального значення набуває кібербезпека. Використання технологій стало звичною нормою повсякденного життя громадян, корпорацій, держави. Одночасно з цим, використання технологій та комунікаційних мереж несе в собі ризики зловживань та зловмисних дій. Тому питання кібербезпеки є актуальними та важливими.

Все більше часу на сьогодні люди проводять у цифровому середовищі – сервіси для бізнесу та розваг, соціальні мережі, ігри тощо. Для того, щоб мінімізувати ризики втрати приватної інформації, досить швидко розвивається спеціальність під назвою «кібербезпека».

Кібербезпека – це процес застосування заходів безпеки з метою забезпечення конфіденційності, цілісності та доступу даних. Кібербезпека забезпечує захист ресурсів (інформація, сервери, підприємства, приватні особи). Кібербезпека покликана захистити дані на етапі їх обміну та збереження. До таких заходів безпеки входять контроль доступу, навчання, аудит та оцінка ризиків, тестування, управління та безпека авторизації.

Відповідно до ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України», «кібербезпека – це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі».

Для України серед чинників, які впливають на розвиток інформаційного простору та кібербезпеки, одним із ключових є рівень добробуту населення та фінансові можливості бізнес-структур. Належний рівень матеріального забезпечення дає можливості як населенню, так і бізнесу інвестувати кошти у новітні технології розробки, інформаційну безпеку та у розвиток інформаційно-комунікаційних мереж. Тому для громадян, які не в змозі на індивідуальному рівні оплачувати послуги з використання інформаційних мереж, держава має створити умови для безпечного громадського доступу та користування такими мережами. Водночас наявна небезпека протиправних дій у сфері впровадження та використання новітніх інформаційних технологій полягає у незаконному копіюванні та спотворенні даних, що може мати незворотні наслідки для системи державного управління. В Україні така загроза набуває особливого значення,

оскільки в державних органах недостатньо висококваліфікованих фахівців з інформаційної та кібербезпеки. Також слід зважати і на те, що для ефективного використання новітніх технологій громадянам України потрібно володіти належним рівнем знань і навиків. Для цього є доцільним створення з боку держави умов для отримання громадянами відповідної освіти та необхідних знань у сфері використання інформаційних технологій.

В Україні для забезпечення кібербезпеки необхідно забезпечити дотримання принципів та норм міжнародного та національного законодавства, сформувати чіткі вимоги та алгоритми для протидії кібератакам, несанкціонованому втручанню, копіюванню та незаконному поширенню інформації, забезпечити доступ до отримання знань і навичок у використанні інформаційних технологій, взяти під контроль вартість і якість надання інформаційних послуг. Також важливим аспектом є пошук можливостей для збільшення державних та приватних інвестицій у кібербезпеку.

Спеціалісти з кібербезпеки займаються розробкою охоронних систем для різних телекомунікаційних мереж і електронних баз даних, тестують і вдосконалюють власні та сторонні розробки для уникнення ризиків витоку відомостей, що становлять державну або комерційну таємницю, конфіденційну інформацію. Дана професія є порівняно «молодою», сучасною і отримала широке розповсюдження у світі у зв'язку із впровадженням комп'ютерних та мережевих технологій практично в усіх організаціях – від невеликих комерційних фірм до органів державної безпеки.

У наш час абсолютно всі інформаційні системи мають функції авторизації і реєстрації з використанням особистого паролю. Більшість успішних кібератак на держави, громадян та бізнес були можливі через те, що в користувачів різних систем були встановлені прості паролі, що призводило до великих збитків. Іноді користувачі нехтують складними паролями, створюючи прості паролі, які легко дізнатися.

В усіх системах потрібно завжди використовувати додаткову перевірку основного паролю, а саме – двофакторну (двокрокову), або багатофакторну аутентифікацію, це може бути відбиток пальця, або додатковий пароль, який приходить повідомленням на особистий мобільний номер користувача. Майже щодня на екранах гаджетів можна побачити повідомлення про те, що з'явилася нова версія програмного забезпечення і його потрібно оновити. Якщо не оновлювати програми своєчасно, то зловмисники можуть використати ці вразливості під час кібератак, адже після появи нових оновлень ці вразливості публікуються у відкритих джерелах, таким чином вони стають доступними для хакерів, які можуть скористатися ними у цілях шахрайства. Оновлювати потрібно усі пристрої, які підключені до мережі Інтернет та їх операційні системи, а також потрібно оновлювати браузери і програми.

Якщо оновлювати програми несвоєчасно, то наслідки можуть бути невиправними. Персональна інформація, яка зберігалася роками, може зникнути або нею може заволодіти хакер після кібератаки, оскільки зламати можна будь-який пристрій, який під'єднано до мережі Інтернет.

Під час користування комп'ютерними пристроями не потрібно нехтувати антивірусними програмами, які можуть бути вбудовані в операційну систему. Їх потрібно регулярно використовувати і оновлювати, адже вони значно знижують ймовірність кібератак до операційної системи.

Кіберзлочинці полюють на персональні дані користувачів, банківські рахунки, паролі та іншу інформацію, яка існує в електронному вигляді, що в подальшому використовують для крадіжки коштів з банківських рахунків і т.д.

Кібербезпека є важливою, оскільки вона забезпечує належну роботу сервісів, на яких побудований сучасний світ. Більшість систем керування сервісами, без яких важко уявити наше повсякденне життя, працює через Інтернет – від фінансових організацій і закладів охорони здоров'я до електричних мереж, що живлять цілі міста.

Отже, переходячи у світ цифрових технологій слід пам'ятати про те, що у повсякденному житті варто дотримуватися основних правил безпеки із захисту приватних даних в мережі Інтернет, при роботі з гаджетами. Саме кібербезпека забезпечує захист електронних ресурсів і є важливою галуззю, яку слід знати всім, хто використовує гаджети та мережу Інтернет.

Слюсар А.І.
Національна академія Служби безпеки України

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ВІД КІБЕРАТАК

Захист критичної інфраструктури від кібератак стає все важливішим завданням у забезпеченні безпеки нації та суспільства. Розвиток кіберзлочинності та загроз кібербезпеці спонукають організації до пошуку нових технологій для захисту КІ, а штучний інтелект може стати одним з найбільш ефективних засобів.

Застосування ШІ для захисту КІ передбачає використання алгоритмів машинного навчання для виявлення аномалій у поведінці користувачів, знаходження вразливостей та виявлення шкідливих програм. Крім того, застосування ШІ може забезпечити прогнозування кібератак та автоматизувати процес їх реагування, що значно скорочує час реакції та підвищує ефективність захисту.

Наприклад, ШІ може бути використаний для виявлення аномальних мережевих активностей за допомогою машинного навчання. Він навчається

розрізняти нормальні мережеві активності від потенційно шкідливих, таких як сканування портів або спроби несанкціонованого доступу до системи. Після виявлення аномалії ШІ може автоматично виконувати певні дії, такі як блокування доступу до системи або сповіщення професійних кібербезпекових аналітиків.

Ще одним прикладом використання ШІ для захисту КІ є використання нейронних мереж для виявлення нових видів шкідливих програм. Нейронні мережі можуть навчитися розрізняти шкідливі програми від нормальних, а також визначати нові види шкідливих програм, які ще не були виявлені. Це дозволяє забезпечити більш ефективний захист від нових загроз, що з'являються щодня.

Книга "Data Mining and Machine Learning in Cybersecurity" авторства Sumeet Dua та Xian Du пропонує огляд методів машинного навчання для захисту від кібернападів та виявлення кіберзлочинності. Дерева рішень, наївний Баєс та метод опорних векторів є основними методами машинного навчання, розглянутими в цій книзі.

Дерева прийняття рішень - це один з методів машинного навчання, який використовується для класифікації та прогнозування даних. Кожен вузол дерева представляє параметр, за яким приймається рішення про класифікацію даних. Цей метод може бути використаний для виявлення та прогнозування нових видів шкідливих програм, які ще не були виявлені.

Метод наївного Баєса – це інший метод машинного навчання, який використовується для класифікації даних. Його основна ідея полягає в тому, щоб використовувати вірогідності того, що деякий об'єкт належить до певного класу, для прийняття рішення про класифікацію. Цей метод може бути застосований для виявлення та блокування спаму в електронній пошті та виявлення нових видів шкідливих програм.

Метод опорних векторів (SVM) - це ще один метод машинного навчання, який шукає гіперплощину, що розділяє дані у дві або більше класів. Цей метод може бути використаний для виявлення нових видів шкідливих програм та виявлення вразливостей у системі. Інноваційні підходи до захисту КІ забезпечують ефективний захист від нових загроз, що з'являються щодня.

Наука про машинне навчання постійно розвивається, та не завжди вимагає нагляду. Існують методи навчання без нагляду, які дозволяють системі самостійно навчатися. До них відносяться наступні методи:

- K-means кластеризація - цей метод шукає k центрів кластерів, де кожен елемент даних належить до кластера з ближчим до нього центром.
- DBSCAN (Density-Based Spatial Clustering of Applications with Noise) - цей метод кластеризації базується на густині точок у просторі та знаходить області з високою густиною точок як кластери.
- Hierarchical clustering - цей метод кластеризації об'єднує найбільш близькі кластери, поки не залишиться один кластер або досягне певного рівня злиття.

- Principal Component Analysis (PCA) - цей метод зменшення розмірності даних знаходить головні компоненти даних, які мають найбільшу варіативність.
- Independent Component Analysis (ICA) - цей метод зменшення розмірності даних знаходить незалежні компоненти даних, які мають найбільшу незалежність.
- Association Rule Mining - цей метод аналізу даних знаходить зв'язки між різними елементами даних та встановлює правила на основі цих зв'язків.
- Clustering of Categorical Data - цей метод кластеризації для даних з категоріальними змінними використовує міру подібності між категоріями.

Використання штучного інтелекту (ШІ) є дуже важливою технологією для захисту критичної інфраструктури від кібератак. Застосування методів машинного навчання та нейронних мереж дозволяє ШІ навчитися виявляти нові загрози та розпізнавати аномальні активності, що робить захист критичної інфраструктури більш ефективним. В результаті цього захист критичної інфраструктури може бути ефективнішим, що дозволить системі бути більш підготовленою до різних видів кібератак.

Література

1.Parisi A. Hands-On Artificial Intelligence for Cybersecurity. Бірмінґем : Packt Publishing Ltd., 2019. 317 p.

2. Dua S., Du X. Data Mining and Machine Learning in Cybersecurity. New-York : Auerbach Publications, 2011. 223 p.

Тарасюк. К.І.
Національна академія СБ України

ПРОБЛЕМИ ТА ШЛЯХИ ВИРІШЕННЯ ПРОТИДІЇ КІБЕРНЕТИЧНИМ АТАКАМ рф НА ОБ'ЄКТИ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Законом України "Про основні засади забезпечення кібербезпеки України" [1] визначено правові та організаційні основи захисту життєво важливих інтересів людини і громадянина, суспільства і держави та національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, а також засади координації їхньої діяльності із забезпечення кібербезпеки.

Підпунктом 2 пункту 3 статті 8 Закону визначено, що функціонування національної системи кібербезпеки забезпечується шляхом створення нормативно-правової і термінологічної бази у сфері кібербезпеки, гармонізації нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної

безпеки та кібербезпеки відповідно до міжнародних стандартів, зокрема стандартів Європейського Союзу і НАТО.

Згідно щорічного плану Державною службою спеціального зв’язку та захисту інформації України здійснюються заходи з оцінки стану захищеності інформаційних систем в державних органах, органах місцевого самоврядування, військових формуваннях, на підприємствах, в установах і організаціях незалежно від форм власності. Заходи полягають в детальному аналізі мереж і систем з точки зору можливого втручання потенційних зловмисників та правопорушень. Однак, кількість інцидентів в інформаційно-телекомунікаційних системах протягом останніх років не зменшується.

Метою дослідження: визначення понять та обґрунтування позиції щодо кібернетичних атак рф проти України, та її вплив на національну безпеку.

Виклад основного матеріалу дослідження: Кібернетичні атаки рф на об'єкти критичної інформаційної інфраструктури є серйозними загрозами для національної безпеки і економічного добробуту країни. У зв'язку з цим існують деякі проблеми, пов'язані з протидією цим атакам. Деякі з них включають наступне:

1) Недостатня захищеність системи інформаційної безпеки. У багатьох випадках об'єкти критичної інформаційної інфраструктури не обладнують потрібними заходами безпеки, що дозволяє кіберзлочинцям виконувати атаки.

2) Необхідність вдосконалення стратегій захисту від кібератак. Існуючі стратегії захисту від кібератак можуть бути недостатніми або застарілими. Тому потрібно розробляти нові методи протидії кібератакам, враховуючи останні тенденції в цій сфері.

3) Недостатня кваліфікація фахівців з інформаційної безпеки. У багатьох випадках відсутність кваліфікованих фахівців з інформаційної безпеки ускладнює боротьбу з кібератаками. Тому потрібно зробити зусилля для набору та навчання кадрів.

4) Непотрібність усунення вразливостей системи. Багато компаній в цілях економії часто ігнорують усунення вразливостей в системах, що використовують технології, які вже застаріли, що може спровокувати атаки на них та порушення безпеки.

5) Брак координації і зв'язку в органах державного управління. Взаємодія між органами державного управління може бути слабкою, що ускладнює виявлення і протидію кібератакам.

Ці проблеми потрібно вирішувати, розвиваючи сучасні технології захисту інформації та удосконалюючи стратегії протидії кібератакам. Також важливо підвищувати свідомість про безпеку в інформаційному просторі серед населення і підприємств.

В сучасних умовах, як видається, до найбільш важливих напрямів кіберзахисту слід віднести: об’єкти критичної інфраструктури; суб’єкти фінансової системи

(НБУ, Мінфін, Держказначейство); інформаційні ресурси, реєстри, системи і бази даних. Нині в Україні налічується понад 350 публічних електронних реєстрів, які перебувають у власності більш ніж 80 державних установ (Міністерств, служб, агентств тощо). При цьому, значні обсяги персональних даних громадян дублюються і накопичуються у численних базах даних, які далеко не завжди контролюються чи перебувають у власності держави [3].

Хочу виділити, засоби запобігання, які на мою думку, можуть бути ефективними у боротьбі з кібернетичним атакам рф:
Одним з ключових засобів запобігання впливу кібернетичних атак рф на об'єкти критичної інформаційної інфраструктури є створення високого рівня кібербезпеки. Для цього необхідно забезпечити:

1. Аудит безпеки. Майже кожен об'єкт критичної інформаційної інфраструктури потребує аудиту безпеки. Іншими словами, необхідно провести ретельний аналіз, який дозволить виявити слабкі місця, які можуть стати причиною вразливості системи в цілому.

2. Використання захисту від відкритих атак. Система захисту від відкритих атак – це захисна технологія, яка дозволяє забезпечити комп'ютерну безпеку за допомогою блокування кібернетичних проникнень на різних рівнях ієрархії.

3. Системи моніторингу та аналізу мережі. Ці технології дозволяють виявляти підозрілі дії користувачів або ненормальні режими роботи різних компонентів мережі.

4. Відповідність міжнародним стандартам із кібербезпеки. Відповідність міжнародним стандартам дозволяє більш точно визначити необхідні обов'язки та відповідальність.

5. Навчання персоналу. Чим більше співробітників компанії знають про кібербезпеку, тим менше ризик її порушення. Тому навчання персоналу з цієї теми є дуже важливим засобом запобігання впливу кібернетичних атак рф на об'єкти критичної інформаційної інфраструктури.

Слід відмітити основні проблеми протидії кібернетичним атакам:

1) Недостатня увага та фінансування: Деякі країни мають недостатнє фінансування та ресурси для адекватного захисту своєї критичної інформаційної інфраструктури від кібернетичних атак з боку рф.

2) Недостатня координація: Іноді національні програми з кібербезпеки не координуються добре з іншими програмами, які займаються критичною інформаційною інфраструктурою, що може призвести до прогалин у захисті.

3) Недостатня свідомість: Не всі люди, які працюють у сфері критичної інформаційної інфраструктури, розуміють, що кібербезпека є однією з найбільш важливих проблем. Тому вони можуть не дотримуватися базових правил безпеки.

4) Технічна складність: Сучасна критична інформаційна інфраструктура може містити різні захисні рішення, що заважає координації і захисту від кібернетичних атак.

5) Недостатня правова база: Нормативно-правова база у сфері забезпечення кібербезпеки перебуває на етапі становлення для протидії кібернетичним атакам на критичну інформаційну інфраструктуру.

Висновки. Кібернетичні атаки з боку рф на об’єкти критичної інформаційної інфраструктури можуть призвести до серйозних наслідків, одним з провідних заходів попередження кібернетичних атак є забезпечення досконалої безпеки мереж і створення надійних механізмів захисту, а також постійного вдосконалення цих систем відповідно до нових загроз.

Крім того, важливими є взаємодія з іншими країнами, обмін досвідом в протидії кібернетичним загрозам та розвиток міжнародних стандартів і правил щодо кібернетичної безпеки.

Необхідно активно працювати над інформаційною безпекою на всіх рівнях — від окремих користувачів до компаній і держав. Для ефективного протистояння кібернетичним атакам важливо розробити комплексні плани дій на випадок небезпеки, навчити людей правильно поводитись в ІТ сфері, вибирати надійні паролі і не допускати загроз до баз даних і систем.

Нарешті, щоб успішно протистояти кібератакам, необхідно, щоб були розроблені нові, більш криптографічні системи, і спеціальні технології захисту, що зав'язані на поведінці користувача. Захистити систему обробки інформації можна, якщо постійно зростати кваліфікацію персоналу та оновлювати системи захисту.

Отже, протидія кібернетичним атакам рф на об’єкти критичної інформаційної інфраструктури потребує всебічного підходу та передбачення комплексних заходів у сфері кібербезпеки. Варто зауважити, що протидія кібератакам має бути призначена на тривалий термін, оскільки кібернетичні загрози постійно змінюються і вдосконалюються.

Література

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

2. Сучасні правові стандарти Європейського Союзу у сфері захисту персональних даних: зб. документів / неоф. пер. з англ. І. Майстренко; за ред. В. Брижко; передмова В. Пилипчука. – (НДІ інформатики і права Національної академії правових наук України). Київ: ТОВ “Видавничий дім “АртЕк”, 2018. 180 с.

3. Костенко О.В. Проблеми правового регулювання та розвиток кібернетичної ьещпеки України та сучасному етапі. Інформація і Право. № 3(30)/2019. 96.

4. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. – Інформаційна та кібербезпека:соціотехнічний аспект.

Телелим В. М.
д.в.н., професор,
Національний університет оборони України імені Івана Черняховського

ПРОЯВИ КІБЕРАТАК НА ДЕРЖАВНУ, ВІЙСЬКОВУ ТА КРИТИЧНУ ІНФРАСТРУКТУРУ

Кібератаки стають все більш поширеними та серйозними загрозами для державної, військової та практичної інфраструктури. У зв'язку з цим, дослідження проявів кібератак та їх наслідків на різні види інфраструктури є надзвичайно важливим для забезпечення інформаційної безпеки. Метою даної тези є проаналізувати прояви кібератак на державну, військову та практичну інфраструктуру, описати їх наслідки та визначити рівень підготовки інфраструктури до захисту від кібератак. Це дослідження має на меті надати новітні знання щодо захисту від кібератак та сприяти розвитку стратегій забезпечення інформаційної безпеки.

І. Теоретичний аналіз проблеми.

Кібератака є складним явищем, що має різні прояви та наслідки для інфраструктури.

Згідно зі стандартом "CNSSI 4009-2015 under computer network attack (CNA)" кібер-атака – це дії, здійснені за допомогою комп'ютерних мереж з метою порушення, відмови, деградації або знищення інформації, що знаходиться в комп'ютерах та комп'ютерних мережах, або самі комп'ютери та мережі. Також важливо зазначити, що в межах Міністерства оборони США, Joint Publication 3-13 "Операції з інформацією" від 27 листопада 2012 року затвердило вилучення термінів та визначень комп'ютерного мережевого нападу (CNA), захисту комп'ютерних мереж (CND), експлуатації комп'ютерних мереж та операцій у комп'ютерних мережах (CNO) та починаючи з JP -1-02, "Словник термінів Міністерства оборони та асоційованих термінів". Цей термін та визначення більше не публікуються в JP 1-02. JP 1-02 є основним джерелом термінології під час ділового листування та підготовки планувальних документів з політики, стратегії, доктрини. Терміни більше не використовуються в документах, що оновлюються в межах Департаменту міністерства оборони США. JP 1-02, після публікації JP 3-12, "Операції в кіберпросторі", надає нові терміни та визначення, такі як кіберпростір, операції в кіберпросторі, кіберперевага, оборонні дії в кіберпросторі, захисні дії в кіберпросторі, операції з мереж інформації Міністерства оборони США та напади в кіберпросторі [1-2].

Інформаційна безпека є важливою складовою захисту від кібератак. Вона полягає в забезпеченні конфіденційності, цілісності та доступності інформації. Інфраструктура – це система технічних засобів, яка забезпечує функціонування різних галузей економіки та соціальної сфери.

Типи кібератак можна класифікувати за різними ознаками, такими як метод атаки, ціль атаки, масштаб та складність [3]. Одним з видів кібератак є DDoS-атака, при якій здійснюється завдання великої кількості запитів на сервер, що призводить до перевантаження та відмови в обслуговуванні [4]. Іншим типом кібератак є віруси, черв'яки та троянські програми, що можуть призвести до руйнування даних, злому паролів або іншої шкоди [1].

Наслідки кібератак для державної, військової та практичної інфраструктури можуть бути надзвичайно серйозними. Наприклад, кібератака на електронну систему голосування може спричинити перебої в голосуванні та порушити демократичний процес. Кібератаки на військові об'єкти можуть призвести до руйнування збройних сил та поширення конфіденційної інформації [1]. Кібератаки на критичну інфраструктуру, таку як енергетичні мережі, можуть призвести до масштабних відключень електропостачання, відсутності гарячої води та колапс транспортної системи, що може вплинути на життя тисяч людей [2].

Все це свідчить про важливість розуміння і запобігання кібератакам на державну, військову та практичну інфраструктуру. Необхідною умовою ефективного захисту є розуміння сучасних загроз та розробка заходів для забезпечення безпеки інфраструктури від кібератак.

II. Методика дослідження.

У даному дослідженні використаний аналітичний метод, який полягає у зборі та аналізі відповідної інформації про кібератаки на державну, військову та практичну інфраструктуру. Для цього використані наукові джерела, зокрема статті та дослідження відомих експертів у галузі кібербезпеки, таких як Брюс Шнайер, а також нормативні документи, такі як ISO/IEC 27000:2018.

Також використані документи від урядових та військових організацій, таких як U.S. Department of Defense, що містять відомості про кібератаки на державну та військову інфраструктуру. Проаналізовані статистичні дані про кількість кібератак за останні роки, що надається організаціями, такими як Panda Security та Cloudflare.

Для оцінки наслідків кібератак на практичну інфраструктуру проаналізовані звіти з моніторингу критичних систем, що проводяться відповідними організаціями, а також дані про пропущені відправлення чи затримки в роботі транспортних засобів та інших систем, що можуть бути піддались кібератакам [3].

Отже, метою тез доповіді є аналіз проявів кібератак на державну, військову та критичну інфраструктуру.

III. Аналіз проявів кібератак на державну, військову та критичну інфраструктуру.

Аналіз наслідків кібератак на державну, військову та критичну інфраструктуру свідчить про те, що ці напади можуть мати серйозні наслідки для безпеки та функціонування інфраструктури. Наприклад, кібератаки на енергетичні системи можуть призвести до відключення електропостачання, яке може

відбутися на значні терміни, порушивши роботу різних підприємств та населення. Кібератаки на банки можуть спричинити втрату грошей користувачів та навіть привести до краху фінансової системи. Кібератаки на системи зв'язку можуть призвести до втрати зв'язку, що збільшує ризик виникнення надзвичайних ситуацій та ускладнює координацію дій рятувальних служб.

Крім того, кібератаки на військову інфраструктуру можуть привести до втрати контролю над зброєю та ураження важливих військових об'єктів. Наприклад, у 2007 році Російська Федерація провела кібератаку на Естонію, яка мала на увазі призупинити роботу естонської інтернет-інфраструктури та завадити роботі уряду. Це призвело до великих збитків у естонської економіці та негативно позначилося на міжнародних відносинах [4].

Аналіз наслідків кібератак на критичну інфраструктуру також показує серйозні ризики. Кібератаки на системи зв'язку можуть призвести до зупинки роботи інтернет-сервісів та соціальних мереж, що забезпечують комунікацію мільйонів людей. Кібератаки на електронні системи голосування можуть призвести до порушення виборчого процесу та підірвати довіру до демократичних інститутів. Кібератаки на фінансову інфраструктуру можуть призвести до викрадення грошових коштів та збитків для банків та інших фінансових установ. Кібератаки на промислові системи керування можуть призвести до зупинки виробничих процесів та зниження продуктивності підприємств. Наслідки кібератак можуть бути надзвичайно серйозними та потенційно небезпечними для життя та здоров'я людей, зокрема, при атаках на системи керування транспортними засобами або медичні прилади [4, 5].

Згідно з дослідженням, проведеним компанією Cybersecurity Ventures, до 2025 року загальний обсяг збитків, пов'язаних з кіберзлочинністю, може скласти більше 10,5 трильйонів доларів [6], що становить надзвичайно високий ризик для економічної та соціальної стабільності в світі. У своїх дослідженнях, також вказують на те, що кібератаки на критичну інфраструктуру можуть мати далекосяжні наслідки, такі як руйнування міжнародних відносин та зростання політичної нестабільності.

Дослідження, проведені спеціалістами з кібербезпеки, також показують, що держави є одними з найбільш вразливих об'єктів кібератак. За даними компанії Accenture, більше половини країн світу мають недостатній рівень кіберзахисту. Крім того, згідно з дослідженнями фірми McAfee, державні організації є найчастішою метою кібератак. У 2020 році було зафіксовано 23 % більше кібератак на державні структури, ніж у 2019 році. Також становлення кіберармій в деяких країнах та конфлікти між ними можуть призвести до зростання кількості кібератак на державні об'єкти [7].

Рівень підготовки інфраструктури до захисту від кібератак залежить від країни та галузі, однак загалом можна зробити висновок, що він є недостатнім. Деякі держави та організації активно працюють над захистом своєї

інфраструктури від кібератак, використовуючи сучасні методи та технології. Однак, за даними дослідження компанії Accenture, понад 75 % урядів та компаній недостатньо підготовлені до виявлення та відповіді на кібератаки. Більшість держав зосереджуються на захисті своїх критичних інфраструктур, таких як енергетика, транспорт та комунікації, але недостатньо уваги приділяється захисту менш важливих систем, таких як медичні заклади та освітні установи.

У разі кібератак на державну інфраструктуру, можуть бути порушені процеси влади та управління країною. Кібератаки на військову інфраструктуру можуть призвести до порушення функціонування військових систем та забезпечення безпеки держави. Кібератаки на практичну інфраструктуру, таку як енергетика, транспорт та комунікації, можуть призвести до перерв у роботі цих систем та негативно вплинути на життя мільйонів людей.

Загалом, кібератаки можуть мати серйозні наслідки для функціонування інфраструктури та впливати на життя мільйонів людей. Попередження та ефективна відповідь на кібератаки є важливими завданнями для держав та організацій, щоб забезпечити захист від цих загроз [8].

Висновки. Згідно з проведеним дослідженням, кібератаки стали дедалі більш поширеними та складними, а їх наслідки можуть бути катастрофічними для інфраструктури, що є найбільш вразливими об’єктами кібератак. При цьому, державна, військова та практична інфраструктури виявилися особливо чутливими до кіберзагроз, оскільки їх робота має важливе значення для безпеки та економіки країни.

Незважаючи на те, що інфраструктура постійно піддається кібератакам, її рівень підготовки до захисту залишається недостатнім. Багато компаній та держав не забезпечують достатній рівень захисту, і це може призвести до значних втрат. Для того, щоб зменшити ризик кібератак, потрібно посилити заходи захисту та збільшити увагу до кібербезпеки.

Отже, ураховуючи високий рівень загроз, пов’язаних з кібербезпекою, державам, компаніям та іншим суб’єктам інфраструктури потрібно приділити належну увагу кіберзахисту та забезпечити достатній рівень захисту від кібератак. Для досягнення цього мети потрібно враховувати найновіші тенденції та розробляти ефективні стратегії захисту від кіберагресії.

Література

1. Richard Kissel. Glossary of Key Information Security Terms / National Institute of Standards and Technology P. 222 pages (May 2013).

2. CNSSI 4009: Committee on National Security Systems (CNSS) Glossary March 2, 2022

3. International Organization for Standardization. (2018). ISO/IEC 27000:2018 – Information technology – Security techniques – Information security management systems – Overview and vocabulary.

4. Шелест, В. (2016). Інфраструктура: теорія та практика створення. Київ: НАН України.
5. Panda Security. (2022). Cyber Attacks: Types, Examples and Prevention. Retrieved from https://www.pandasecurity.com/en/security-info/what-is-a-cyber-attack/
6. Cloudflare. (2022). What is a DDoS Attack? Retrieved from https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/
7. Symantec Corporation. (2022). What is a Virus? Retrieved from https://www.symantec.com/security-center/virus-definitions/what-is-a-virus
8. Schneier, B. (2018). The security risks of voting online. Communications of the ACM, 61(3), 27-29.

Титов В.М.
Ситник С.С.
Національна академія СБ України

ДО ПИТАННЯ ЗАРУБІЖНОГО ДОСВІДУ РОЗВІДКИ НА ОСНОВІ ВІДКРИТИХ ДЖЕРЕЛ OSINT: ОРГАНІЗАЦІЙНИЙ АСПЕКТ

У реаліях сьогодення соціальні мережі та різноманітна онлайн-активність дозволяє застосовувати безліч легальних розвідок OSINT. Критеріями пошуку може бути профіль людини, його ім’я, сфера діяльності організації або назва компанії. Тому актуальність питань розвідки на основі відкритих джерел OSINT під час дії правового режиму в Україні, набуває окремого значення.

Так, на сьогодні існують різні методи збирання інформації, що використовуються комплексно або окремо. Одним із таких є розвідка з відкритих джерел. Розвідка на основі відкритих джерел, яку ще називають Open source intelligence (OSINT), – є однією з розвідувальних навчальних дисциплін. Вона включає в себе пошук, вибір і збирання інформації, отриманої із загальнодоступних джерел, та її аналіз.

Також OSINT асоціювався виключно з поняттям «конкурентна розвідка», але після 24 лютого 2022 р. цей термін отримав нового значення. Фотографії з супутників, ідентифікація воєнних злочинів по відео, розслідування терактів – все це стало новим етапом для українських OSINT’ерів [1].

У розвідувальному співтоваристві термін «відкритий» вказує на загальнодоступність джерела (на відміну від секретних джерел та джерел з обмеженим використанням), він не пов’язаний із поняттям open source (відкрите програмне забезпечення) або public intelligence (громадська розвідка). За твердженнями аналітика ЦРУ Шермана Кента, висловленими у 1947 р., політики отримують до 80 % інформації, необхідної їм для прийняття рішень у мирний час із відкритих джерел.

Специфічна категорія технічних і людських ресурсів, джерела інформації і методи їх збирання – все це відрізняє OSINT від інших видів розвідки. Перевагами OSINT, на відміну від інших видів розвідки, є доступність джерел інформації, обсяг джерел інформації, різносторонність, оперативність отримання, легкість подальшого використання та вартість.

Відкриті джерела інформації вивчаються у всіх країнах світу, які приділяють увагу розвідці. Але організована ця робота в кожній країні по-різному. Так, наприклад, в Австралії головним експертом щодо відкритих джерел визначено Управління національних оцінок, яке офіційно є однією з розвідувальних держструктур. У Великій Британії існує інформаційна служба «BBC Monitoring», зусилля якої зосереджені лише на збиранні доступної інформації силами працюючих тут цивільних журналістів.

Якщо мову вести про Ізраїль, то у структурі воєнної розвідки «Аман» створений спеціальний підрозділ «Хатсав», який займається тільки відкритими джерелами інформації. Завданнями «Хатсав» є збирання інформації через електронну пресу, включаючи інтернет та інші джерела, винятково для військових цілей [2, с. 146].

Отже, OSINT охоплює дані, які можна шукати на різних видах ресурсів. Окрім тексту - це фото-, відео контент, матеріали з вебінарів, публічних зборів, конференцій. Утім, для здійснення оперативно-розшукової та контррозвідувальної діяльності цього недостатньо. Важливу роль також відіграє інформація, яка надходить від оперативних джерел, що свідчить про важливість організації роботи вітчизняних спецслужб з підбору, навчання, використання та їх мотиваційної складової.

Ураховуючи викладене, можна констатувати, що інформація отримана з відкритих та оперативних джерел є взаємодоповнюючою для прийняття раціональних управлінських рішень із забезпечення національної безпеки України.

Література

1. OSINT: навіщо вивчати та які перспективи. [Електронний ресурс] – Режим доступ:ain.ua/2022/12/14/osint-navishho-ta-yaki.

2. Подолянчук Р. І. Аналітична розвідка в мережі Інтернет як метод інформаційно-аналітичного забезпечення діяльності спецпідрозділів БОЗ / Р. І. Подолянчук // Організація і тактика документування підрозділами ДСБЕЗ злочинів у комп’ютерних мережах електрозв’язку : матеріали Всеукр. наук.-практ. конф., (Донецьк, 4 груд. 2009 р.). – Донецьк, 2009. – С. 145-147.

Толюпа С.В.
д.т.н., професор,
Пампуха І.В.
Шевченко А.М.
Київский національний університет ім. Тараса Шевченка

ІНТЕЛЕКТУАЛЬНИЙ ПІДХІД ПРИ ПОБУДОВІ СИСТЕМ ВИЯВЛЕННЯ АТАК

Основним засобом захисту інформаційних систем та мереж (ІСМ) від інформаційно-руйнівних впливів (втручань) у вигляді кібернетичних вторгнень (КВ) є системи виявлення та/або запобігання вторгненням (СВВ/СЗВ/СВА), основна задача яких зводиться до оперативної їх ідентифікації (встановлення відповідності між об'єктом і його ідентифікатором (унікальним атрибутом) та в ідеальному випадку ініціювання ефективного захисного сценарію щодо припинення факту порушення конфіденційності, доступності та цілісності інформаційних ресурсів, сервісів. На сьогодні системи виявлення вторгнень і атак зазвичай являють собою програмні або апаратно-програмні рішення, які автоматизують процес контролю подій, що відбуваються в інформаційній системі або мережі, а також самостійно аналізують ці події в пошуках ознак проблем безпеки. Оскільки кількість різних типів і способів організації несанкціонованих проникнень в чужі мережі за останні роки значно збільшилася, системи виявлення атак (СВА) стали необхідним компонентом інфраструктури безпеки більшості організацій.

Найбільш ефективним способом запобігання несанкціонованому використанню інформаційних систем і мережевих ресурсів є підтримка багаторівневого захисту, коли спільно використовуються міжмережеві екрани, системи виявлення вторгнень, системи аудиту, політика безпеки і інші засоби захисту.

Найбільш загальна структура системи виявлення вторгнень, розроблена групою дослідників CIDF (Common Intrusion Detection Framework) [4], представлена на рис. 1.

Блок збору даних (сенсор, Event-box) - аналізує дані для обробки та прийняття рішення аналізатором. У даних можуть міститися імена контрольованих параметрів, їх особливості та значення. Сенсор може виконувати перетворення даних для перетворення в необхідний формат або для скорочення обсягу даних, що передаються.

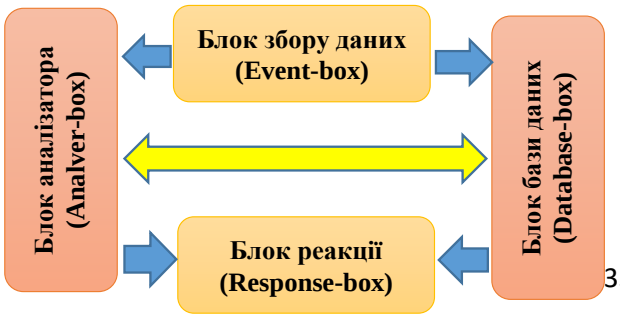


Рис. 1. Загальна структура системи виявлення вторгнень

Блок аналізатора (Analyzer-box) - приймає рішення про наявність або відсутність ознак атаки або аномалії на підставі даних від сенсорів. В рамках аналізу даний блок може виконувати

функції фільтрації, нормалізації, перетворення і кореляції даних. При виявленні атаки блок аналізатора може додати до вихідних даних опис виявленої атаки. Блок аналізатора може мати багаторівневу систему.

Блок бази даних (сховище даних, Database-box) - містить множини вирішальних правил і семантичний опис атак, а також накопичувальну інформацію від сенсорів. Дані можуть перебувати в текстових файлах, базі даних, і т.д.

Блок реакції (Response-box) - інформує адміністратора про зафіксовану атаку, а в випадку системи запобігання вторгнень формує активну реакцію. Системи запобігання вторгнень відстежують активність в режимі реального часу і швидко реалізовують дії щодо запобігання атак. Можливі заходи - блокування потоків трафіку в мережі, скидання з'єднань, видача сигналів оператору. Також системи запобігання вторгнень можуть виконувати дефрагментацію пакетів, упорядкування пакетів TCP для захисту від пакетів з зміненими номерами послідовності і підтвердження.

Системи виявлення мережевих атак збирають інформацію з пакетів мережевого трафіку, системних журналів і показників функціонування системи. Традиційні системи виявлення мережевих атак будуються на сигнатурному підході: за допомогою набору правил або сигнатур, що формуються експертами і розміщені в базу вирішальних правил, описуються всі можливі сценарії і особливості атак. У цього підходу існує безліч відомих недоліків. За допомогою аналізу сигнатур неможливо виявити нові види атак, тому що база вирішальних правил не містить інформації про відповідну атаці. Процес аналізу сигнатур для розподілених атак є вкрай складним завданням. Крім того, бази вирішальних правил популярних систем виявлення вторгнень практично є загальнодоступними, тому порушник може протестувати можливості приховування атаки.

Перераховані проблеми підходу пошуку сигнатур змушують фахівців шукати альтернативні шляхи для організації захисту від мережевих атак. Одним з популярних напрямків досліджень є застосування різних методів Data Mining в системах виявлення мережевих атак [5]. Data mining (інтелектуальний аналіз даних, глибинний аналіз даних) - сукупність методів виявлення в даних раніше невідомих, нетривіальних, практично корисних і доступних інтерпретації знань, необхідних для прийняття рішень в різних сферах людської діяльності. В основі даних методів лежить припущення, що вся легітимна активність в системі може бути представлена у вигляді математичної моделі. Методи, які застосовуються для виявлення мережевих атак методи Data Mining переслідують одну з наступних цілей: виявлення порушень; виявлення аномалій.

Перші моделюють атаки і застосовують засоби класифікації, другі моделюють нормальну поведінку і виконують пошук винятків.

При використанні методів Data Mining для виявлення мережевих атак можна виділити наступні проблеми: дані, аналізовані системами виявлення, мають

високу розмірність і обсяг; вимога обробки даних в режимі реального часу; велика кількість шумів і невідповідностей в даних, що обробляються що викликають неадекватну реакцію методів інтелектуального аналізу даних.

Звичайно протидіяти вторгненням і атакам основуючись тільки на одному з методів Data Mining малоефективно, тому необхідно підійти до цього питання комплексно і побудувати інтелектуальну систему протидії вторгненням (рис. 2). При побудові такої інтелектуальної (експертної) системи пропонується вибрати нечітку модель. Це пов'язано з тим, що значна частина інформації про причини і джерела атак може бути отримана тільки експертним шляхом або у вигляді евристичних описів процесів. Для визначення джерел атак система безпеки має бути представлена моделлю тієї інформаційної мережі на яку вона орієнтується. Данна модель ділить завдання переміщення інформації між комп'ютерами через середовище мережі на кількість рівнів менш великих і легше вирішуваних підзадач. Кожна з цих підзадач вирішується за допомогою одного рівня мережі. Тому первинне завдання після фахівця безпеки може бути представлене декомпозицією завдань безпеки по окремих рівнів мережі.

Комплексна інтелектуальна система підтримки прийняття рішень (ІСППР) для визначення вторгнень містить набір функціональних компонент, що дозволяють максимально автоматизувати і прискорити вироблення дій, що управляють, при зміні ситуації в системі безпеки (рис. 2).

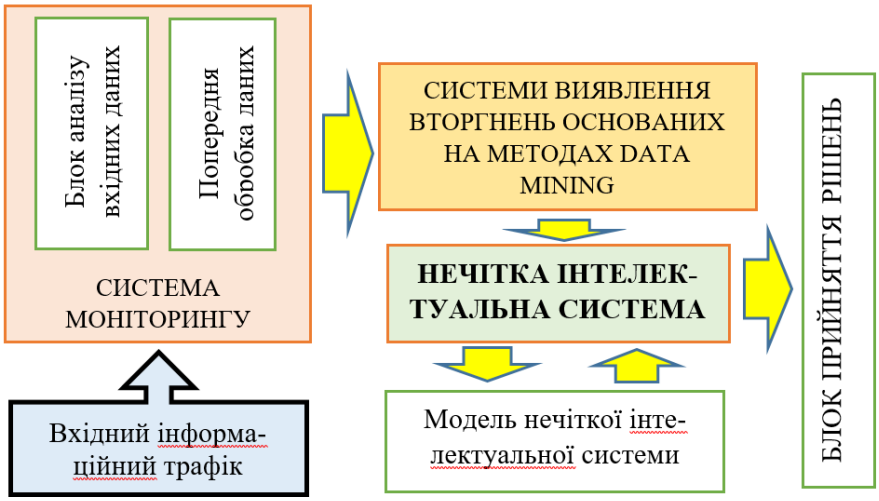


Рис. 2. Структура інформаційної системи прийняття рішення для визначення вторгнень

Сучасний підхід до побудови систем виявлення атак на інформаційні системи сповнений недоліків і вразливостей, що дозволяють, на жаль, шкідливим впливам успішно долати системи захисту інформації. Перехід від пошуку сигнатур атак до виявлення передумов виникнення загроз інформаційної безпеки має сприяти тому, щоб докорінно змінити дану ситуацію, скоротивши дистанцію відставання в розвитку систем захисту від систем їх подолання. Крім того, такий перехід має

сприяти підвищенню ефективності управління інформаційною безпекою і, нарешті, більш конкретних прикладів застосування нормативних і керівних документів, що вже стали стандартами.

Проведене імітаційне моделювання та застосування інтелектуальної системи підтвердило правильність вибору множини методів Data Mining в якості побудови систем виявлення вторгнень. Так метод опорних векторів дозволив ідентифікувати більшість атак з результатом 98-100%. Метод головних компонент скоротив обсяг інформації, необхідної для класифікації мережевих пакетів, і підвищив швидкість формування модулів виявлення, але виявив проблему перенавчання. Методи кластеризації дозволили сформувати безліч модулів виявлення, виділивши типові фрагменти атак в окремі модулі виявлення і розбивши комплексні атаки на окремі модулі. Застосування нечіткої логіки підвищило результати роботи системи і дозволило класифікувати вектори, що мають різні мітки в навчальній вибірці.

Література

1. Субач І.Ю., Фесьоха В.В. Модель виявлення аномалій в інформаційно – телекомунікаційних мережах органів військового управління на основі нечітких множин та нечіткого логічного виводу. Збірник наукових праць ВІТІ № 3 – 2017

2. І.М. Павлов, С.В. Толюпа, В.І. Ніщенко Аналіз таксономії систем виявлення атак у контексті сучасного рівня розвитку інформаційних систем. Сучасний захист інформації №4, 2014,с. 44-52

3. Зоріна Т.І. Системи виявлення і запобігання атак в комп'ютерних мережах. Вісник східноукраїнського національного університету імені Володимира Даля № 15 (204) ч.1 2013. – с. 48-54.

4. Толюпа С.В. Системи виявлення вторгнень та функціональна стійкість розподілених інформаційних систем до кібернетичних загроз / Лукова-Чуйко Н.В., С.В. Толюпа, В.С. Наконечний, Браіловський М.М.: монографія - К.: Формат, 2021. – 407 с.

Форноляк В.М.
к.п.н., доцент,
Національна академія СБ України

ОРГАНІЗАЦІЙНО-ПРАВОВІ ОСНОВИ ЗАБЕЗПЕЧЕННЯ КІБРЕНЕТИЧНОЇ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ВОЄННОГО СТАНУ

Наразі для всього цивілізованого світу безпрецедентним є виклик здійснення російською федерацією (далі – рф) збройної агресії та нападу на Україну, котрий супроводжується багаточисленними обстрілами та знищенням об'єктів критичної

інфраструктури. У зв'язку з військовим вторгнення збройних сил рф на територію незалежної та суверенної України, Указом Президента України від 24.02.22 р. № 64 в на всій території держави введено воєнний стан. Зазначеним правовим актом передбачається надання відповідним органам державної влади, військовому командуванню, військовим адміністраціям та органам місцевого самоврядування повноважень, необхідних для відвернення загрози, відсічі збройної агресії та забезпечення національної безпеки [1].

Від початку воєнних дій фіксується збільшення кількості та інтенсивності кібератак, що здійснюються на об'єкти критичної інфраструктури в Україні. Через мережу Інтернет зазнають кібератак сервери державних установ, фінансові установи, промислові підприємства, інформаційно-телекомунікаційна інфраструктура воєнних об'єктів тощо.

Слід також зазначити, що Україна через своє географічне розташування тісно взаємодіє з енергетичною та транспортною інфраструктурою країн-членів Європейського Союзу та є невіддільним елементом глобального кіберпростору. Тому слід усвідомити, враховуючи нинішні геополітичні реалії, зокрема, газотранспортна чи електроенергетична система України може сприйматися європейськими та трансатлантичними партнерами як частина критичної інфраструктури загальноєвропейського значення.

За таким обставин невідкладними постають питання правового врегулювання у сфері забезпечення безпеки об'єктів критичної інфраструктури в Україні, зокрема забезпечення кібернетичної безпеки зазначених об'єктів. Водночас зауважимо, що вирішення таких питань ускладняються через бойові дії, чисельні ракетні обстріли тощо.

Враховуючи положення Стратегії забезпечення державної безпеки (далі – Стратегія), що затверджена Указом Президента України від 16.02.22 р. № 56/20, об'єктами державної безпеки є об'єкти критичної інфраструктури. У вказаному документі позначається тенденція щодо посилення загроз для критичної інфраструктури у зв'язку з тимчасовою окупацією частини території України, гібридними впливами, що здійснюються з боку російських ЗМІ, погіршенням технічного стану об'єктів інфраструктури, недостатністю інвестицій для її оновлення та розвитку, намаганням несанкціонованого втручання в її діяльність, зокрема фізичного і кіберхарактеру (п. 19), а також триваючими бойовими діями (п. 27) [2].

У Стратегії задекларовано, що держава: створить ефективну систему безпеки та стійкості об'єктів критичної інфраструктури, що ґрунтується на чіткому розподілі відповідальності її суб'єктів та державно-приватного партнерства [2].

Згідно з чинним законодавством відповідальність за функціонування і забезпечення безпеки системи критичної інфраструктури покладається на наступні органи державної влади: Службу безпеки України, Антитерористичний центр при СБ України, Національну комісію з питань захисту критичної інфраструктури, Державну службу із надзвичайних ситуацій, Державну інспекцію

ядерного регулювання України, Національну поліцію, Національну гвардію, Генеральний штаб ЗС України, Державну прикордонну службу, Державну службу спеціального зв'язку та захисту інформації [3]. У зв'язку зі збільшенням кількості хакерських атак на об'єкти критичної інфраструктури, зокрема в нинішніх умовах воєнного стану стратегічного характеру набувають питання кібернетичного захисту об'єктів критичної інфраструктури.

На сьогодні в правовому полі України прийнято низку правових актів, котрі унормовують питання забезпечення безпеки об'єктів критичної інфраструктури. Проте варто відмітити, що недостатньо опрацьованими залишаються питання управління захистом та безпекою таких об'єктів, трапляються епізоди дублювання функцій уповноваженими органами, а загрози стосовно зазначених об'єктів опрацьовуються переважно в «відомчому» розрізі. Такі обставини вказують на необхідність запровадження на державному, регіональному та галузевому рівнях низки конститутивних заходів щодо: правового та організаційного регулювання; координації та взаємодії органів державної влади у вирішення питань забезпечення ресурсами систем державної безпеки та захисту; спільного впровадження відповідних безпекових заходів.

Варто відзначити, що на сьогодні в нашій державі функціонують три осібні системи, що регламентують питання забезпечення безпеки та захисту об'єктів критичної інфраструктури: Єдина система запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків (Положення про яку затверджено постановою Кабінету Міністрів України від 15.08.07 р. № 1051); Єдина державна система цивільного захисту населення і територій (Закон України «Про правові засади цивільного захисту» від 24.06.04 р. № 1859-IV); Єдина державна система запобігання і реагування на надзвичайні ситуації техногенного та природного характеру (Положення про яку затверджено постановою Кабінету Міністрів України від 03.08.98 р. № 1198, зі змінами від 29.07.99 р. № 1376, від 09.08.01 р. № 1006, від 15.05.03 р. № 717, від 04.09.03 р. № 1402, від 08.12.06 р. № 1700).

Вказані «системи» розроблені, зокрема, для забезпечення безпеки життєво-важливих об'єктів держави від різних видів загроз, зокрема також кібернетичних. Вони функціонують незалежно одна від одної, що вказує на домінування відомчих підходів щодо вирішення безпекових питань національного масштабу. Водночас слід засвідчити, що за таких умов імовірне дублювання функцій уповноваженими органами та поява неузгодженостей у питаннях поділу повноважень щодо забезпечення безпеки зазначених об'єктів. Специфічної уваги вимагає рішення таких питань в умовах воєнного стану, у зв'язку з цим потребують ретельного опрацювання діючі концепції забезпечення безпеки об'єктів критичної інфраструктури України.

Наразі затверджено низку важливих правових актів, котрі регламентують засади державної політики в питаннях забезпечення безпеки об'єктів критичної інфраструктури та забезпечення їхньої кібернетичної безпеки, зокрема: Закон

України «Про критичну інфраструктуру» від 16.11.2021 № 1882 IX; Постанови КМУ: від 09.10.2020 № 943 «Деякі питання об'єктів критичної інформаційної інфраструктури»; від 09.10.2020 № 1109 «Деякі питання об'єктів критичної інфраструктури»; від 19.06.2019 № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» та Рішення Правління Національного банку України від 20.04.2021 № 148 «Про об'єкти критичної інфраструктури в банківській системі України» та інші.

Водночас слід зазначити, що чинна правова база у сфері забезпечення кібернетичної безпеки об'єктів критичної інфраструктури, зокрема в умовах воєнного стану є недостатньою. Проте зауважимо, що в Законі України «Про основні засади забезпечення кібербезпеки України» сформульовано поняття «об'єкта критичної інфраструктури», визначено повноваження для переліку таких об'єктів, але не охарактеризованими є критерії ідентифікації таких об'єктів.

З метою удосконалення правового регулювання питань забезпечення кібернетичної безпеки об'єктів критичної інфраструктури прийнятий Закон України «Про критичну інфраструктуру та її захист», котрий набув чинності з 15.06.22 р. [4], у якому визначено головні терміни, принципи та засади діяльності органів державної влади у цій сфері.

Таким чином, насущними питаннями правого регулювання забезпечення безпеки об'єктів критичної інфраструктури в умовах воєнного стану є започаткування державної системи кібернетичної безпеки об'єктів критичної інфраструктури, впровадження єдиних підходів щодо організації управління такими об'єктами як на державному так й на місцевому рівнях, опрацювання правового регулювання взаємодії відповідних органів державної влади в питаннях забезпечення безпеки об'єктів критичної інфраструктури.

Прийняття закону котрий унормує правовідносини у сфері забезпечення кібернетичної безпеки об'єктів критичної інфраструктури сприятиме формуванню єдиної загальнодержавної системи у цій сфері.

Потребує також вирішення питання щодо створення єдиної державної системи попередження та протидії кібернетичним атакам на об'єкти критичної інфраструктури України, оцінки рівня її захищеності, організації діяльності сил та засобів які виявлятимуть та попереджуватимуть кібератаки.

Література

1. Про введення воєнного стану в Україні. Указ Президента України від 24 лютого 2022 року № 64/2022. Документ 64/2022, чинний, поточна редакція — Редакція від 18.11.2022, підстава - 757/2022. URL: https://zakon.rada.gov.ua/laws/show/64/2022#Text (дата звернення 15.03.2023).

2. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки: затверджено Указом Президента України від 16.02.22 р. № 56//2022. Документ 56/2022, чинний,

поточна редакція — Прийняття від 16.02.2022. URL: https://zakon.rada.gov.ua/laws/show/56/2022#Text (дата звернення 15.03.2023).

3. Захист об'єктів критичної інфраструктури. URL: https://ssu.gov.ua/zakhystobiektiv-krytychnoi-infrastruktury (дата звернення: 14.02.2023).

4. Про критичну інфраструктуру: Закону України від 16 листопада 2021 року № 1882-IX. Документ 1882-IX, чинний, поточна редакція — Редакція від 05.12.2022, підстава - 2664-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення 15.03.2023).

Худинцев М.М.
к.ф.-м.н., доцент,
Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України
Хоменко О.А.
аспірант
Інститут телекомунікацій і глобального інформаційного простору
НАН України

ЗАСТОСУВАННЯ ІНДЕКСІВ КІБЕРБЕЗПЕКИ ДЛЯ ОЦІНКИ СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРАСТРУКТУРИ В УМОВАХ ВІЙСЬКОВОГО ЧАСУ

Кількісне вимірювання показників національної секторальної (галузевої) інформаційної безпеки та кібербезпеки лише останнім часом присвячені чисельні публікації (наприклад, [1-5]). До загальновідомих індексів належать, наприклад, Глобальний індекс кібербезпеки GCI Міжнародного союзу електрозв'язку та Національний індекс кібербезпеки NSCI Академії електронного управління (м.Таллінн) [5].

Суб'єктами індексування у залежності від типу індексу є країни, галузі (сектори) економіки, корпорації та організації. Об'єктами індексування є процеси діяльності цих суб'єктів у відповідних сферах, стан безпеки та рівень захищеності цих суб'єктів від загроз безпеки, а також окремі показники безпеки та захищеності.

Класифікація індексів кібербезпеки за типами, категоріями, організацією доступу та іншими показниками зроблено у [5].

У військовий час велику увагу привертають індекси, які оцінюють стан галузевої (секторальної) безпеки, а також кібероборони окремих країн. Предметом дослідження були мережеві індекси (рейтинги) кібербезпеки та Національний індекс сил кібербезпеки (або Індекс кіберпотужності) (релізи 2022-го року), наведені у табл.1.

Таблиця 1

Світові індекси (рейтинги) кібербезпеки (для оцінки стану безпеки критичної інфраструктури)

Індекс			Видавець		
Назва	Name	Abbr.	Назва	Abbr.	Країна
Автоматизована незалежна платформа оцінювання безпеки	Automate Third-Party Security Rating Platform	A3SRP	Panorays	PNR	США
Рейтингова платформа кіберризиків Black Kite	Black Kite Cyber Risk Ratings Platform	BKCRRP	Black Kite Inc.	BKI	США
Платформа рейтингів безпеки BitSight	BitSight Security Ratings Platform	BSSR	BitSight Technology LTD	BST	США
Індекс кібервпливу	Cyber Exposure Index	CEI	Cyber Intelligence House	CIH	Сінгапур
Індекс Cyber Green	Cyber Green Index	CGI	Cyber Green Institute	CGI	США
Національний індекс сил кібербезпеки	National Cyber Power Index	NCPI	Belfer Centre Harvard University	BCH	Великобританія
Монітор загроз Prevalent	Prevalent Vendor Threat Monitor	PVTM	Prevalent Inc.	PRV	США
Рейтинги кібербезпеки RiskRecon	Risk Recon Cybersecurity Ratings	RRCR	Risk Recon Co.	RRC	США
Платформа рейтингів Security Scorecard	Security Scorecard Ratings Platform	SSR	Security Scorecard Co.	SSC	США
Платформа рейтингів UpGuard	UpGuard Ratings Platform	UGR	UpGuard Inc.	UGI	США

Предмет та об’єкт індексування (рейтингування) визначається окремо для кожного індексу. Вплив особливостей військового часу на показники ризиків досліджується шляхом порівняння з аналогічними показниками у мирний час.

Таблиця 2. Світовий рейтинг кіберпотужності у 2020 та 2022 роках

Місце	2020 рік	2022 рік
1	США	США
2	КНР	КНР
3	Великобританія	Росія
4	Росія	Великобританія
5	Нідерланди	Австралія
6	Франція	Нідерланди
7	Німеччина	Південна Корея
8	Канада	В’єтнам
9	Японія	Франція
10	Австралія	Іран
…	…	…
12	Іспанія	Україна
…	…	…
26	Україна	Індія

Окремо досліджується питання про застосування до процедури зменшення ризиків технології страхування операційних ризиків у кіберпросторі з використанням заходів з резервування функціоналу і зобов’язань, а також технологічних і бізнес-процесів.

Використання окремих індексів для оцінки галузевих (секторальних) суб’єктів дозволяє: - отримати якісну і кількісну картину стану інформаційної безпеки (кібербезпеки, кіберзахисту) суб’єкта та галузі в цілому; - провести порівняння неоднорідних суб’єктів; - порівняти з результатами індексування результати інших досліджень стану безпеки, отримані з використанням існуючих технічних рішень (засобів) захисту; - визначити характер та динаміку змін ризиків та загроз безпеки, ефективність заходів захисту.

Література

1. Кібербезпека енергетики, науково-практична конференція Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук

України : матеріали, 27 травня 2022 р. / Київ : ІПМЕ ім. Г.Є.Пухова НАН України, 2022. 128 с.

2. Оцінка стійкості енергетичної інфраструктури України : аналітичний звіт / Павленко О., Антоненко А., Ніцович Р., Євтушок С., Суходоля О. Київ : ГО «Діксі Груп», 2022. 72 с.

3. Потій О., Семенченко А., Дубов Д., Бакалинський О., Мялковський Д. Концептуальні засади впровадження організаційно-технічної моделі кіберзахисту України. *Захист інформації*. 2021. Т.23, №1. С.47-60.

4. Boyarchuk R., Khudyntsev M., Lebid O., Trofymchuk O. Organizational and Technical Model of National Cybersecurity and Cyber Protection, Workshop on Cybersecurity Providing in Information and Telecommunication Systems, Kyiv, Ukraine, CPITS'2021. *CEUR Workshop Proceedings*. 2021. Vol. 2923, P. 37–46.

5. Худинцев М.М., Жилін А.В., Давидюк А.В. Світові індекси кібербезпеки: огляд та методики формування (Глобальний звіт / Каталог) : монографія. Київ : Міжнародний університет кібербезпеки, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, 2021. 240 с. ISBN 978-966-136-887-2.

Цюцюра М.О.
Національна академія СБ України

ПРОБЛЕМИ ПРОТИДІЇ КІБЕРНЕТИЧНИМ АТАКАМ рф НА ОБ'ЄКТИ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Кібербезпека стала однією з найбільш актуальних тем останніх років. Сучасні технології і зв'язана з ними залежність людей від Інтернету і комп'ютерних мереж роблять інформаційну інфраструктуру суспільства дедалі більш вразливою до кібератак. Водночас, Росія стала однією з найбільш агресивних держав у сфері кібербезпеки, що викликає серйозні збої в роботі критичної інформаційної інфраструктури (КІІ) інших держав.

Протидія кібернетичним атакам рф на об'єкти критичної інформаційної інфраструктури є актуальною проблемою для багатьох країн світу. Зокрема, за даними ФБР та Міністерства внутрішніх справ США, росія здійснювала спроби зламати інформаційні системи американських компаній та державних установ, включаючи виборчі системи, що може порушити роботу цілого суспільства. Такі напади можуть викликати відключення електропостачання, водопостачання, транспортну кризу та інші небезпеки.

Однією з головних причин вразливості інформаційної інфраструктури є застарілість програмного та апаратного забезпечення, використання застарілих протоколів і нестача висококваліфікованих фахівців з кібербезпеки. Ці проблеми потребують системних рішень, таких як модернізація інфраструктури та

встановлення сучасних систем захисту, розробка та виконання планів реагування на кібератаки, підготовка фахівців з кібербезпеки тощо.

Однією з проблем у протидії кібернетичним атакам рф на об'єкти КІІ є складність виявлення та аналізування таких нападів. Кіберзлочинці можуть здійснювати атаки з різних країн, за допомогою різних методів, в тому числі через використання ботнетів, фішингових атак, використання програмного забезпечення з вразливостями та інших методів. Це може призвести до того, що країни не можуть вчасно виявити та відповісти на кібернетичні загрози.

Іншою проблемою є необхідність підвищення кібербезпеки об'єктів КІІ. Багато країн, зокрема ті, що стали об'єктом кібератак рф, визнають, що їх системи захисту є недостатньо ефективними. Більшість об'єктів КІІ побудовані за допомогою застарілої техніки та програмного забезпечення з відомими вразливостями.

Україна – країна, яка зіткнулася з великою кількістю кібернетичних загроз від російської федерації, особливо під час повномасштабного вторгнення. Оскільки об'єкти критичної інформаційної інфраструктури (ОКІІ) є важливими для функціонування держави та її громадян, захист цих об'єктів є надзвичайно важливою задачею для уряду та керівництва України. Проте, існують ряд проблем, які перешкоджають ефективній протидії кібернетичним атакам рф на ОКІІ України.

Основні проблеми, що виникають під час реагування на інциденти:

- На даний момент, не встановлено, хто буде нести відповідальність за захист ОКІІ України від кібернетичних атак. Це може призвести до ситуації, коли кожен відділ та агенція відповідає за свою частину, але ніхто не відповідає за загальну безпеку.

- Наступна проблема полягає в недостатньому розумінні кібербезпеки в окремих ОКІІ. У багатьох випадках, керівники ОКІІ не мають достатнього розуміння про кібербезпеку та її важливість для їх роботи. Це може призвести до неправильного використання технологій та програм, які не забезпечують належного рівня кібербезпеки, що створює потенційну загрозу для ОКІІ.

- Відсутність належних засобів захисту. Україна не має достатньо належних засобів для захисту ОКІІ від кібернетичних атак. Це стосується як обладнання, так і кваліфікованих фахівців у галузі кібербезпеки, що можуть залучатися під час реагування на інциденти, які націлені на ОКІІ. Без належних засобів захисту, ОКІІ стають вразливими перед кібернетичними атаками, що може призвести до серйозних наслідків.

- Остання проблема - відсутність співпраці між Україною та іншими країнами. Співпраця з іншими країнами є надзвичайно важливою для ефективної протидії кібернетичним загрозам, включаючи атаки на ОКІІ. Однак, на даний момент Україна не має достатньої співпраці з іншими країнами у галузі

кібербезпеки, проте Міністерство цифрової трансформації вже намагається зменшити вплив даної на захист кібербезпеки.

Окрім прямих атак на об'єкти критичної інфраструктури, росія також відома своєю участю в дезінформаційних кампаніях, які мають на меті посіяти розгубленість і недовіру в країнах-мішенях. Ці кампанії часто спрямовані на політичні та соціальні питання і мають на меті маніпулювання громадською думкою та створення розколу всередині країни. Це може мати дестабілізуючий вплив на країну і може завдати такої ж шкоди, як і пряма кібератака на об'єкти критичної інфраструктури.

Загалом, загроза, яку становлять російські кібератаки на об'єкти критичної інфраструктури, є значною і постійно зростає. Також, для забезпечення належного рівня кібербезпеки в окремих ОКІІ необхідно вдосконалити технічні засоби захисту та забезпечити належний рівень кваліфікації персоналу, що буде забезпечувати кібербезпеку та проведення тренінгів серед керівництва та персоналу, що не є залученим до реагування на кібер інциденти, але може виступати, як один із ключових механізмів впливу на системи. Наприклад, можливо застосовувати різні технології захисту, такі як інтелектуальний аналіз поведінки користувачів, мультифакторну аутентифікацію та інші.

Тому країнам необхідно вжити заходів для захисту своєї критичної інфраструктури від цих атак. Це включає в себе інвестиції в заходи кібербезпеки, розробку планів реагування на надзвичайні ситуації та співпрацю з іншими країнами для обміну інформацією та ресурсами. Лише застосовуючи проактивний і скоординований підхід, ми можемо сподіватися на зменшення загрози, яку становлять російські кібератаки на об'єкти критичної інфраструктури.

Література

1. За підтримки Мінцифри стартує програма безоплатного навчання спеціалістів з кібербезпеки [Електронний ресурс]. – 1. – Режим доступу до ресурсу: https://thedigital.gov.ua/news/za-pidtrimki-mintsifri-startue-programa-bezoplatnogo-navchannya-spetsialistiv-z-kiberbezpeki

2. Кібервійна проти України: Держспецзв'язку дослідила мотивацію, методи та інструменти російських хакерів [Електронний ресурс]. – 8. – Режим доступу до ресурсу: https://ms.detector.media/withoutsection/post/31351/2023-03-08-kiberviyna-proty-ukrainy-derzhspetszvyazku-doslidyla-motyvatsiyu-metody-ta-instrumenty-rosiyskykh-khakeriv/

3. Код, який зупинить усе. Чому критична інфраструктура потребує сьогодні посиленого захисту [Електронний ресурс]. – 28. – Режим доступу до ресурсу: https://biz.nv.ua/ukr/markets/ukrposhta-zavershit-vstanovlennya-front-ofisnoji-sistemi-do-kincya-2022-roku-novini-ukrajini-50205166.html

4. Огляд подій в сфері кібербезпеки [Електронний ресурс] – Режим доступу до ресурсу:

https://www.rnbo.gov.ua/files/%D0%9D%D0%9A%D0%A6%D0%9A/%D0%9D%D0%9A%D0%A6%D0%9A-1/Cyber%20digest_December_2022.pdf

5. Стасюк В.В. Психологічне забезпечення діяльності військ (сил) / В.В. Стасюк. – К.: НУОУ, 2014. – 504 с.

6. Тищенко К. За минулий рік зареєстровано понад 2 тисячі кіберінцидентів – Держспецзв'язку [Електронний ресурс] / Катерина Тищенко // Українська правда. – 25. – Режим доступу до ресурсу: https://www.pravda.com.ua/news/2023/02/25/7391031/

Шерстюк В.А.
Новицький А.М.
д.ю.н., професор,
Національна академія СБ України

КІБЕРБЕЗПЕКА ТА ІНТЕЛЕКТУАЛЬНА ВЛАСНІСТЬ

Кібербезпека та інтелектуальна власність є взаємопов'язаними поняттями, оскільки кібератаки можуть спричинити витік інформації та порушення прав на інтелектуальну власність.

Одна з найбільш актуальних проблем управління кібербезпекою інтелектуальної власності полягає у захисті від крадіжки та незаконного використання конфіденційної інформації. Це може бути особливо важливо для компаній, які мають конкурентні переваги через свої технології та інтелектуальну власність.

Ефективність захисту прав інтелектуальної власності у цифровому просторі мережі Інтернет визначається можливістю протистояти таким порушенням, а також загрозам їх настання. Загрози порушення прав інтелектуальної власності в кіберпросторі (кіберзагрози) пов'язані з певними ризиками та можуть мати вплив на існування об'єкта виключних прав інтелектуальної власності. В результаті кібератак існує загроза втрати баз даних, що містять інформацію, яка є важливою для розвитку окремого суб'єкта господарювання та держави, або можуть бути розголошені відомості, які містять комерційну таємницю. Тому, ефективна система захисту прав інтелектуальної власності є частиною кібербезпеки та національної безпеки, оскільки наукова творчість є основою інновацій, які дають змогу державам перемагати в конкурентній боротьбі та закладають підвалини економічного і соціального розвитку.

За останнє десятиліття кіберпростір став окремою важливою сферою ведення боротьби під час війни. Звичним стало застосування державами кіберзброї, здійснення кібероборони, кібероперацій та кібератак.

В українській Стратегії кібербезпеки зазначається, що «враховано положення Стратегії кібербезпеки ЄС на цифрове десятиліття, стратегій кібербезпеки окремих держав-членів ЄС та держав-членів НАТО». Однак документ не містить переліку або окремого додатка про те, які саме положення враховані, за винятком одного з пунктів Плану реалізації, що передбачає імплементацію Директиви Європейського парламенту і Ради ЄС 2016/1148 від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу як елементу євроінтеграції України. [1]

З початку минулого року Україна зазнала двох потужних кібератак: перша з 13 на 14 січня та стала найпотужнішою за останні кілька років, охопивши 70 урядових сайтів. Ця атака була початком загострення війни. Атаку 15 лютого, яка порушила роботу двох найбільших банків держави («ПриватБанк» та «Ощадбанк»), фахівці вважають «найбільшою DDoS-атакою в історії України». [2]

Тому ми визначаємо ризик застосування кібератак на систему інтелектуальної власності як окремих суб'єктів підприємницької діяльності так і на державні органи, які забезпечують політику в сфері інтелектуальної власності. Ми вважаємо, що є необхідність постійного удосконалення національного законодавства у сфері кібербезпеки, задля належної реалізації завдань і функцій національної кібербезпеки та кібероборони в тому числі і в сфері інтелектуальної власності.

Література

1. Бакалінська О. / СУЧАСНІ ТЕНДЕНЦІЇ ПРАВОВОГО РЕГУЛЮВАННЯ КІБЕРБЕЗПЕКИ ТА ІНТЕЛЕКТУАЛЬНА ВЛАСНІСТЬ / 2022 р. – с. 87.

2. Держспецзв'язку: з початку 2022 року в Україні зафіксували 436 кіберінцидентів — це у сім разів більше, ніж за аналогічний період торік (18.02.2022). Режим доступу (URL): https://itc.ua/news/derzhspeczzvyazku-z-pochatku-2022-roku-v-ukrayinizafiksuvali-436-kiberinczidentiv-cze-u-sim-raziv-bilshe-nizh-za-analogichnij-period-torik.

Щебланін Ю.М.
к.т.н., с.н.с.,
Курченко О.А.
к.т.н., доцент,
Київський національний університет ім. Тараса Шевченка
Загиней А.Ю.
Державне підприємство «Українські спеціальні системи»

ВПЛИВ ТЕХНОЛОГІЙ ХМАРНИХ ОБЧИСЛЕНЬ НА СТАНДАРТНІ МЕТОДИ РЕАГУВАННЯ НА ІНЦИДЕНТИ

Хмарні технології дедалі частіше використовуються для зберігання та обробки державних інформаційних ресурсів. Відтак захист такої інформації потребує детального розгляду та опису певних стандартів, які повинні виконуватися відповідними установами. Певні процеси уже відбуваються на законодавчому рівні України, як результат 16 вересня 2022 року набрав чинності Закон України «Про хмарні послуги» [1], а 12 березня 2022 року Постановою Кабінету Міністрів України № 263 «Деякі питання забезпечення інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану» визначено вимоги щодо розміщення державних інформаційних ресурсів та публічних електронних реєстрів на хмарних ресурсах та/або центрах обробки даних, що розташовані за межами України [2], тому питання забезпечення захисту такої інформації є надзвичайно актуальним.

Застосування хмарних технологій напряму впливає на кожну з фаз життєвого циклу реагування на інциденти. Деякі з них подібні до реагування на інциденти в зовнішньому середовищі, де потрібно координувати дії з третьою стороною [3].

Під час підготовки до реагування на інциденти хмарних послуг, необхідно виділити наступне: наявність Договору про рівень обслуговування та управління сервісом (ресурсом) у хмарі; будь-який інцидент із використанням загальнодоступної хмари або розміщеного сервісу у постачальника хмарних послуг вимагає чітко прописаних окремих пунктів у договорі про рівень обслуговування і, ймовірно, координації з постачальником хмарних послуг у випадку інциденту тощо. Водночас, під час використання приватної хмари в сторонньому центрі обробки даних, необхідно визначити усі процеси, які будуть використані для виявлення, локалізації та нейтралізації інциденту, тощо.

Ключові моменти, які виникають на етапі підготовки реагування на інциденти: яка основна ціль розгорнутої системи (сервісу/ресурсу) у хмарному середовищі? За що відповідає постачальник хмарних послуг? Хто є контактними особами? Який очікуваний час відповіді у разі виникнення інциденту? Які є процедури відновлення (сервісу/ресурсу)? Чи є зв’язок виділеним каналом (на

випадок негативного впливу на мережі) з надавачем хмарних послуг? Як працює така передача даних? До яких даних користувач матимете доступ? Чи наявні сертифіковані фахівці та системи реагування на інциденти? та ін.

Необхідно переконатися, що методи реагування на інциденти та ролі/обов'язки постачальника та користувача хмарних послуг чітко визначені. А також необхідно проконтролювати, що постачальник має контакти для сповіщення про інциденти, які він виявляє, і що такі сповіщення інтегровані у ваш процес забезпечення захисту інформації.

В залежності він моделі обслуговування, а саме IaaS, PaaS та SaaS, тобто інфраструктура як послуга, платформа як послуга, програмне забезпечення як послуга [1], а також від конкретних служб які використовуються, повинен бути складений список з тих даних, та журналів подій, які будуть доступні під час реагування на інциденти. Адже швидше за все зв'язок з постачальником хмарних послуг буде відсутній.

Через динамічну та високошвидкісну природу обробки інформації існує значна потреба в автоматизації багатьох розслідуваних процесів у хмарних середовищах. Наприклад, докази можуть бути втрачені через звичайну діяльність автоматичного масштабування або якщо адміністратор вирішить припинити роботу віртуальної машини, яка бере участь у розслідуванні. Деякі приклади завдань, які можна автоматизувати, включають [4]:

- створення знімку віртуальної машини;
- збирання будь-яких метаданих під час виявлення інциденту, щоб на їх основі можна було провести аналіз того, як виглядала інфраструктура на момент виникнення інциденту;
- якщо постачальник хмарних послуг підтримує, «призупинення» віртуальної машини, це забезпечить збереження енергозалежної пам'яті та ін.
- аналіз мережевих потоків необхідний для перевірки, чи забезпечується ізоляція мережі. Можливість використання API для знімку мережі та стану правил віртуального брандмауера, що може дати вам точне уявлення про весь стек на момент інциденту;
- перевірку даних конфігурації, для встановлення факту атаки на аналогічну інфраструктуру;
- перегляд журналів доступу до даних (для хмарного сховища, контейнера тощо.) та журнали рівня керування, щоб визначити, чи вплинув інцидент на хмарну платформу і чи поширився на неї.

Журнали хмарної платформи можуть бути додатковим функціоналом, але вони не є базовими функціями. В ідеалі вони повинні показувати всю діяльність у площині керування хмарою.

Важливо розуміти, чи реєструються загрози, які можуть вплинути на аналіз інциденту, чи реєструється управлінська діяльність користувача послуги? та ін. Однією з проблем збору інформації для розслідування інциденту може бути

обмежена видимість мережі на стороні постачальника послуги. Мережеві журнали від постачальника, як правило, будуть записами потоків інформації, але не повним захопленням пакетів.

Окрім збору технологічної інформації про систему в певні моменти часу, а саме журналів подій та лог-файли потрібно переконатися, що у наявності необхідних фахівців та інструментів для проведення віддаленого дослідження інцидентів. Наприклад, чи є автоматизовані інструменти для збору журналів подій конкретно з хмарної платформи або гіпервізора.

Яким чином можна отримати образи запущених віртуальних машин і до якого типу сховищ у вас буде доступ, конкретно до дискового сховища, чи енергонезалежної пам'яті в цілому. Зазначені питання повинні бути визначені та прописані у відповідних договірних документах, в залежності від конкретної системи яка розгортається у хмарному середовищі [4].

Також крім забезпечення збору інформації, слід проконтролювати, чи доступні засоби для виявлення інцидентів та реагування на них (ізоляції сервісів для запобігання поширенню атак та компрометації усієї системи).

Виявлення та аналіз інцидентів у хмарному середовищі відрізняється для різних моделей хмарних послуг (IaaS, PaaS та SaaS). Однак у всіх випадках сфера моніторингу повинна охоплювати не лише розгорнуті сервіси (послуги), але й площину керування хмарою.

За можливості краще реалізувати так звані «незмінні сервери», тобто образи завідома справних віртуальних машин. Відповідно, у разі компрометації якогось сервісу, задля забезпечення доступу до системи необхідно буде перемістити робоче навантаження на новий екземпляр. Однак у такому випадку необхідно приділити увагу моніторингу цілісності файлів та управлінню конфігурацією.

Таким чином, використання нових технологій для збереження та обробки інформації створює нові виклики, щодо її захисту. Відтак коли державні інформаційні ресурси розміщуються за технологією хмарних обчислень, питання їх захисту повинно бути одним з пріоритетних. Однак окрім самої безпеки, яка має бути на найвищому рівні, за обставин сьогодення, питання реагування на інциденти в інфраструктурах розгорнутих з використанням хмарних рішень потребує значної уваги, адже саме розслідування різних типів атак допоможе у розробці новітніх та передових засобів захисту технології хмарних обчислень.

Література

1. Про хмарні послуги: Закон України від 17.02.2022 р. № 2075-IX URL: https://zakon.rada.gov.ua/laws/show/2075-20#Text. (дата звернення 19.03.2023).

2. Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану: Постанова Кабінету Міністрів

України від 12.03.2022 р. № 263. *Урядовий портал.* URL: https://www.kmu.gov.ua/npas/deyaki-pitannya-zabezpechennya-funkcionuvannya-informacijno-komunikacijnih-sistem-elektronnih-komunikacijnih-sistem-publichnih-elektronnih-reyestriv-v-umovah-voyennogo-stanu-263. (дата звернення 19.03.2023).

3. Cichonskiy P., Millar T., Grance T., Scarefone K., Computer Security Incident Handling Guide Recommendations of the National Institute of Standards and Technology. *National Institute of Standards and Technology.* 2012. DOI: http://dx.doi.org/10.6028/NIST.SP.800-61r2

4. The Security Guidance for Critical Areas of Focus in Cloud Computing v4.0. URL: https://cloudsecurityalliance.org/artifacts/security-guidance-v4/. (дата звернення 19.03.2023).

Яровий К.В.
к.ю.н.,
Національна академія внутрішніх справ

ПРІОРИТЕТНІ НАПРЯМКИ ПРОТИДІЇ ІНФОРМАЦІЙНИМ АТАКАМ У КІБЕРПРОСТОРІ

Українська стійкість до російських інформаційних атак останнім часом стала досить багатогранна. На державному та на суспільному рівнях є усвідомлення того, що інформаційний та психологічний вплив кремлівського режиму є невід'ємною частиною гібридної війни, військової агресії, анексії та окупації, політичної дестабілізації.

У свою чергу, для протистояння яким, у кіберпросторі вживаються заходи, направлені на забезпечення інформаційної безпеки та протидію поширенню інформаційним атакам на території нашої держави.

Сьогодні індивідуалізація систем безпеки є важливим елементом інформаційного захисту як на рівні держави, так і окремих цільових об'єктах критичної інформаційної інфраструктури [1, с. 12].

Так, з перших днів початку повномасштабної війни на території України з боку окупанта організовано роботу направлену на інформаційне протистояння ворогу у кіберпросторі.

Варто погодитися, що важливим аспектом інформаційних атак у кіберпросторі є реакція цільових груп і суспільства у цілому на їхнє розгортання у часі [2, с. 63].

Тому, вважаємо, що головними завданнями протидії інформаційним та психологічним впливам з боку країни агресорки стало:

- розповсюдження фото- та відео- матеріалів, розсилка статей про військові злочини країни-агресорки на території України у соціальних мережах (Twitter, Instagram, TikTok);
- створення постів на російських платформах про заклик мешканців російських міст щодо створення петицій про повалення тоталітарного кремлівського режиму та негайного припинення окупаційних військових дій в Україні;
- дії, направлені на пошук і збір інформації щодо переміщення військової ворожої техніки, диверсійно-розвідувальних груп, ворожих планів, корегування артилерією;
- видалення з геопозицій «фейкових» міток для нанесення ракетних, авіаційних та артилерійських ударів з мап Google та Яндекс;
- висвітлення реалій війни на Україні з боку агресора у форматі відеороликів на наших каналах (TikTok, YouTube).

На нашу думку, пріоритетними напрямками протидії інформаційним атакам у кіберпросторі можна вважати:

Розповсюдження інформації про масові заходи. Важливою є організація мирних мітингів для привернення уваги світової спільноти щодо негайного припинення військових дій держави-агресора на території України. Крім цього, організація антимобілізаційних мітингів на тимчасово окупованих територіях. Подібні мітинги організовані на території країни-агресора та білоруської держави, АР Крим, на тимчасово окупованих територіях України та інших країнах світу.

Створення каналів за напрямками. Створення тематичних каналів у соціальних мережах (Telegram, TikTok, YouTube) для висвітлення правдивої інформації про Україну та справжні події війни в усіх її подробицях. У свою чергу, обробляється та перевіряється отримана інформацію на правдивість зазначених даних та публікує новини на каналах. Вказані канали адаптовані під росіян, матерів російських солдатів, кримчан, білорусів, мешканців тимчасово окупованих територій України та жителів країн Європейського Союзу.

Блокування ворожих каналів, сайтів, акаунтів у соцмережах. Блокування ворожих каналів, сайтів, акаунтів у соцмережах стало звичним явищем для усіх небайдужих громадян України, які хоч якось намагаються протидіяти російській агресії. Наразі це найпоширеніша протидія ворогові у кіберпросторі.

Привернення уваги публічних осіб. Листування з відомими діячами, блогерами, зірками шоубізнесу щодо висвітлення інформації про Україну через особисті їх акаунти у соцмережах. Такі люди мають велике коло впливу, значну кількість аудиторії. Таким чином, вони розповсюджують на своїх акаунтах у соціальних мережах відео- і фото- матеріали, які дивляться мільйони людей по всьому світу.

Думка відомих особистостей впливає на людей, оскільки вони до них дослуховуються, і тому важливо окреслити свою чітку позицію, що дає змогу привернути більше уваги спільноти на дії агресора на території Україні.

Враховуючи вищевикладене, треба зазначити, що через розпочату проти України війну окупанти зіткнулися з безпрецедентними за потужністю і масштабами кібератаками, блокуванням акаунтів і груп у соціальних мережах, ворожих інформаційних каналів. Тому, необхідно переглянути підходи до запровадження сучасних інформаційних технологій під час протидії інформаційним атакам у кіберпросторі.

На основі отриманих результатів можна розробити потужні методи для виявлення характеристик і параметрів інформаційних атак у кіберпросторі, через які можуть бути виражені кількісні значення параметрів запропонованої моделі. Таким чином, відкриваються можливості для розробки комп'ютерної системи для підтримки прийняття рішень на їхній основі для структур управління кібербезпекою країни в цілому.

Література

1. Хорошко В.О., Хохлачова Ю.Є., Кібальчич І.В. Концепція кібербезпеки та моделювання процесів оптимального управління системою кіберзахисту держави. Інформатика та математичні методи в моделюванні. 2020. Т. 10, № 3–4. С. 230–242.

2. Трофименко О., Прокоп Ю., Логінова Н., Задерейко О. Кібербезпека України: аналіз сучасного стану. Захист інформації. 2019. Т. 21, № 3. С. 150–157.

СЕКЦІЯ 3
ПРОБЛЕМНІ ПИТАННЯ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ В УМОВАХ ЗБРОЙНОЇ АГРЕСІЇ рф

Авдошин І.В.
доктор юридичних наук, старший науковий співробітник,
Національна академія Служби безпеки України

ЗАРУБІЖНИЙ ДОСВІД УНОРМОВАНОСТІ ПЕРЕВІРКИ НА БЛАГОНАДІЙНІСТЬ ПРИ ОФОРМЛЕННІ ДОПУСКУ ДО СЕКРЕТНОЇ ІНФОРМАЦІЇ

В умовах триваючої російської агресії необхідність посилення заходів охорони та контррозвідувального захисту секретної інформації не викликає жодних сумнівів. Одним з напрямів цієї діяльності традиційно розглядається удосконалення законодавства у сфері охорони державної таємниці (ОДТ), зокрема перевірки громадян у зв'язку з допуском їх до державної таємниці.

Особливо гостро це питання постало після низки публічних скандалів коли до державної таємниці були допущені особи, які таку перевірку не проходили взагалі, або проходили формально, що не дозволило виявити факти та обставин, що перешкоджають їх допуску (доступу) до секретів.

Причинами таких випадків стали як необґрунтовані управлінські рішення та порушення існуючих законодавчих приписів, так і недосконаліть визначених в законі підстав для проведення перевірочних заходів в умовах особливого періоду, скорочення термінів перевірки (відомі випадки, коли допуск, за вказівкою керівництва, оформлявся за декілька робочих днів) та відсутність серед питань перевірки особи з'ясування її благонадійності як громадянина та рівня можливої уразливості до сторонніх впливів (шантажу, вербувальної уразливості, підкупу тощо).

У цьому контексті корисним, на наш погляд, є досвід нормативно-правового врегулювання цих питань в законодавстві колишніх постсоціалістичних країн (зокрема Республіки Болгарія, Естонської Республіки, Литовської Республіки), які пройшли схожий з Україною шлях реформування пострадянського законодавства та адаптації його до європейських вимог.

На сьогодні законодавство цих країн передбачає здійснення низки перевірочних заходів у т.ч. оперативного (контррозвідувального) опитування осіб, які мають намір отримати доступ до секретної інформації у зв'язку з виконанням функцій державного службовця. При цьому, якщо спецслужбами цих держав, які здійснюють відповідну перевірку, виявляються факти, обставини або ознаки, що свідчать про підвищену вербувальну уразливість особи з боку іноземних

спецслужб чи кримінальних структур (розбіжність між рівнем життя особи та її доходами, подружня невірність, ігроманія, зловживання алкоголем чи вживання наркотичних (психотропних) речовин тощо) то така особа за жодних обставин не отримає допуску та доступу до державної таємниці і, відповідно, не зможе бути призначена на державну посаду.

Натомість, в українському законодавстві з питань охорони державної таємниці з'ясування наявності чи відсутності зазначених вище ознак, фактів та обставини на сьогодні не є завданням перевірки осіб у зв'язку з їх допуском до державної таємниці, яка здійснюється органами Служби безпеки України.

Така ситуація звужує спектр перевірочних заходів, призводить до формалізму та, зрештою, унеможливлює належну перевірку осіб на благонадійність у зв'язку з оформленням допуску до секретної інформації.

Така ситуація несприятливо позначається не лише на збереженні державної таємниці, але й дозволяє проникнути на відповідальні державні посади особам з низькими моральними якостями, не чистим на руку, не патріотично налаштованим громадянам, які в подальшому, через свою посаду та особистісні якості, можуть становити інтерес для іноземних, передусім – російських, спецслужб і стати об'єктом вербувального вивчення та залучення до негласного співробітництва на шкоду інтересам України.

Розглядаючи особливості організації та правового регулювання проведення спецслужбами окремих європейських держав (зокрема Республіки Болгарія, Естонської Республіки, Литовської Республіки) перевірочних заходів (включаючи контррозвідувальне опитування), пов'язаних з доступом до державних секретів, встановлено, що кожна з цих систем (моделей) по-своєму унікальна, та містить позитивні аспекти організації перевірки, варті запозичення в українське законодавство.

Зокрема, болгарська модель проведення заходів перевірки передбачає диференційовану повноту перевірки в залежності від ступеня секретності інформації, до якої буде допущена особа. Відповідно змінюються вимоги й до опитування такої особи. Якщо на етапі звичайної перевірки опитування має суто формальний характер, то на етапах розширеної та спеціальної перевірок воно набуває характеру контррозвідувальної спрямованості, оскільки проводиться співробітником контррозвідувального підрозділу та стосується переважно безпекових питань (можливої причетності до розвідувально-підривної чи іншої протиправної діяльності на шкоду державній безпеці, наявності ознак (обставин) вербувальної уразливості, наявності інших обставин, що несприятливо позначаються на спроможності особи надійно зберігати довірену їй секретну інформацію.

Позитивним та актуальним для України елементом литовської системи допуску до секретної інформації є можливість його спрощення в умовах воєнного та надзвичайного станів, коли, у разі службової необхідності, такий доступ може

бути наданий без проведення заходів з перевірки за умови, якщо благонадійність особи, яка його отримує, та її лояльність Литовській державі не викликає сумнівів у органів державної безпеки.

Проте, найбільш важливим та вартим імплементації в українське законодавство аспектом перевірки особи на доступ до секретної інформації в законодавстві аналізованих держав вважаємо з'ясування уповноваженими контррозвідувальними органами обставин (фактів, ознак) життя (діяльності) такої особи, що свідчать про її підвищену вербувальну уразливість (а отже можуть бути використані представниками іноземних спецслужб чи кримінальних структур при вербувальних підходах, шантажі чи компрометації майбутнього держслужбовця-секретоносія). До таких обставин, зарубіжне законодавство відносить, зокрема, корупційні прояви, схильність до незаконного збагачення та не доброчесних вчинків, невідповідність рівня життя особи рівню її доходів, політичні погляди особи, які визначають її лояльність до держави та ступінь патріотизму. Ступінь відсутності цих обставин визначає межі благонадійності громадянина та істотно впливає на висновок по результатам перевірки.

Зрештою вивчення та адаптування зарубіжного досвіду унормування діяльності іноземних спецслужб, зокрема Республіки Болгарія, Естонської Республіки та Литовської Республіки з проведення перевірочних заходів у т.ч. контррозвідувального опитування, стосовно осіб, яким оформляється допуск та доступ до державної таємниці у зв'язку з виконанням відповідних завдань від імені держави, є нагальною теоретичною та прикладною проблемою. Вважаємо, що позитивний досвід у цій сфері має бути використаний для удосконалення вітчизняної системи охорони державної таємниці, яка на сьогодні є основним запобіжником потрапляння на державну службу осіб з підвищеним рівнем вербувальної уразливості, зумовленої корупційними, клептократичними, аморальними та іншими негативними схильностями та вадами світоглядного сприйняття.

Література

1. Про державну таємницю: Закон України від 21 січні 1994 року № 3855-XII (станом на 15.03.2022) / *Відомості Верховної Ради України*. 1994. № 16. Ст. 93.

2. Про захист секретної інформації: Закон Республіки Болгарія від 30.04.2002 р. (в редакції станом на 13.09.2016). URL : http://lex.bg/bg/laws/ldoc/2135448577 (дата звернення 22.02.2023).

3. Про Державне агентство національної безпеки: Закон Республіки Болгарія від 20.12.2007 р. URL : http://law.dir.bg/reference.php?f=zdans-07 (дата звернення 22.02.2023).

4. Закон Естонської Республіки «Про державну таємницю та секретну інформацію іноземних держав» від 25 січня 2007 року (в редакції Закону від 22

грудня 2007 року, зі змінами та доповненнями станом на 1 липня 2017 року. URL: http://www.legalltext. ee/en/andmebass/ava. asp?m = 022 (дата звернення 22.02.2023).

5. Закон Литовської Республіки від 25 листопада 1999 року № VIII-1443 «Про державну і службову таємницю» (зі змінами та доповненнями станом на 13 червня 2017 року). URL: http://www.litlex.lt (дата звернення 22.02.2023).

Артамонов Є.Б.
к.т.н.,
Національний авіаційний університет,
Данкович Н.І.
Навчально-науковий інститут інформаційної безпеки та стратегічних комунікацій Національної академії Служби безпеки України,
Крант Д.В.
Національний авіаційний університет

ПІДВИЩЕННЯ РІВНЯ ЗАХИЩЕНОСТІ ВНУТРІШНІХ БАЗ ДАНИХ ЗА РАХУНОК АНАЛІЗУ ПОВЕДІНКОВИХ ОЗНАК КОРИСТУВАЧА

В останні роки все більше організацій переходять на використання внутрішніх баз даних (подібні рішення часто називають корпоративними базами даних) замість зберігання даних на зовнішніх серверах. Це має декілька причин.

– забезпечення безпеки даних;
– покращення ефективності та продуктивності;
– кращий контроль за даними;
– зменшення витрат.

Отже, використання внутрішніх баз даних дозволяє організаціям забезпечити захист даних та покращити ефективність та продуктивність, що допомагає забезпечити більш точну та надійну роботу з даними.

Але також підвищується ризик викрадення паролів та несанкціонованого доступу до внутрішніх баз даних організації, бо рівень захисту хмарних рішень набагато вище, ніж той, який можуть забезпечити навіть найкращі фахівці в організації, а також співробітники можуть не так ретельно відноситись до безпеки, бо будуть помилково вважати, що внутрішні системи більш захищені [1]. Це може стати причиною серйозної загрози безпеці та конфіденційності даних організації.

Одним з найбільш поширених методів атак на внутрішні бази даних є викрадення паролів користувачів [2]. Якщо зловмисник отримає доступ до пароля одного користувача, він може отримати доступ до всієї бази даних (особливо у випадку, якщо це користувач з правами адміністратора). Також підвищується загроза втрати конфіденційної інформації, відкриття бізнес-таємниць, втручання в дані для аналітичного аналізу.

В цій статті більш детально розглянемо спосіб підвищення безпеки доступу до внутрішніх баз даних за рахунок використання методів аналізу поведінкових ознак користувача, як додаткової системи аутентифікації користувача.

Аналіз методів оцінки поведінки користувача, щоб підтвердити аутентифікацію

Методи аналізу поведінкових ознак користувача [3] базуються на тому, що кожен користувач має унікальні характеристики свого поведінки, такі як швидкість писання, ритм натискання клавіш, рух миші та інші.

Одним із методів є аналіз шаблону набору тексту (keystroke Dynamics). Цей метод вимірює час між натисканням різних клавіш і швидкість писання [4], що дозволяє визначити унікальний шаблон поведінки користувача. Інший метод – це аналіз рухів миші (mouse Dynamics). Цей метод вимірює різні параметри руху миші, такі як швидкість, прискорення, та шлях, пройдений мишею [5]. Також, існують інші методи поведінкової аутентифікації, такі як аналіз стилю письма, аналіз голосу, натискання клавіш, часу відповіді на запити та інші [2, 6].

Однією з головних переваг методів поведінкової аутентифікації є те, що вони забезпечують більш високий рівень безпеки, оскільки унікальні шаблони поведінки користувачів складніше підробити, ніж зламати пароль або отримати доступ до ключової картки. Також поведінкова аутентифікація дозволяє налаштовувати режими роботи систем та забезпечувати переключення між режимами відображення інформації [7].

Опис запропонованого методу

Для моделювання поведінки користувачів пропонується використовувати такі параметри, як швидкість набору тексту, інтервали між натисканням клавіш, швидкість руху миші та інші параметри, які можуть бути виміряні під час роботи користувача з програмним забезпеченням, тощо.

Для конкретного випадку зі збору і аналізу поведінкових даних користувачів при роботі з внутрішніми базами даних можна розглянути наступну формулу для розрахунку відстані між двома користувачами на основі їхніх поведінкових параметрів.

$$d = \sqrt{\omega_1 (x_1 - y_1)^2 + \omega_2 (x_2 - y_2)^2 + ... + \omega_n (x_n - y_n)^2} ,$$

де d – це відстань між векторами поведінкових параметрів двох користувачів,

$x_1, x_2, ..., x_n$ – це значення поведінкових параметрів першого користувача,

$y_1, y_2, ..., y_n$ – це значення поведінкових параметрів другого користувача,

$\omega_1, \omega_2, ..., \omega_n$ – це вагові коефіцієнти, які використовуються для призначення важливості кожного поведінкового параметра (можна дати більшу вагу швидкості набору тексту порівняно з частотою перегляду каталогів).

Для розрахунку значень поведінкових параметрів можуть використовуватися різноманітні методи, такі як аналіз логів користувачів, використання датчиків руху

в пристроях або збір інформації з миші і клавіатури. Параметри можуть бути нормалізовані до значень від 0 до 1, щоб зробити їх сумісними для порівняння.

Таким чином, враховуючи певні поведінкові параметри користувачів, створено математичну модель, що враховує вагу кожного параметра та дозволяє розрахувати відстань між користувачами, що в свою чергу може бути використана для вирішення різних задачі поведінкової аутентифікації користувачів.

Загалом, використання даної формули може забезпечити більш точний та об'єктивний аналіз поведінки користувачів при роботі з внутрішніми базами даних, що дозволяє покращити функціональність програмного забезпечення, підвищити його ефективність та забезпечити зручне та безпечне користування. Крім того, використання даної формули дозволяє знизити ризик помилкових рішень при прийнятті рішень на основі поведінкових даних користувачів та сприяє підвищенню рівня безпеки у використанні програмного забезпечення.

Висновки

Методи аналізу поведінкових ознак користувача можуть допомогти підвищити безпеку доступу до внутрішніх баз даних. Ці методи дозволяють визначити унікальний шаблон поведінки кожного користувача, що може бути використано для аутентифікації. Порівняно з традиційними методами аутентифікації, такими як введення пароля або використання ключових карток, методи поведінкової біометрії є більш безпечними, оскільки вони важко підробити.

Проте, існує ризик, що користувач може змінити свій шаблон поведінки, якщо він змінить свій стиль набору тексту, швидкість писання або інші параметри поведінки. Крім того, методи поведінкової біометрії можуть бути складніші для використання в бізнес-середовищах, оскільки вони вимагають спеціального програмного забезпечення та обладнання.

Отже, хоча методи поведінкової біометрії можуть допомогти підвищити безпеку доступу до внутрішніх баз даних, вони не повинні бути єдиною формою аутентифікації. Краще використовувати їх разом з іншими методами, такими як паролі та ключові картки, для забезпечення максимального рівня безпеки.

Для досягнення максимальної ефективності, методи поведінкової аутентифікації можуть бути поєднані з іншими методами аутентифікації, такими як двофакторна аутентифікація або використання сильних паролів. Комбінування декількох методів аутентифікації може допомогти зменшити ризики та підвищити безпеку користувача.

Окрім того збір та аналіз поведінкових ознак користувачів може бути пов'язаний з збором та обробкою персональних даних, що може створювати проблеми з конфіденційністю та захистом особистої інформації. Тому, необхідно забезпечувати відповідну обробку та зберігання персональних даних згідно з вимогами законодавства та стандартами безпеки.

Таким чином успіх методів поведінкової аутентифікації при роботі з онлайновими продуктами залежить від використання відповідної комбінації методів аутентифікації, захисту персональних даних та врахування ризиків та потенційних загроз.

Література

1. Venkadesh S., Palanivel K. A Survey on Password Stealing Attacks and Its Protecting Mechanism // International Journal of Engineering Trends and Technology (IJETT). – V19(4). – 2015. – pp. 223-226. DOI: 10.14445/22315381/IJETT-V19P239.

2. Ahmed, A.A. Future effects and impacts of biometrics integrations on everyday living // Al-Mustansiriyah J. Sci. – 2019. № 29. – pp. 139–144.

3. Wong-In S., Netinant P. Designing an examinee personal verification system using biometric technology // J. Curr. Sci. Tecnnol. – 2018. – № 8. – pp. 75–86.

4. Campisi P., Maiorana E., Lo Bosco M., Neri A. User authentication using keystroke dynamics for cellular phones, Signal Processing, IET. – 2009. – 3(4). pp. 333 –341.

5. Khan S., Hou D. Mouse Dynamics Behavioral Biometrics: A Survey // ACM Comput. Surv. – 2022. – № 37 (4). https://doi.org/10.48550/arXiv.2208.09061.

6. Stylios I., Kokolakis S., Thanou J. Chatzis S. Behavioral biometrics & continuous user authentication on mobile devices: A survey // Information Fusion. – Volume 66. – 2020. – pp. 76-99. https://doi.org/10.1016/j.inffus.2020.08.021.

7. Artamonov Y., Golovach I., Krant D., Rosinska H., Nechyporuk O., Stanko S. Dynamic Content Generation Methods Based on User Behavioral Ranking // IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT). – Kyiv, 2022. – pp. 313-318, doi: 10.1109/ATIT58178.2022.10024196.

Блавацька Н.М.
кандидат технічних наук, доцент
НА СБУ

ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ ХМАРНИХ ТЕХНОЛОГІЙ ДЛЯ ЗДЕШЕВЛЕННЯ ВИКОРИСТАННЯ ПЛАТНОГО VPN

Сучасні реалії динамічно вносять зміни в усі сфери нашого життя. В умовах інформаційної війни, яка отримала новий виток з початком повномасштабної воєнної агресії російської федерації проти України важливою складовою є збір інформації. Один із засобів, за допомогою яких можна конфіденційно збирати інформацію із загальнодоступних джерел є VPN. Активізація доступу до ресурсів та технологій глобальної мережі Інтернет з використанням VPN обумовлена в

тому числі і збиранням інформації про численні воєнні злочини рф в Україні та їх документування.

Коли користувач отримує доступ до Інтернету без VPN, з його історією пошуку, місцем знаходження та інформацією про його Інтернет-провайдера можуть ознайомитись сторонні зацікавлені особи, які мають відповідні навички. VPN захищає онлайн-інформацію від доступу до неї зацікавлених осіб. Крім того більшість російського контенту закрито для користувачів з України. Все це спричиняє використання VPN при пошуку потрібної інформації зі збереженням конфіденційності.

Необхідно зазначити, що ефективні та безпечні VPN не безкоштовні. Тут на допомогу можуть прийти хмарні технології.

Хмарні технології – це технології розподіленої обробки цифрових даних, за допомогою яких комп'ютерні ресурси надаються інтернет-користувачу як онлайн-сервіс. Різноманітні апаратні, програмні засоби надаються користувачу, як інтернет-сервіси, для реалізації його завдань та проектів. Програмні додатки запускаються та видають результати роботи у вікні web-браузера на локальному комп'ютері. При цьому всі необхідні для роботи програми та їх дані знаходяться на віддаленому інтернет-сервері. А з використанням апаратних можливостей хмарних технологій можна значно збільшити обчислювальні можливості свого комп'ютера при потребі.

Переваги технології полягають в тому, що користувач має доступ до власної інформації, проте не повинен перейматися стосовно інфраструктури, операційної системи та програмного забезпечення, на якому в нього є потреба працювати.

Можливості хмарних технологій:

- доступ до своєї інформації з будь-якого пристрою (комп'ютер, телефон, планшет), який підключений до Інтернету;
- веб-сервіси працюють в браузерах будь-яких операційних систем;
- більшість платних програм стануть безкоштовними для вас (або набагато дешевшими);
- непотрібно перейматись стосовно оновлень програмного забезпечення, сервіс дає змогу користуватися найновішими версіями програмних продуктів;
- вся ваша інформація в хмарі збережеться, навіть коли вона буде втрачена безпосередньо на вашому комп'ютері.

Хмарні технології дають можливість здешевити використання ефективних але дорогих VPN для збереження конфіденційності вашої особистої інформації при роботі в мережі Інтернет. Це лише один з варіантів застосування хмарних технологій. Цей шлях вказує на можливість менше коштів витрачати на платне програмне забезпечення для своєї професійної діяльності.

Бойченко О.С.
кандидат технічних наук
Житомирський військовий інститут імені С. П. Корольова
Кримець Б.В.
Центральне управління охорони державної таємниці та захисту інформації
Генерального штабу Збройних Сил України

ПРОПОЗИЦІЇ З УДОСКОНАЛЕННЯ ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧІВ

На початку XXI століття з метою розширення послуг із захисту інформації та інформаційних ресурсів в інформаційно-комунікаційних системах (ІКС) почав широко застосовуватись електронний підпис, який заснований на відповідних криптографічних механізмах. Це сприяло тому, що у системах електронного документообігу (СЕДО) в умовах протидії порушникам (зловмисникам) почали надаватися базові послуги (виконуватися функції) або розв'язуватися задачі забезпечення з необхідним рівнем гарантій конфіденційності, цілісності, справжності (автентичності), неспростовності (спостережливості), доступності та надійності.

У Збройних Силах (ЗС) України розроблена та введена в дію Захищена СЕДО, яка використовує технологію електронного підпису та використовує електронні довірчі послуги (ЕДП).

Застосування Захищеної СЕДО дозволило скоротити час на доставку документу, що значно підвищило ефективність управління військами (силами). Поряд з тим у ЗС України існують такі проблемні питання:

відсутність у законодавстві України нормативно-правових актів, які визначають поняття секретного електронного документа (СЕД), його юридичний статус та порядок роботи з ним, а також суб'єктів електронної взаємодії системи обігу секретних електронних документів;

електронні документи, які циркулюють у Захищеній СЕДО нетаємні, а сама система не може бути застосована для передачі СЕД (бойових наказів, розпоряджень);

повільне впровадження технічних рішень, які забезпечать можливість надання кваліфікованих ЕДП в ІКС, де обробляється ІзОД;

відсутність порядку взаємодії інфраструктури відкритих ключів (ІВК) ЗС України з ІВК ЗС держав-членів НАТО.

Тому перед ЗС України постає важливе завдання щодо розробки технології надання кваліфікованих ЕДП в ІКС ЗС України, в яких обробляється ІзОД. Виникнення цього актуального науково-технічного завдання зумовлено об'єктивним протиріччям між високими вимогами до захисту ІзОД відповідно до вимог законодавства України і стандартів НАТО та принциповою неможливістю її захисту за рахунок використання існуючої ІВК у ЗС України.

Одним з можливих способів рішення цього завдання є удосконалення ІВК ЗС України для надання кваліфікованих ЕДП в ІКС ЗС України, де обробляється ІзОД.

Головною вимогою до ІВК ЗС України є забезпечення гарантованої довіри до ЕДП, які надаються в ІКС, де обробляється ІзОД.

Для надання ЕДП в ІКС ЗС України, де обробляється ІзОД, необхідно забезпечити доступ до цієї ІКС за рахунок застосування організаційних та технічних заходів [1]. Організаційні заходи повинні забезпечити обмеження доступу підписувачам та користувачам ЕДП до об'єкту інформаційної діяльності, на якому розміщене автоматизоване робоче місце (АРМ) з можливістю роботи в ІКС, де обробляється ІзОД, відповідно до форми допуску до державної таємниці користувача ЕДП. Технічні заходи повинні бути реалізовані за рахунок використання функцій електронної ідентифікації та авторизації користувачів ІКС, де обробляється ІзОД.

Під СЕД слід розуміти секретний документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити секретного документа.

З метою удосконалення ІВК ЗС України пропонується:

1) створити розподілену базу даних СЕД ЗС України з впровадженою системою розмежування доступу;

2) створити механізм взаємодії між ІКС, в яких обробляється інформація з різним ступенем секретності;

3) розробити порядок надання кваліфікованих ЕДП в ІКС, де обробляється ІзОД;

4) розробити військові публікації, які регламентують встановлення довіреної ідентифікації між ІКС ЗС України та ІКС ЗС держав-членів НАТО в федеративній мережі місій.

Враховуючи вищенаведене, ІВК ЗС України матиме таку структуру: уповноважений орган у сфері ЕДП у ЗС України, кваліфікований надавач ЕДП у ЗС України, підписувачі та користувачі ЕДП.

Уповноважений орган у ЗС України призначений для організації спеціального зв'язку та захисту інформації у сферах ЕДП та електронної ідентифікації у ЗС України.

Кваліфікований надавач ЕДП у ЗС України – визначений підрозділ, який надає одну або більше кваліфікованих ЕДП в ІКС, де обробляється ІзОД.

Підписувачі та користувачі ЕДП у ЗС України – створювачі електронних печаток, відправники та отримувачі електронних даних, які отримують ЕДП у кваліфікованих надавачів ЕДП у ЗС України.

Безпосередньо функції довірчої сторони виконують програмно-технічні комплекси, які використовуються під час надання ЕДП і являють собою апаратні,

апаратно-програмні та програмні засоби кваліфікованого надавача ЕДП у ЗС України.

Враховуючи вище наведене та результати науково-дослідних робіт [2, 3] перспективна схема організації ІВК у ЗС України складається з наведених нижче компонентів.

Сервер взаємодії – окремо виділені спеціальні апаратні та програмно-апаратні засоби, які призначені для унеможливлення витоку СЕД при їх передачі між ІКС різного рівня секретності, у тому числі й у федеративній мережі місій.

Інформаційно-комунікаційна мережа (ІКМ) ІКС, де обробляються СЕД з грифом секретності "Цілком таємно", може бути представлена як ІКС класу 2.

ІКМ ІКС, де обробляються СЕД з грифом секретності "Таємно", може бути виконана як розподілена ІКС класу 3 з каналами зв'язку, які використовуються ЗС України.

ІКМ ІКС, де обробляються електронні документи з грифом обмеження доступу "Для службового користування", може бути виконана як ІКС класу 3.

Сервер баз даних – електронно-обчислювальний засіб у серверному виконанні із встановленим спеціалізованим програмним забезпеченням, який виконує функції серверу додатків на базі Web-технологій для забезпечення обміну СЕД між користувачами ІКС, їх зберігання, розмежування доступу до СЕД користувачів та обробки СЕД відповідно до політки безпеки інформації в ІКС за допомогою пристрою розмежування доступу.

Пристрій розмежування доступу – електронно-обчислювальний засіб із встановленим спеціалізованим програмним забезпеченням.

Комутатор – пристрій, призначений для з'єднання декількох АРМ в межах одного об'єкту (центрального або віддаленого).

АРМ – електронно-обчислювальний засіб на основі персональної електронної обчислювальної машини або засобу спеціального зв'язку, на якому встановлений мінімально потрібний комплект програмного забезпечення з обов'язковою наявністю інтернет браузера.

Відповідно до політики безпеки в ІКС на АРМ за допомогою програмних засобів, які розміщені на сервері даних, створюється особистий кабінет користувача ІКС. Передбачається, що авторизований користувач ІКС може мати доступ до свого особистого кабінету з будь-якого АРМ. При цьому ступінь секретності інформації, яку може обробляти користувач ІКС буде обмежена ступенем секретності інформації, яку можна обробляти на відповідному АРМ.

Міжмережевий екран – програмно-апаратний комплекс, який реалізує функцію контролю вхідного і вихідного трафіку в ІКМ ІКС одного рівня секретності.

Програмно-технічний комплекс кваліфікованого надавача ЕДП у ЗС України у закритому контурі – апаратні, апаратно-програмні та програмні засоби

призначені для надання кваліфікованих ЕДП в ІКС ЗС України відповідного рівня секретності.

Таким чином, надання ЕДП користувачам ІКС ЗС України буде здійснюватися за грифами секретності СЕД та за рівнем допуску до роботи з державною таємницею відповідного користувача ІКС ЗС України.

Застосування серверів взаємодії дозволить реалізувати взаємодію ІВК ЗС України з ІВК ЗС держав-членів НАТО для здійснення обміну інформацією та розвідувальними даними під час спільних операцій держав-членів НАТО.

Література

1. Про затвердження Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : Постанова Кабінету Міністрів України від 16.02.1998 № 180. URL:https://zakon.rada.gov.ua/laws/show/180-98-%D0%BF#Text (дата звернення: 07.03.2023)

2. Науково-дослідна робота шифр “Фундамент”: звіт про НДР (остаточний), кер. О. Бойченко. Житомирський військовий інститут імені С. П. Корольова, 2019. 119 с.

3. Науково-дослідна робота шифр “Фундамент-ТТЗ”: звіт про НДР (остаточний), кер. О. Бойченко. Житомирський військовий інститут імені С. П. Корольова, 2020. 103 с.

Благодарний А.М.
доктор юридичних наук, професор,
професор кафедри загальноправових дисциплін
Національної академії Служби безпеки України

ПОПЕРЕДЖЕННЯ АДМІНІСТРАТИВНИХ ПОРУШЕНЬ ЗАКОНОДАВСТВА ПРО ДЕРЖАВНУ ТАЄМНИЦЮ

Розвиток України як демократичної, соціальної, правової держави передбачає профілактику різних форм протиправної поведінки, однією з яких є вчинення адміністративних правопорушень. За допомогою норм, що встановлюють адміністративну відповідальність, здійснюється охорона широкого кола суспільних відносин (лише Кодекс України про адміністративні правопорушення (далі – КУпАП) містить чотирнадцяти глав, в яких зосереджено норми, що визначають склади більше семиста адміністративних правопорушень). Звісно, що кожній групі правопорушень властиві певні особливості детермінації. Розглянемо питання попередження адміністративних порушень законодавства про державну

таємницю (ст. 212-2 КУпАП) – проступку, що завдає шкоди одним з найбільш досконало регламентованих чинним законодавством (насамперед, Законом України «Про державну таємницю») правовідносинам.

Усі чинники (детермінанти) правопорушень у науковій літературі прийнято поділяти на суб'єктивні та об'єктивні. При цьому до суб'єктивного відноситься усе те, що залежить від людини, і навпаки, об'єктивний означає, що предмети, властивості та відносини існують поза суб'єктом і незалежно від нього. Суб'єктивні чинники є переважно причинами вчинення правопорушень, об'єктивні ж чинники – умовами [1, с. 144].

Вважаємо, що навіть для такої специфічної групи адміністративних правопорушень, як порушення законодавства про державну таємницю, властиві загальні детермінанти адміністративної деліктності. До загальних причин адміністративних правопорушень у науковій літературі як правило відносять: недостатнє врахування законів управління у змісті рішень, що приймаються; неповноту або нечіткість правового регулювання певних суспільних відносин; слабкість соціального контролю; недостатньо високий рівень правосвідомості учасників відносин; відхилену від правових і моральних норм поведінку окремих громадян та інші причини [1, с. 145]. Поряд із загальними чинниками, що породжують явище в цілому, в даному випадку адміністративну деліктність, у науковій літературі виділяють також причини і умови певних видів (категорій, груп) правопорушень. Так, особи, які вступають у конфлікт зі встановленими правилами, що діють у сфері державного управління, характеризуються індивідуалістично-анархічною антисоціальною спрямованістю, а це означає, що пояснення причин існування у суспільстві адміністративної деліктності потрібно шукати в дії тих факторів, які сприяють формуванню (хоча й неглибокої і незначно відхиленої від системи ціннісних орієнтацій, сприйнятих у нашому суспільстві), антисуспільної установки, що має анархо-індивідуалістичну спрямованість [2, с. 51–52].

Не заперечуючи проти дії вказаного чинника, зауважимо, що визначального впливу на поведінку осіб, які вчинюють порушення законодавства про державну таємницю, цей чинник не матиме. Пояснюється це тим, що з боку зазначених осіб вимагається дисциплінованість, до певної міри підкорення і слухняність, тому їм навряд чи буде властива індивідуалістично-анархічна спрямованість. Хоча, причини конкретних порушень законодавства про державну таємницю у деяких випадках можуть зумовлюватись психологічними антисуспільними особливостями конкретного правопорушника – особи, яка добре знає, або, принаймні, достатньо ознайомлена із законодавством про державну таємницю, але не має внутрішнього переконання у необхідності суворого дотримання його.

Для деяких осіб, які порушують законодавство про державну таємницю, детермінація їх адміністративно-караних порушень у зазначеній сфері пов'язана з тим, що вони здебільшого виступають щодо інших осіб як підлеглі. Вони

практично позбавлені змоги тримати себе на рівні своїх можливостей і обирати соціальну роль відповідно до своїх «природних нахилів», іншими словами, ці особи в наказовому порядку можуть бути зобов'язані вчинювати дії, що порушують законодавство про державну таємницю [1, с. 147].

Результати аналізу судових рішень по справах про адміністративні порушення законодавства про державну таємницю засвідчують, що основними причинами вчинення зазначених проступків виступають:

– недостатнє знання деякими особами норм чинного законодавства про державну таємницю;

– нехтування деякими особами нормами чинного законодавства, так іноді керівники підприємств, установ та організацій, які здійснюють діяльність, пов'язану з державною таємницею, вважають, що вони не володіють інформацією, розголошення якої може завдати шкоди національній безпеці України [3].

На сьогодні правове регулювання профілактики адміністративних правопорушень в цілому має лише фрагментарний характер. Відповідно до ч. 1 ст. 6 КУпАП органи виконавчої влади та органи місцевого самоврядування, громадські організації, трудові колективи розробляють і здійснюють заходи, спрямовані на запобігання адміністративним правопорушенням, виявлення й усунення причин та умов, які сприяють їх вчиненню, на виховання громадян у дусі високої свідомості і дисципліни, суворого додержання законів України. Певні норми щодо профілактики окремих видів правопорушень містяться в інших законах України, наприклад, розділ IV Закону України «Про державну таємницю», присвячений охороні державної таємниці, передбачає заходи, спрямовані на попередження порушень законодавства про державну таємницю.

Під час профілактики адміністративних порушень законодавства про державну таємницю слід використовувати методи профілактики, властиві для адміністративної деліктності взагалі, але при цьому не слід нехтувати специфічними особливостями зазначеної діяльності. Профілактична діяльність у сфері недопущення порушення законодавства про державну таємницю спрямована на конкретну групу осіб, а саме – осіб, які мають допуск та доступ до державної таємниці. Це зумовлює певну специфіку, що стосується суб'єктів профілактики, конкретних заходів попередження, правової регламентації запобігання деліктності, усунення причин і умов, що її породжують.

До попереджувальних заходів належить достатньо велика кількість способів, прийомів і дій різноманітних органів та окремих осіб. Однією з дієвих форм профілактичного впливу на свідомість людини є оголошення особі офіційного застереження про неприпустимість протиправної поведінки. Офіційне застереження про неприпустимість протиправної поведінки застосовується до осіб, які систематично порушують законодавство, якщо ці порушення незначні за своїм характером і за їх вчинення не передбачено юридичної відповідальності. Вказаний захід застосовується, якщо немає достатніх підстав для притягнення

особи до кримінальної чи адміністративної відповідальності. Метою його застосування є не тільки реакція на протиправну поведінку, але й недопущення її продовження в майбутньому. Правові підстави застосування цього заходу встановлені законами України «Про Національну поліцію», «Про Службу безпеки України», «Про контррозвідувальну діяльність» тощо, порядок застосування визначається відомчими нормативними актами [4, с. 121].

Зауважимо, що в силу різних обставин офіційне застереження наразі широко не застосовується, значною мірою така ситуація зумовлена тим, що в законах України не міститься конкретних приписів як щодо порядку застосування цього заходу, так і щодо змісту документу про оголошення офіційного застереження. Для підвищення ефективності застосування зазначеного заходу, в чинному законодавстві варто передбачити наслідки продовження протиправної поведінки особою, щодо якої було винесено офіційне застереження. Зазначену протиправну поведінку слід вважати обставиною, що обтяжує відповідальність. Ураховуючи, що ст. 35 КУпАП містить вичерпний перелік обставин, що обтяжують адміністративну відповідальність, слід доповнити п. 2 ч. 1 ст. 35 КУпАП такою обставиною, як оголошення особі офіційного застереження.

Література

1. Благодарний А. М. Адміністративна відповідальність за порушення законодавства про державну таємницю : монографія. Київ : Вид-во НА СБ України, 2008. 180 с.

2. Додин Е. Понятие и причины административной деликтности. Проблемы административного права и совершенствования административной деятельности органов внутренних дел: сборник научных трудов. Киев : КВШ МВД СССР, 1981. С. 44–54.

3. Офіційний веб-порталі судової влади України. URL: http://www.reyestr.court.gov.ua (дата звернення: 14.03.2023).

4. Адміністративне право України : підручник : Т. 1 : Загальна частина / А. М. Благодарний, Д. М. Лук'янець, А. В. Макаренко та ін. Київ : Нац. акад. СБУ, 2016. 260 с.

Вахнов П.В.
старший викладач Національної академії Служби безпеки України

АКТУАЛЬНІ ПИТАННЯ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ В СИСТЕМІ РАДІОЗВ'ЯЗКУ СБ УКРАЇНИ

Система радіозв'язку СБ України потребує впровадження сучасних цифрових технологій. Так, при використанні цифрових систем радіозв'язку значно

розширюється спектр тактичних можливостей оперативних підрозділів СБ України при проведенні контррозвідувальних та оперативно-розшукових заходів.

Використання аналогових систем радіозв'язку підрозділами СБ України збільшує фактор ризику втрати (безконтрольного витоку) оперативно-вагомої інформації стосовно об'єктів зацікавленості. Цифрові системи радіозв'язку мають набагато більший запас захисту інформації, а також дозволяють передавати текстові повідомлення, відео та фото зображення. Використання лінійно-диспетчерських терміналів, а також наявність GPS-модулів в абонентських станціях відкриває широкий спектр можливостей для користувачів, а саме:

- можливість постійної реєстрації всіх сеансів зв'язку та передачі даних (як мовних, так і фото), що забезпечує збереження та відтворення критично важливих сеансів зв'язку з метою їх подальшого аналізу;

- можливість надання абонентам, в режимі реального часу, доступу до необхідних баз даних, у ході проведення ними контррозвідувальних та оперативно-розшукових заходів;

- виключна живучість системи завдяки перемаршрутизації трафіку як у автоматичному режимі, так і в ручному;

- відображення на електронній мапі місця знаходження абонентських терміналів надає можливість координації усіх задіяних сил і засобів на важливих напрямках роботи.

Система цифрового зв'язку зворотно-сумісна з усіма існуючими системами аналогового зв'язку, за рахунок чого, має можливість долучати до себе абонентів інших систем при проведені широкомасштабних заходів.

Можливість використання цифрових скремблерів мовної інформації, Bluetooth-гарнітур значно підвищує конспіративність використання засобів зв'язку під час здійснення оперативних заходів.

Розглянемо варіанти організації роботи радіомереж стандарту DMR на базі обладнання MOTOTRBO та види шифрування інформації в них.

Обладнання системи MOTOTRBO реалізує кілька способів організації роботи радіомережі, такі як, багатозонний конвенціональний зв'язок IP site connect (з'єднання ретрансляторів по ланцюжку), однозоновий транкінг Capacity Plus (одна базова станція), багатозоновий транкінг Linked Capacity Plus (до 15 базових станцій), багатозоновий транкінг Connect+ (система з виділеним каналом управління).

В рамках стандарту DMR передбачається реалізація двох режимів конвенціонального зв'язку:

- режим прямого зв'язку (Direct mode) - симплексна зв'язок.

- режим зв'язку через ретранслятор (Repeater mode) з підтримкою технології двухчастотного симплекса з дуплексним розносом, FDD (Frequency Division

Duplex). В цьому режимі можливі два одночасних незалежних голосових з'єднання.

Таке рішення на сьогодні впроваджено в більшості обласних центрах України для роботи регіональних органів СБ України.

IP Site Connect є спеціалізованим варіантом побудови конвенціональної цифрової мережі радіозв'язку з використанням ретрансляторів (до 16) та абонентського обладнання.

Особливістю радіомережі IP Site Connect є те, що будь-яка активність абонентів у зоні дії одного ретранслятора, буде повністю повторена на всіх інших ретрансляторах включених в мережу IP Site Connect.

Подібний прозорий механізм дублювання радіотрафіка по всіх ретрансляторам дозволяє радіостанціям вільно переміщатися в межах радіомережі IP Site Connect і при цьому завжди залишатися на зв'язку: незалежно від місця розташування радіостанція завжди зможе прийняти свій виклик, ініціювати виклик потрібного абонента, працювати з передачею даних. Недоліком такого рішення є те, що додавання ретрансляторів в типову мережу IP Site Connect не призводить до збільшення пропускної здатності.

Однозонне багатоканальне рішення. Motorola Capacity Plus використовується, коли є потреба забезпечити радіозв'язком більшу кількість абонентів без збільшення зони покриття. Тобто, радіосистема зростає "не вшир, а вглиб" з можливістю об'єднання в одній зоні до 6 ретрансляторів (12 каналів) для передачі голосу і 12 каналів для передачі даних.

Багатозонова транкінгова система Linked Capacity Plus може об’єднати до 15 базових станцій.

Системи Capacity Plus і Linked Capacity Plus використовують технологію розподіленого управління, при якій в системі відсутній такий компонент як центральний комутатор – вся логіка управління роботою повністю знаходиться в пам'яті ретрансляторів, що постійно обмінюються службовою інформацією і відповідають за надання абонентам основних сервісів системи. Застосування розподіленого управління є ефективним в системах малого та середнього масштабу. Поканальний принцип побудови систем забезпечує поступове збільшення розмірів системи: від 2 логічних каналів передачі голосу на одному ретрансляторі система може бути збільшена до 15 базових станцій, що включають сумарно 240 логічних каналів для голосу і 120 логічних каналів даних.

Для захисту інформації від несанкціонованого доступу в професійних системах DMR використовується режим шифрування. Розрізнюють декілька видів шифрування в системі DMR:

- базове шифрування – метод шифрування, який робить просту математичну маніпуляцію з ключем шифрування і корисною інформацією (голосові і текстові повідомлення). Це не повний метод шифрування;

- алгоритм ARC4 з використанням 40-бітного ключа шифрування забезпечує високий рівень безпеки передавання інформації. Це є можливим завдяки тому що в алгоритмі ARC4 (та більш сучасному AES) забезпечується різні ключі шифрування для кожного голосового суперкадру або пакету даних, що вкрай ускладнює розшифрування даних після захоплення голосу або пакету даних. Режим AES, що використовує 256-бітний ключ шифрування забезпечує достатню ступінь безпеки передачи даних.

Враховуючи зазначене, реалії оперативної роботи в умовах збройної агресії рф та важливість завдань, що стоять перед підрозділами СБ України, використання цифрових транкінгових системи радіозв'язку надасть можливість забезпечити надійним, ефективним радіозв’язком підрозділи СБ України під час здійснення ними оперативно-службової діяльності.

Вдовенко С.Г.
Гулак Ю.С.
кандидат військових наук, доцент
Машталір В.В.
доктор історичних наук, професор
Національний університет оборони України

ЗАКОНОДАВЧІ, НОРМАТИВНО-ПРАВОВІ Й ДЕФІНІЦІЙНІ АСПЕКТИ ПРОБЛЕМ У СФЕРІ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ ТА СЛУЖБОВОЇ ІНФОРМАЦІЇ В УМОВАХ ВІЙНИ ТА ШЛЯХИ ЇХ ВИРІШЕННЯ

Досвід збройних конфліктів першій чверті XXI століття, в тому числі відбиття агресії російської федерації проти України, свідчить про зростання вимог до захисту інформації з обмеженим доступом (далі – ІзОД) адекватно до рівня загроз. Суспільні відносини, пов'язані з охороною державної таємниці (ОДТ) регулюються Законом [1], відповідно до вимог якого у ЗС України створена та діє система ОДТ, яка складається з підсистем: режиму секретності та секретного документального забезпечення; захисту інформації (криптографічного та технічного) (КЗІ, ТЗІ) та підсистеми технічного забезпечення [2]. Забезпечення ОДТ [1] та іншої інформації з обмеженим доступом (ІзОД), поряд з КЗІ, і ТЗІ, протидією технічним розвідкам (ПДТР), системою надання кваліфікованих електронно-довірчих послуг (КЕДП) є однією з основних складових частин скритого управління військами (силами) (далі - СУВ). Ці погляди ГШ ЗС України, спираючись на вимоги [3-5] ґрунтуються на практиці бойових дій в умовах широкомасштабної збройної агресії рф та дещо відрізняється від тлумачення викладеного у [6], яке не враховує необхідності захисту службової інформації. Хоча переважна кількість інформації що циркулює при управлінні військами

(силами) в ході підготовки і ведення операції ЗС України належить до службової інформації, що підтверджується [7]. Протиріччя зазначені у таблиці 1. Частково це протиріччя усунуто з прийняттям [8] та у разі прийняття [9].

Таблиця 1

Мирний час	**Особливий період**
Охорона державної таємниці	**Система СУВ**
1. система ОДТ	1. підсистема ОДТ
2. система КЗІ	2. підсистема КЗІ
3. система ТЗІ	3. підсистема ТЗІ
4. система ПДТР	4. підсистема ПДТР
5. -	5. підсистема НКЕДП
6. режим секретності	Впроваджується відповідно до розпорядження зі СУВ органу військового управління вищого рівня та Плану СУВ на операцію
7. оперативно-розшукові заходи	Проводяться автономно уповноваженими органами відповідно до [8, 10, 11], поза рамками Плану СУВ – задача для ЗС не притаманна
Захист іншої інформації з обмеженим доступом	
система НКЕДП	див. п. 5 таблиці
Захист службової інформації – увійде до системи ОДТ та ІзОД, див п. 1 таблиці [8, 9].	задача визначена – підсистема не зазначена

Сучасна нормативно-правова база (далі - НПБ) України сфер ОДТ та ІзОД перебуває в стадії формування та має низку протиріч, які умовно можна об’єднати в три групи:

1.Дефініційно-термінологічні розбіжності НПБ України сфер ОДТ та ІзОД.

2. Нормативно-правові розбіжності НПБ України сфер ОДТ та ІзОД.

3. Законодавчі, нормативно-правові, дефініційно-термінологічні розбіжності між НПБ сфер ОДТ та ІзОД України та сфери безпеки класифікованої інформації (далі – БКІ) міжнародного співтовариства.

Перша група протиріч, полягає в недотриманні вимог розділу лексикології – термінології, в якої аксіомою є те, що визначення будь якого терміну (дефінієндума, Dfd) та зміст і значення визначаючого поняття (дефінієнса, Dfn) мають бути тотожними, вичерпувати один одного і мати один і той же денотат (зміст). До науково-технічних і військових термінів висуваються додаткові вимоги: системність, вмотивованість, однозначність, точність, відсутність

синонімів [11, 12]. У терміносистемі ОДТ одночасно існує й паралельно застосовується низка дефініцій, в яких одному Dfd ставиться у відповідність декілька Dfn. Наприклад дефініція “СУВ” в [6] та доктринальних документах ЗС України мають різні Dfn. Або навпаки, один Dfn розкриває значення різних Dfd, наприклад “державна таємниця” – “секретна інформація” згідно [1], що є ознакою синонімічності. В іншому документі стратегічного планування [14] синонімічно вживається термін “приховане управління”. Термінологічна сфера БКІ, в Україні ще не сформована, тим не менш, процесу її формування притаманні зазначені помилки. Ускладнення цього протиріччя в площині практичного застосування термінологічного апарату сфери БКІ відбувається за рахунок невідповідності термінологічних систем міжнародного співтовариства, зокрема ЄС та НАТО й України.

Щодо другої групи, то існують серйозні протиріччя між законодавчою та НПБ України у сфері ОДТ, сучасними вимогами щодо захисту ІзОД з урахуванням досвіду ЄС та НАТО. Закон [1] та законопроєкт [9] на Раду національної безпеки і оборони України, Кабінет Міністрів України покладаються повноваження щодо спрямування, координації та контролю діяльності із забезпечення реалізації державної політики у сфері ОДТ, які фактично зараз виконуються СБУ, що є спеціально уповноваженим державним органом у сфері забезпечення ОДТ [3] та має стати національним органом безпеки з розширеними повноваженнями [9]. Позитивним у [9] є визначення повноважень органам судової влади. А одним з суттєвих недоліків - слід вважати застосування ступенів класифікації значущої для безпеки держави інформації: “Особливої важливості”, “Цілком таємно”, “Таємно”. Крім України подібні ступені секретності та відповідні ним грифи, законодавчо визначені та застосовуються в Азербайджані, Білорусі, Вірменії, Казахстані, Киргизії, рф, Таджикистані. Градація важливості інформації в більшості країн і міжнародних організацій має 4 ступені, що переважно відповідають аналогам США (TOPSECRET, SECRET, CONFIDENTIAL, RESTRICTED). Ступені класифікації інформації в законодавстві України доцільно приводити до 4-рівневої моделі, розглянувши питання щодо їх семантичного навантаження близько до прийнятих у державах ЄС та НАТО. Класифікація інформації окремих держав та міжнародних організацій наведена у таблиці 2.

Таблиця 2.

Україна	Особливої важливості	Цілком таємно	Таємно	
рф	Особой важности	Совершенно секретно	Секретно	
США	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED*

НАТО	NATO COSMIC TOP SECRET	NATO SECRET	NATO CONFIDENTIAL	NATO RESTRICTED
ЄС	EU TOP SECRET	EU SECRET	EU CONFIDENTIAL	EU RESTRICTED
ESA Європейська Космічна Агенція	ESA TOP SECRET	ESA SECRET	ESA CONFIDENTIAL	ESA RESTRICTED
OCCAR Організація співробітництва у галузі озброєнь	OCCAR TOP SECRET	OCCAR SECRET	OCCAR CONFIDENTIAL	OCCAR RESTRICTED

Одна з невідповідностей третьої, найбільшої, групи протиріч між законодавчою та НПБ України у сфері ОДТ, сучасними вимогами щодо захисту ІзОД з урахуванням досвіду ЄС та НАТО розкрита у таблиці 3.

Таблиця 3.

Держава	Орган державної безпеки	Підпорядков.	Орган військової контррозвідки	Підпорядков.
Греція	Міністерство громадського порядку (МОП) – контррозвідка	Міністр внутрішніх справ	Відділ “Е” (Альфа-2) Генерального штабу – військова розвідка и контррозвідка.	Начальник ГШ
Польща	Агентство внутрішньої безпеки	Прем’єр-міністр	Служба військової контррозвідки	Міністр оборони
Румунія	Служба розвідки Румунії – внутрішня розвідка.	Прем’єр-міністр	Директорат військової безпеки у складі Генерального директорату розвідки МО Румунії	Міністр оборони
НАТО	Бюро безпеки НАТО – окремий орган, на який покладене завдання реалізації політики безпеки НАТО	Генеральний секретар з питань розвідки та безпеки	Об’єднаний підрозділ розвідки та безпеки NATO (JISD)	Генеральний секретар з питань розвідки та безпеки

Наприклад, факт визначення в [8, 9] національним органом безпеки СБУ, що згідно [8, 10] є державним органом спеціального призначення з правоохоронними функціями, суперечить вимогам ЄС та НАТО, які передбачають в НАТО і кожній державі-члені НАТО мати урядове бюро національної безпеки (National Security Organization – NSO), що відповідає за інформаційну безпеку та персонал, збір і реєстрацію відомостей щодо шпигунства та підривної діяльності, та яке не входить до інших державних структур, тим більш - до правоохоронних [15, 16]. В [17] відмічається, що у ряді країн функції НОБ покладаються на національні спецслужби (Греція, Польща, Румунія), які не є правоохоронними органами. З огляду на зазначене з метою вирішення проблем у сферах ОДТ та захисту ІзОД (БКІ) в державі вважається за доцільне здійснити усунення невідповідностей шляхом законодавчого, нормативно-правового й дефініційного врегулювання у сфері БКІ з урахуванням досвіду ЄС та НАТО, як то визначено в [18, 8, 14].

Література

1. Закон України “Про державну таємницю” від 21 січня 1994 року N 3855-XII, зі змінами

2. Вдовенко С.Г. Сучасні вимоги до охорони державної таємниці та захисту інформації з обмеженим доступом в особливий період // Імперативи розвитку цивілізації – 2015 – №2. Київ – ФОП О.С. Ліпкан, С. 93-96.

3. Закон України “Про оборону України” від 6 грудня 1991 № 1932-XII, зі змінами

4. Закон України “Про Збройні Сили України” від 6 грудня 1991 № 1934-XII, зі змінами

5. Закон України від 18 січня 2018 року № 2268-VIII “Про особливості державної політики із забезпечення державного суверенітету України на тимчасово окупованих територіях”

6. Звід відомостей, що становлять державну таємницю, затверджений наказом СБУ від 23.12.2020 N 383, зареєстрований в Міністерстві юстиції України 14.01.2021 за № 52/35674.

7. Перелік відомостей Збройних Сил України, що становлять службову інформацію (ПСІ-2023), затверджений наказом Генерального штабу від 30.01.2023 № 12.

8. Стратегія забезпечення державної безпеки, затверджена Указом Президента України від 16.02.2022 № 56/2022

9. Законопроект 8394 “Про безпеку класифікованої інформації” від 27.01.2023

10. Закон України “Про Службу безпеки України” від 25 березня 1992 N 2229-XII зі змінами 11. Закон України про “Оперативно-розшукову діяльність”.

12. Новейший философский словарь, [Електронний ресурс] – Режим доступу: https://www.google.com/search?q=chrome..69i57.9536j0j8&sourceid=chrome&ie=UTF

-8
13. Л.А. Васенко, В.В.Дубічинський, О.М. Кримець, Фахова українська мова:. Навчальний посібник. К.: Центр учбової літератури, 2008. - 272 с., [Електронний ресурс] – Режим доступу: http://uchebniks.com/book/277-faxova-ukrayinska-mova-navchalnij-posibnik-vasenko-la/23-vimogi-do-terminiv.html
14. Стратегічний оборонний бюлетень України затверджений Указом президента України від 17.09.2021 № 473/2021 "Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року"
15. Security Within the North Atlantic Trean Organisation (NATO), Note by the Secretary General. Document C-M(2002) 49, may 2013. Режим доступу: http://arhives.nato.int/amendments-to-nato-c-m-55-15 final
16. Hans Born, Marina Caparini, Democratic Control of Intelligence Services, Containing Rogue Elefants, 2007, MPG Books Ltd, Bodmin, Comwall, 303 p.p.
17. Болдир С.В. Перспективи реформування системи охорони державної таємниці та службової інформації //"Інформація і право" № 4(23)/2017
18. Конституція України [Електронний ресурс] – Режим доступу: http://zakon0.rada.gov.ua/laws/show/254

Волощенко А.С.
кандидат технічних наук, с.н.с. полковник
Кошманов М.О.
кандидат технічних наук підполковник

ВЛАСНА БЕЗПЕКА ПЕРСОНАЛУ, ЯК СКЛАДОВА ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ В УМОВАХ ВІЙСЬКОВОГО СТАНУ

В умовах повномасштабного військового вторгнення росії в Україну, небувалої за своїми масштабами терористичної агресії (постійні ракетні та інші обстріли), агресії проти нашої держави у кіберпросторі (90 відсотків кібератак здійснюють військові хакери рф та білорусі, діяльність яких фінансується владою) у зону ризиків потрапили підприємства, установи та організації як цивільної інфраструктури (державного та приватного сектору) так і сектору оборони (далі – підприємства ЦІ та СО). [1] Одними з основних загроз на даний час є зменшення дієздатності та ефективності зазначених інституцій України та послаблення їх захисту від будь-яких спроб втручання (ззовні та зсередини). Особливої актуальності за таких умов набувають заходи із забезпечення надійного захисту інформації з обмеженим доступом, що циркулює у інформаційних масивах інформаційно-телекомунікаційних систем (далі – ІТС) та

автоматизованих систем (далі – АС) цих інституцій, які б дозволяли ефективно протидіяти та вчасно реагувати на виникаючі сучасні загрози витоку інформації.

Важливим елементом захисту ІТС та АС, що є власністю підприємств ЦІ та СО від несанкціонованих витоків інформації, є якісно організована власна безпека персоналу, який безпосередньо приймає участь у функціонуванні систем обробки даних, використанні їх ресурсів, яка здійснюється на конкретному об'єкті інформаційної діяльності. Так, під час здійснення ефективних заходів із збезпечення власної безпеки персоналу, можливо на початковому етапі виявити потенційні внутрішні та зовнішні загрози витоку інформації.

За результатами аналізу, здійсненому зарубіжними партнерами встановлено, що за останні роки близько 20 % усіх німецьких компаній стали жертвою промислового шпигунства. Витік інформації відбувався різними шляхами. Приблизно у 15 % випадків конкуренти хакерськими способами підключались до внутрішніх баз даних. У 20 % мала місце нелояльність власних співробітників. У 18,7 % співробітники компанії були залучені до конфіденційного співробітництва фірмою конкурентом або іноземною спецслужбою з метою передачі конфіденційної інформації [2, 49].

Таким чином, безпосередньо недоліки та помилки що припущені керівниками під час організації на підприємстві належного рівню власної безпеки персоналу, спричинили витік конфіденційної інформації, що сумарно набирає 38,7 % і більше ніж у два рази перекриває ефект від технічного проникнення до баз даних. Одночасно слід відмітити, що здобування інформації із залученням конфідентів здійснюється й з використанням технічних засобів, а технічну розвідку в основному ведуть люди (як правило досвідчені розвідники) [2, 49].

В той же час, жоден технічний засіб контролю діяльності особи, що залучена розвідниками до конфіденційного співробітництва не в змозі помітити ті тонкі, а іноді й ледве розпізнавальні зміни його поведінки, які при особистому спілкуванні проявляються лише у певних ситуаціях і уловлюються виключно на рівні підсвідомості [2, 50].

Тому, з огляду на існуючі сучасні загрози, які виникли перед зазначеними суб'єктами системи обробки даних ІТС та АС (у т.ч. використання ресурсів, що містять інформацію з обмеженим доступом), важливим елементом забезпечення заходів з їх захисту є ефективна власна безпека підприємсва, яка передбачає професійний супровід діяльності персоналу, що працює безпосередньо з цими системами та забезпечує дотримання вимог режиму охорони інформації з обмеженим доступом. Так, передбачається застосування широкого спектру психологічної допомоги, профілактичної діяльності, залучення досвідчених фахівців у цих сферах, що суттєво має мінімізувати ризики вербальної уразливості персоналу *(організація семінарів, вебінарів, круглих столів тощо за участю компетентних фахівців діючих підрозділів внутрішньої/власної безпеки розвинутих підприємств, проведення співбесід, опитувань, за необхідності з*

використанням поліграфу, тестувань тощо). При цьому, важливим елементом організації якісної власної безпеки підприємства, є і кадрова безпека, яка має охоплювати:

- сукупність принципів, методів спрямованих на збереження, зміцнення й розвиток кадрового потенціалу підприємства, на створення згуртованого колективу, здатного вчасно реагувати на постійно мінливі зовнішні загрози;
- становище організації як соціальної спільності й індивіда в ній, за якого вплив на них із боку природного, економічного й соціального середовищ, а також внутрішнього середовища колективу та самої людини не здатні заподіяти шкоди;
- процеси запобігання негативних впливів на економічну безпеку підприємства за рахунок ризиків і загроз, пов'язаних з персоналом, його інтелектуальним потенціалом і трудовими відносинами ;
- стан захищеності підприємства від ризиків і загроз, пов'язаних із персоналом;
- сукупність заходів, спрямованих на запобігання протиправних дій або сприяння їм з боку персоналу підприємства [5].

Отже, кадрова безпека в цілому має враховувати безпеку життєдіяльності (безпека здоров'я, фізична безпека), соціально-мотиваційну складову (фінансова безпека, кар'єрна безпека, технологічна безпека, естетична безпека, адміністративна безпека), професійну (безпека праці, інформаційна безпека, інтелектуальна безпека, пенсійно-страхова безпека, правова безпека, підвищення фахового рівня тощо) та антиконфліктну безпеку (психологічна безпека, патріотична безпека, комунікаційна безпека) [5].

Також, кадрові підрозділи і підрозділи власної безпеки мають постійно здійснювати моніторинг зовнішньої/внутрішньої небезпеки підприємства *(кращі умови мотивації у конкурентів, «переманювання», зовнішній тиск на персонал, втягування співробітників у різні види залежності, схильності окремих співробітників до сугестивності, прийняття навіюваності та інших впливів),* якими можуть скористатися спецслужби країни агресорки [3; 5].

Разом з тим, ще і досі існують певні проблемні питання, які виникають під час організації заходів, спрямованих на підвищення рівня безпеки (захисту) циркулюючої в ІТС та АС інформації.

Зокрема, у більшості випадків створення належної кількості нових комплексних систем захисту інформації (далі - КСЗІ) в ІТС та АС ускладнюється технічними й фізичними можливостями профільних підприємств та організацій (недостатня кількість співробітників, обладнання та часу, що потрібно витратити на проведення робіт з інструментального контролю, проведення обробки їх результатів, підготовці відповідних документів тощо) [4].

Крім того, на даний час актуальним питанням залишається необхідність залучення нових джерел фінансування для вирішення потреб у заміні застарілих атестованих АС на об'єктах електронно-обчислювальної техніки, де

використовуються атестовані АС вже понад 10-12 років, які ще працюють але мають частково технічні несправності й можуть вийти з ладу у будь який час. Над вирішенням цього питання необхідно працювати системно, а саме, постійно: доводити до керівників, що приймають управлінські рішення та відповідають за матеріально-технічне забезпечення діяльності підприємства необхідність включення у бюджети створення нових КСЗІ; здійснювати пошук альтернативних джерел фінансування (пошук волонтерів, участь зацікавлених небайдужих співробітників підприємства, використання технологій фандрейзингу, спільнокоштом (краудфандингові платформи), донорськими програмами тощо).

Водночас, на окремих підприємствах, для низки ПЕОМ придбаних до 2020 року існує проблемне питання, пов'язане з відсутністю ліцензійних операційних систем (нові ПЕОМ підтримують тільки операційні системи з версіями Windows 8 та Windows 10) [4].

В окремих випадках має місце послаблення управлінського впливу з боку окремих керівників підприємств, де здійснюється обробка циркулюючої у ІТС та АС інформації з обмеженим доступом, в частині здійснення належного контролю за діяльністю підлеглих. Як наслідок, виникають передумови до витоку інформації з обмеженим доступом, на підставі чого призначаються відповідні службові перевірки і розслідування [4].

Також, в окремих підприємствах потребує удосконалення організація дотримання вимог власної (внутрішньої) безпеки персоналу, який задіяний у обробці циркулюючої у ІТС та АС інформації з обмеженим доступом, та організація системної роботи співробітників кадрових підрозділів у напрямку постійного підвищення їх професійного та морального рівня, контролю психоемоційного стану, вербальної уразливості [4].

Отже, сукупність заходів щодо удосконалення: 1) управлінського контролю за персоналом суб'єктів системи обробки даних ІТС та АС; 2) організації ефективної власної (внутрішньої) та кадрової безпеки на підприємстві; 3) залучення альтернативних джерел фінансування для створення у необхідної кількості нових КСЗІ; створить сприятливі умови для мінімізації ризиків витоку інформації з обмеженим доступом, і, як наслідок, суттєво посилить захищеність підприємств цивільної інфраструктури та сектору оборони і правоохоронних органів від загроз витоку інформації з обмеженим доступом, що виникли в умовах військового стану.

Література

1. Офіційний сайт Державної служби спеціального зв’язку та захисту інформації України. - [Електронний ресурс] – Режим доступу: https://cip.gov.ua/news/vimogi-do-zakhistu-informaciyi-v-informaciinikh-sistemakh-u-voyennii-chas-roz-yasnennya-derzhspeczvyazku.

2. Лебедєв О.Р. Методи збирання розвідінформації: аналіз іноземного досвіду. Науковий журнал «Інформаційна безпека» № 2, 2018. К.: НА СБ України- С. 45-52.

3. Зарицька О.В., Іванова Н.Г., Андрусишин Ю.І. Методичні рекомендації «Психологічні особливості виявлення співробітниками СБ України ознак маніпулятивної поведінки» 2016- К.: НА СБ України - С.9.

4. Волощенко А.С., Кошманов М.О. «Людський фактор у забезпеченні збережності інформації, що обробляється у відомчих ІТС», Збірник матеріалів відомчої науково-практичної конференції «Актуальні проблеми ОСД СБУ в умовах воєнного стану» 2022-К.: НА СБ України – С. 68-70.

5. Кравченко В.О. «Кадрова безпека – основа економічної безпеки підприємства» 2014. О. - [Електронний ресурс] – Режим доступу: https://core.ac.uk.

Зизич І.І.
НА СБ України
Наукові керівники:
Кононова Д.В.
канд. філол. наук, доцент НА СБ України
Кобус О.С.
канд. фіз.-мат. наук ННІ ІБ НА СБ України

ЩОДО ПИТАНЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, ЗАХИСТУ ІНФОРМАЦІЇ, У ТОМУ ЧИСЛІ З ОБМЕЖЕНИМ ДОСТУПОМ (ДЕРЖАВНОЇ ТАЄМНИЦІ), В УМОВАХ ЗБРОЙНОЇ АГРЕСІЇ рф

В умовах гібридної війни з рф критично важливим є забезпечення державної безпеки шляхом захисту інформації з обмеженим доступом. Щоб розуміти про що йде мова, потрібно дати визначення поняттям інформації з обмеженим доступом. Відповідно до частини першої статті 21 Закону України «Про Інформацію» «інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація»; «конфіденційна інформація - інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов» (ч.1 ст. 7 ЗУ «Про доступ до публічної інформації); «таємна інформація - інформація, доступ до якої обмежується відповідно до частини другої статті 6 цього Закону, розголошення якої може завдати шкоди особі, суспільству і державі. Таємною визнається інформація, яка містить державну, професійну, банківську, розвідувальну таємницю, таємницю

досудового розслідування та іншу передбачену законом таємницю» (ч. 1 ст. 8 ЗУ «Про доступ до публічної інформації»).

Відповідно до частини першої статті 9 Закону України «Про доступ до публічної інформації» до службової може належати така інформація:

1) що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень;

2) зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

Ворог кожен день намагається впливати на суспільство в Україні через дезінформування, пропаганду, кібератаки на інформаційні об’єкти (телеканали, соціальні мережі, інтернет-ресурси тощо), в тому числі на інформацію з обмеженим доступом.

Історично склалося, що загрози слід поділяти на дві великі групи: зовнішні та внутрішні. До внутрішніх загроз можна віднести шпигунство з боку суб’єктів забезпечення інформаційної безпеки, надання відомостей, що становлять державну таємницю іноземним державам, організаціям або їх представникам. Щодо зовнішніх загроз то це: розвідувально підривна діяльність іноземних спецслужб, кібертероризм, пропаганда тощо. Виникає питання, як та кому захищати інформацію, в тому числі державну таємницю, розголошення якої може завдати значної шкоди національним інтересам держави та суспільства.

По-перше, слід визначити суб’єктів захисту інформаційної складової держави. Одним з них є Служба безпеки України. Відповідно до статті 5 ЗУ «Про державну таємницю» «спеціально уповноваженим державним органом у сфері забезпечення охорони державної таємниці є Служба безпеки України». Держава, міністерства, зокрема Міністерство з питань культури та інформаційної політики, а також Міністерство оборони, які теж в свою чергу є суб’єктами забезпечення інформаційної безпеки.

По-друге, треба розуміти якими методами та засобами можна протидіяти загрозам, які виникають. Їх можна умовно розділити на:

-**Профілактичні методи** - це ті, які використовуються для запобігання потенційним загрозам, наприклад діяльність центрів протидії дезінформації;

-**Правові методи**. До них слід віднести закони, постанови кабміну, укази президента тощо;

-**Технічні засоби**. Слід виділити пристрої криптографічного захисту, які дозволяють шифрувати потрібну інформацію;

-**Програмні засоби**. Сюди можна віднести різні застосунки, які допомагають боротися з шкідливими ПЗ, вірусами тощо

Отже, враховуючи вищезгадане, можна дійти висновку, що одними з найбільших проблем, які існують на даний момент є забезпечення інформаційної безпеки, захист інформації та протидія розвідувально-підривній діяльності іноземних спецслужб. Протидія цим загрозам є надважливою складовою для забезпечення державної безпеки, а постійне вдосконалення механізмів боротьби з ними, в умовах гібридної війни є основою для настання миру та відсічі збройної агресії рф.

Література

2. Закон України «Про інформацію» [Редакція від 01.01.2023 р.]. https://zakon.rada.gov.ua/laws/show/2657-12#Text
3. Закон України «Про державну таємницю» [Редакція від 15.03.2022 р.]. https://zakon.rada.gov.ua/laws/show/3855-12#Text
4. Закон України «Про доступ до публічної інформації» [Редакція від 01.01.2023 р.]. https://zakon.rada.gov.ua/laws/show/2939-17#n40
5. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки": указ Президента України від 28 грудня 2021 р. №685/2021. https://www.president.gov.ua/documents/6852021-41069
6. Гребенюк А. М., Рибальченко Л.В. Основи управління інформаційною безпекою : навчальний посібник, 2020. С. 76-82.

Глинчак Ю.Я.
студент Національної академії СБ України

ПРОБЛЕМНІ ПИТАННЯ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ В УМОВАХ ЗБРОЙНОЇ АГРЕСІЇ рф

У сучасних умовах інформаційна безпека є однією з найбільш актуальних проблем. Особливо важливою вона стає в умовах збройної агресії російської федерації, коли збільшується кількість зловмисників, які займаються кібератаками та іншими видами кіберзлочинності з метою отримання інформації з обмеженим доступом. Такі напади можуть завдати значної шкоди як національній безпеці країни, так і окремим користувачам, чия конфіденційна інформація може бути викрадена.

Одним із основних проблемних питань у сфері захисту інформації з обмеженим доступом є забезпечення безпеки інформаційних систем. Згідно з дослідженнями, найбільші загрози існують для таких інформаційних систем, як системи електронної пошти та бази даних з обмеженим доступом [1]. Зокрема, зловмисники можуть використовувати різноманітні методи для злому таких

систем, наприклад, використовуючи вразливості в програмному забезпеченні або за допомогою соціальної інженерії.

Ще одним проблемним питанням є забезпечення фізичної безпеки інформації. Умови збройної агресії рф можуть призвести до того, що користувачі не зможуть фізично зберегти свою інформацію в безпечному місці. Наприклад, в разі зайняття території ворогом, обладнання та приміщення, де зберігається конфіденційна інформація, можуть потрапити в руки ворога [2].

Окрім цього, проблемним питанням є забезпечення правильного використання обладнання та програмного забезпечення. Якщо користувач не знає, як правильно використовувати засоби захисту, то його інформація може стати вразливою для кібератак. Також, важливо, щоб інформаційні системи та засоби захисту були завжди оновлені до останньої версії, щоб запобігти використанню вразливостей, які можуть бути використані для злому системи.

Відповідно до різних досліджень, у світі існує велика кількість загроз, пов'язаних з кіберзлочинністю та кібератаками [3]. Умови збройної агресії рф призводять до того, що такі загрози можуть стати ще більш серйозними, оскільки збільшується кількість зловмисників, які можуть використовувати кіберзлочинність як зброю.

Висновки. Таким чином, захист інформації з обмеженим доступом є однією з найбільш актуальних проблем у сучасному світі, особливо в умовах збройної агресії рф. Основними проблемними питаннями є забезпечення безпеки інформаційних систем, фізичної безпеки інформації та правильного використання обладнання та програмного забезпечення. Щоб запобігти кіберзлочинності та кібератакам, необхідно підтримувати системи та засоби захисту в оновленому стані і забезпечувати належне навчання користувачів їх правильному використанню.

Проте, проблеми захисту інформації з обмеженим доступом в умовах збройної агресії рф не можуть бути вирішені лише на рівні окремих користувачів чи підприємств. Для ефективного захисту інформації потрібно систематично працювати на рівні державної політики та міжнародної співпраці.

Можна виділити такий перелік проблем та їх вирішень у сучасних реаліях інформаційної безпеки за умови військової агресії рф:

1. Збройна агресія рф суттєво підвищує загрозу для інформаційної безпеки, зокрема для захисту інформації з обмеженим доступом.

2. Однією з найбільш актуальних проблем є забезпечення цілісності і конфіденційності інформації в умовах збройної агресії рф.

3. Застосування спеціальних технологій та методів шифрування може бути ефективним способом захисту інформації з обмеженим доступом в умовах збройної агресії рф.

4. З метою підвищення ефективності захисту інформації з обмеженим доступом необхідно проводити систематичний аналіз потенційних загроз та розробляти відповідні стратегії захисту.

5. Важливим елементом захисту інформації з обмеженим доступом є забезпечення безпеки фізичних місць, де зберігається ця інформація, а також забезпечення контролю доступу до неї.

6. Необхідно проводити регулярні тренування та навчання персоналу з питань захисту інформації з обмеженим доступом в умовах збройної агресії рф.

Література

1. Кривенко, І. О., Кох, І. В. Захист інформації з обмеженим доступом на підприємствах енергетичного комплексу. Економіка та суспільство, 2016. 436-440.

2. Яценко, А. В., Семенов, О. В. Аналіз методів та засобів захисту інформації з обмеженим доступом. Науковий вісник Херсонського державного університету. Серія: Технічні науки, 2016. 87-92.

3. Cybersecurity Ventures. Cybercrime statistics & facts for 2021. Retrieved from https://cybersecurityventures.com/cybercrime-damage-costs-6-trillion-by-2021/

Гуз А.М.
доктор історичних наук, професор
Національна академія Служби безпеки України

СКЛАДАННЯ СИСТЕМИ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ У КРАЇНАХ ЦЕНТРАЛЬНО-СХІДНОЇ ЄВРОПИ В ДРУГІЙ ПОЛОВИНІ XX СТ. – НА ПОЧАТКУ XXI СТ.

Життя у сучасному світі дуже швидко глобалізується. Цим процесам піддані різні галузі життєдіяльності, навіть така чутлива сфера як державна таємниця. Нині у кожній країні Центрально-Східної Європи (країни Балтії, Балкан, Вишеградської четвірки) створені дієві механізми охорони державної таємниці. Разом з тим, співпраця між країнами Центрально-Східної Європи, а також частини у межах Північноатлантичного альянсу та ЄС спонукала до прийняття стандартів цих організацій і у зазначеній сфері. Хоча кожна країна Центрально-Східної Європи має свої специфічні підході у охороні цього важливого виду інформації з обмеженим доступом, зараз чітко прослідковуються єдині принципи, на яких побудована їх система охорони державної таємниці. Практично у кожній країні Центрально-Східної Європи громадяни, які працюють з відомостями, що складають державну таємницю мають відповідати встановленим критеріям та здійснюється їх перевірка, у зв’язку із наданням їм допуску до такого виду інформації. Також характерні механізми режимних обмежень на підприємствах,

установах, що провадять таку діяльність. Варто відмітити і ведення секретного діловодства, засекречування, використання та зберігання матеріальних носіїв секретної інформації тощо.

Разом з тим зазначимо, що низці країн Центрально-Східної Європи (Болгарія, Хорватія, Естонія, Угорщина, Латвія, Литва, Польща, Румунія, Словаччина, Словенія, Чехія, Чорногорія, Північна Македонія) притаманні три основні етапи (періоди) становлення системи охорони державної таємниці.

Перший – початковий етап формування системи охорони державної таємниці країн Центрально-Східної Європи, з 40-х років XX ст. до 1988 року. Цей період характеризується поширенням радянських принципів охорони державної таємниці на окреслені країни під час політичного співробітництва у межах Варшавського договору.

Напрацьовані механізми охорони державної таємниці у цих країнах проіснували до 1988 року. У 1989 році у країнах Центрально-Східної Європи проходять «оксамитові революції», розпадається система політичного співробітництва у межах Варшавського договору.

Після звільнення цих країн від радянського впливу вони до кінця 90-х років XX ст. відновлюють правові механізми охорони державної таємниці незалежних, суверенних країн. Зміни були пов'язані з будівництвом нових органів державної влади, у тому числі й тих, які відповідали за питання охорони державної таємниці.

Саме це є другий етап – будівництво власних незалежних систем охорони секретів країн Центрально-Східної Європи з врахуванням політичних змін всередині країн, а також трансформації органів державного управління після «оксамитових революцій» та розпаду Варшавського договору (1989-1998 роки).

Третій етап – це період удосконалення системи охорони державної таємниці країн Центрально-Східної Європи та приведення її у відповідність до вимог Організації Північноатлантичного договору та Європейського Союзу, міжнародних договорів та світових стандартів (1999 – 2022 роки).

Цей період також характеризується прийняттям законів про захист секретної інформації, про захист класифікованої інформації.

Також для цього періоду характерно внесення змін до законодавства, яке регулювало питання охорони секретів країн. Законодавство, яке регулювало охорону державних секретів було доповнено положеннями законодавства цієї сфери Організації Північноатлантичного договору та Європейського Союзу. Крім того, законодавство цих країн доповнено угодами між країнами та Організацією Північноатлантичного договору про захист інформації, двосторонніми угодами про взаємний захист секретної інформації.

Князєв С.О.
кандидат юридичних наук, с.н.с. полковник

ВАЖЛИВІСТЬ ВВЕДЕННЯ В ДІЮ ТА ВИКОРИСТАННЯ ЗВОДУ ВІДОМОСТЕЙ, ЩО СТАНОВЛЯТЬ ДЕРЖАВНУ ТАЄМНИЦЮ ДЛЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Інформаційна безпека України визначається як складова частина національної безпеки, й включає стан захищеності, у тому числі, життєво важливих інтересів держави, у контексті збирання, зберігання, поширення та доступу до інформації.

Звідти, постійної актуальності для держави набувають питання пов'язані із обігом державної таємниці, оскільки неправомірне використання даного виду інформації з обмеженим доступом може безпосередньо завдати шкоди національній безпеці.

Особливості використання державної таємниці розмежовуються відповідно до її важливості яка визначається за допомогою Зводу відомостей, що становлять державну таємницю України (далі - ЗВДТ).

Закон України «Про державну таємницю» визначає ЗВДТ як акт, в якому зведено переліки відомостей, що згідно з рішеннями державних експертів з питань таємниць становлять державну таємницю у визначених цим Законом сферах.

Практична цінність використання ЗВДТ полягає у тому, що саме він стає підставою для засекречування матеріальних носіїв секретної інформації (далі - МНСІ), а у подальшому і можливого розсекречування МНСІ.

Надання МНСІ відповідних грифів секретності під час засекречування дозволяє виділити їх важливість для держави та встановити необхідний рівень охорони.

У цьому році виповнюється 28 років введенню в дію першого ЗВДТ незалежної України.

Варто відзначити, що наша країна стала першою на пострадянському просторі яка відмовилась від радянських «Переліків відомостей, що становили державну таємницю СРСР».

Безперечно це був прогресивний крок від тоталітарного минулого до створення нового демократичного суспільства у якому правомірність отримання і обмеження доступу до інформації повинна гарантуватись державою із дотриманням життєво важливих інтересів людини, суспільства і держави.

ЗВДТ став єдиною формою реєстрації відомостей, що становлять державну таємницю в Україні. З моменту опублікування ЗВДТ держава забезпечує захист і правову охорону відомостей, які зареєстровані в ньому.

Понад чверть століття використання державою ЗВДТ вже не малий термін, який у цілому засвідчив його дієвість для інформаційної безпеки України.

Загалом, введення в дію ЗВДТ пов’язано із створенням в Україні, так званого, Інституту державних експертів з питань таємниць – уповноважених посадових осіб, які здійснюють віднесення інформації у сферах де циркулює державна таємниця до державної таємниці, забезпечують зміну ступеня секретності цієї інформації та її розсекречування.

Створення Інституту державних експертів з питань таємниць стало однією з принципово нових рушійних сил щодо реалізації інформаційної політики у сфері охорони державної таємниці в Україні, оскільки його запровадження здійснювало перехід до виправданого багаторічною практикою розвинутих країн світу порядку, який надає можливість науково обґрунтованого віднесення інформації до державної таємниці, забезпечення персональної відповідальності за прийняття рішень стосовно визначення ступеня секретності інформації.

У 1995 році в Інституті державних експертів працювало 143 державних експерти, на яких ці функції були покладені відповідним Указом Президента України.

На підставі прийнятих ними близько 350 рішень про віднесення інформації до державної таємниці було сформовано і введено у дію 31 липня 1995 року перший ЗВДТ незалежної України.

Його прийняття створило правові умови для виділення із загального інформаційного ресурсу нашої країни інформації, яка становила державну таємницю і підлягала захисту з боку держави.

Поява ЗВДТ надавала, у тому числі, змогу установам розробити передбачені законодавством відомчі переліки відомостей, що становлять державну таємницю, з метою визначення підстав для надання, зниження чи зняття грифу секретності з документів та виробів, які створювали в цих установах та у підпорядкованих їм структурах, а також визначати належність до державної таємниці України великого масиву секретних документів і виробів, які залишалися на той час від колишнього СРСР.

У 1999 році, згідно із змінами у законодавстві, спеціально уповноваженим державним органом у сфері забезпечення охорони державної таємниці визначається Служба безпеки України (далі – СБ України). Відповідно, ЗВДТ починає формувати СБ України на підставі рішень державних експертів з питань таємниць.

ЗВДТ та зміни до нього набирають чинності з моменту опублікування в офіційних виданнях України.

У березні 2001 року, наказом Голови СБ України, після державної реєстрації у Міністерстві юстиції України та відкритого опублікування в офіційних виданнях вводиться у дію другий ЗВДТ.

Третій ЗВДТ вводиться у дію в серпні 2005 року.

Останній, діючий на теперішній час, ЗВДТ з’являється у кінці 2020 року (Наказ ЦУ СБ України від 23 грудня 2020 року № 383).

Новий ЗВДТ починається з тлумачення термінів та визначення понять, що використовуються у ньому.

Для зручності користування сам ЗВДТ представляє собою табличну форму розмежовану за чотирма сферами у яких циркулює державна таємниця: 1. Оборони; 2. Економіки, науки і техніки; 3. Зовнішніх відносин; 4. Державної безпеки і охорони правопорядку.

Інформація представлена у ЗВДТ включає: номер статті ЗВДТ; зміст відомостей, що становлять державну таємницю; ступінь секретності; відомості про «суб'єктів режимно-секретної діяльності, державними експертами яких прийняті рішення про віднесення інформації до державної таємниці»

Таким чином, важливість введення в дію та використання ЗВДТ для інформаційної безпеки України, у сучасних умовах, полягає у можливості забезпечення своєчасного реагування на загрози та зміни, що відбуваються у інформаційному середовищі, економіці, міжнародних відношеннях та суспільному житті країни, уникати безпідставного прийняття рішень про віднесення інформації до державної таємниці, виключати випадки необґрунтованого позбавлення захисту відомостей про життєво важливі інтереси держави, які безпосередньо можуть завдати шкоди національній безпеці, а також бути зручним у користуванні.

Разом з тим, аналіз досвіду введення в дію та використання ЗВДТ дозволяє виділити окремі спірні питання, вирішення яких, певним чином, може підвищити ефективність його використання:

- визначення можливості перевірки обґрунтованості прийняття державним експертом рішення про віднесення інформації до державної таємниці, яке є підставою для подальшого формування відповідної статті у ЗВДТ;

- з метою впорядкування строків засекречування виконавцями матеріальних носіїв та подальшого, своєчасного перегляду грифів секретності, визначення у ЗВДТ номера, строку та дати реєстрації рішення державного експерта, на підставі якого відомості включені до Зводу;

- нормативно-правове закріплення строків засекречування виконавцями матеріальних носіїв інформації відповідно до дати конкретного рішення державного експерта (наприклад, для ступеня секретності «цілком таємно» рішення державним експертом прийнято у 2021 році терміном 10 років, при засекречуванні матеріального носія виконавцем у 2023 році, на підставі цього рішення, термін засекречування буде становити вже 8 років);

- з метою оптимізації процедури перегляду наявних у державі матеріальних носіїв секретної інформації розгляд можливості введення у дію нового ЗВДТ кожні п'ять років, відповідно до терміну мінімального ступеня секретності.

Література
1. Про державну таємницю : Закон України від 21.01.1994 р. № 3856-XII : станом на 6 березня 2023 р. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text (дата звернення: 6.03.2023).
2. Про затвердження Зводу відомостей, що становлять державну таємницю : Наказ ЦУ СБ України від 23 грудня 2020 року № 383, зареєстровано в Міністерстві юстиції України 14 січня 2021 року №52/35674 : станом на 6 березня 2023 р. URL: https://zakon.rada.gov.ua/laws/show/z0052-21#Text (дата звернення: 6.03.2023).

Корчига Є.В.
студентка групи Н-221мз ННІ ІБ СК НА СБ України
Науковий керівник:
Жевелєва І.С.
к.ю.н., доцент
доцент кафедри ОЗІОД ННІ ІБ СК НА СБ України

ВПЛИВ ІНФОРМАЦІЙНИХ ВІЙН НА БЕЗПЕКУ БІЗНЕСУ

Інформаційна ера кардинально змінила суспільство, дозволивши людям взаємодіяти в цифровому режимі, але водночас дає можливість використовувати масовий вплив для досягнення своїх цілей. Інформаційна війна є вкрай небезпечним явищем зараз, адже інформація оточує нас усюди і перевірити достовірність та правдивість дуже складно.

Вчені визначають поняття «інформаційна війна», як конкуренцію на стратегічному, оперативному та тактичному рівнях у всьому спектрі миру, кризи, ескалації кризи, конфлікту, війни, припинення війни та реконструкції/відновлення між конкурентами або ворогами з використанням інформаційних засобів для досягнення своїх цілей [1].

На нашу думку, це визначення є занадто широким, але, так чи інакше, охоплює більшість людських видів діяльності.

За останні кілька десятиліть відбулось швидке зростання інформаційних і комунікаційних технологій і їх все більша поширеність у нашому суспільстві революціонізували процес комунікації, а разом з ним і значення та наслідки інформаційної війни.

Комунікаційні та інформаційні процеси сучасного суспільства складаються з чотирьох критично важливих, надзвичайно взаємопов’язаних інфраструктур:

- енергетичної мережі
- комунікаційної інфраструктури
- фінансової інфраструктури

- транспортної інфраструктури [3].

Через високі темпи інформатизації суспільство стає все більш сприйнятливим до впливу інформаційного середовища. Низький рівень інформаційної гігієни у великої кількості користувачів, легкодоступність маніпуляційного контенту і відсутність компетентності в його належній оцінці дозволяє таким технікам, як дезінформація, пропаганда та психологічні операції глибше проникнути в соціальні структури та формувати громадську думку.

Варто зазначити, що інформаційна війна в бізнес просторі розглядається як діяльність з контролю, захисту та потенційного підриву економічної діяльності за допомогою інформації та інформаційних систем.

Як зазначає Пол С., глобалізація призвела до майже миттєвих коливань в бізнес-просторі, зокрема в сфері ціноутворення через передбачення надлишку або дефіциту пропозиції. Із зростанням довіри до інформаційних технологій та їх ролі в глобалізації концепція економічної інформаційної війни з'явилася як аспект інформаційної війни та є тісно пов'язана з кібероперaціями [7].

Тому, як спостерігаємо, із швидким розвитком технологій – пропорційно зростає поширеність кібератак як основного засобу інформаційної війни. За допомогою кібератак відбуваються стратегічні атаки на економіку, незалежно від виду діяльності бізнесу.

Проведені дослідження інформаційної війни та кібербезпеки зокрема показали, що бізнес є основою економіки, яка в свою чергу, працює завдяки ланцюгам створення вартості або торговельним коридорам. Тому інформаційна атака на будь-яку частину впливає на економіку бізнесу загалом [6].

Погоджуємось з думкою Ільницької У., що дилема безпеки сьогодення — це теорія, згідно з якою нація, яка прагне зберегти або покращити свою безпеку, тим самим знижує безпеку інших націй [2].

Так вчені виділяють три фактори конкурентних аспектів бізнесу:

- конкурентне суперництво,
- загроза нових учасників
- загроза заміни [1].

Вважається, що кібервійна не має правил ведення. Кібератаки серйозно порушують економічну систему й можуть бути потенційно руйнівними для бізнесу.

В умовах широкомасштабної війни російської федерації проти України агресор активно використовує наявні сили та засоби ведення інформаційної війни, здійснюючи кібератаки на критичну інфраструктуру, фінансові установи та бізнес, використовує методи пропаганди та маніпуляцій, ІПСО.

Виходячи з вищезазначеного, можемо виділити такі ризики впливу інформаційної війни на бізнес:

1. Людський фактор: важче вести бізнес в атмосфері невизначеності, недовіри та страху. Люди перебувають у підвищеному вразливому стані через

нинішню глобалізацію та війну. Наслідки кібератак або маніпуляцій новинами, спрямованих на шкоду компаніям, можуть бути серйозними, адже робочий персонал зазнає прямого впливу [4].

2. Фішингові шахрайства: ера комп'ютеризації розвиває бізнес в нових напрямках, й водночас створює міцну основу для розбудови злочинців та інших зловмисників. Серед поширених методів такого виду шахрайств є створення підроблених, але правдоподібних профілів і змішування зламаних облікових записів для надання легітимності, може бути дуже ефективним, щоб переконати людей передати конфіденційні дані.

3. Фактор соціальних мереж: використовуючи зламані та підроблені облікові записи і ботів, відносно легко поширювати нові ідеї та використовувати соціальні мережі для їх розповсюдження. Фейкові новини, неправдиві статті, є підґрунтям, яке спрямоване на розкол бізнесу. Так, відповідно до звіту Оксфордського університету, з 2017 року кількість організованих маніпуляцій у соціальних мережах зросла на 150%, і зараз принаймні 70 країн ведуть комп'ютерну пропаганду, спрямовану на вплив на громадську думку [5].

Проаналізувавши зв'язок ризиків між собою та їх загальний вплив на бізнес-сферу, можемо сказати, що людський фактор є найбільш вразливішою ланкою в інформаційній війні. А через те, що багато часу люди проводять в соціальних мережах – цей фактор є дуже важливим для засобів інформаційної війни.

Підсумовуючи вищесказане можна сказати, що розвиток інформаційної сфери людської діяльності призвів, з одного боку, до прозорості та відкритості життя, а з іншого – до використання інформаційного простору для проведення інформаційних війн. Інформаційні війни стали невід'ємним елементом проведення воєнних операцій, а техніки та засоби інформаційних війн активно використовуються для отримання конкурентних переваг у бізнес-середовищі.

Література

1. Денисюк Ж.З. Пропаганда та контрпропаганда в контексті стратегій державної інформаційної політики. Вчені записки ТНУ імені В.І. Вернадського. Серія: Державне управління. 2021. No2. С. 46–51.

2. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози, та механізми протидії негативними інформаційно-психологічним впливам. Політичні науки. 2019. No2. С. 27–32.

3. Носов В. Окремі аспекти протидії інформаційній війні в Україні. Правове, нормативне, метрологічне забезпечення системи захисту інформації в Україні. 2015. No1. С. 26–32.

4. Хомич С.В., Юськів Б.М. Роль медіа-пропаганди в умовах «гібридної війни». Актуальні проблеми міжнародних відносин. 2017. №132. С. 27–43.

5. Хорошоко В.О., Хохлачова Ю. Є. Інформаційна війна. ЗМІ як інструмент інформаційного впливу на суспільство. Безпека інформації. 2016. URL :https://jrnl.nau.edu.ua/index.php/Infosecurity/article/view/11104.

6. Шевчук П. Інформаційно-психологічна війна Росії проти України : як їй протидіяти. Демократичне врядування. 2014. №13. С. 16–23.

7.Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote. NATO review.2021.URL: https://www.nato.int/docu/review/articles/2021/11/30/hybrid- warfare-new-threats-complexity-and-trust-as-the-antidote/index.html.

Марущак А.І.
доктор юридичних наук, професор,
професор кафедри Національної академії СБ України, стратегічний радник
Міжнародної академії інформації.

ПРОТИДІЯ РОСІЙСЬКІЙ ДЕЗІНФОРМАЦІЇ В УМОВАХ ВОЄННОГО СТАНУ

Більше року повномасштабної війни російської федерації проти України супроводжуються використанням дезінформаційних операцій. Український досвід у протидії російській дезінформації є цінним для зарубіжних держав задля розуміння ними викликів та формування стійкості проти дезінформації. Український уряд, громадянське суспільство та ЗМІ досягли значного прогресу у відповіді на кампанії російської дезінформації.

Значно покращили спроможність України протидіяти російській дезінформації діяльність Центру протидії дезінформації РНБО України та Центру стратегічних комунікацій та інформаційної безпеки Міністерства культури та інформаційної політики України, зокрема у напрямку координації зусиль уряду, громадянського суспільства і ЗМІ в умовах воєнного стану. Створення скоординованої системи реагування має вирішальне значення для ефективної протидії дезінформації.

Безумовно, визнання у Стратегії національної безпеки України Стратегія інформаційної безпеки загрози російської дезінформації та пропаганди стали основою для посилення стійкості проти дезінформації, а також здійснення відповідних відкритих і негласних заходів іншими державними органами відповідно до їх компетенції.

Освіта та медіаграмотність також є важливими для формування стійкості населення України проти дезінформації. Це включає розвиток навичок критичного мислення та навчання медіаграмотності у закладах освіти. Крім того, засоби масової інформації в Україні запроваджують практику перевірки фактів і сприяти прозорості своїх повідомлень. У цьому контексті варто відзначити проект

StopFake - українську платформу перевірки фактів, яка стала орієнтиром для розвінчання неправдивої інформації

Звернемо увагу і на міжнародну співпрацю України, яка має важливе значення для протидії кампаніям російської дезінформації. Український досвід показав важливість побудови партнерства з іншими державами, міжнародними організаціями і великими технологічними компаніями соціальних медіа для обміну інформацією та координації зусиль. Низка проектів взаємодії з Європейським Союзом та іншими міжнародними організаціями, а також іноземними державними органами і приватними компаніями стали запорукою успішної протидії російській дезінформації.

Новий Закон «Про медіа» суттєво посилює роль Національної ради України з питань телебачення і радіомовлення, надаючи регулятору повноваження для обмеження доступу до каналів та сервісів провайдерів рф, а також контенту лінійних каналів на платформах спільного доступу до відео. Національна рада України з питань телебачення і радіомовлення має право укладати договори та меморандуми про співпрацю з іноземними юридичними особами з питань співпраці «у сфері протидії поширенню дезінформації під час підготовки та проведення референдуму, забезпечення прозорості агітації на платформах» тощо [1].

Загалом, побудова стійкості проти дезінформації потребує комплексного підходу, який включає належне демократичне правове регулювання, освіту та медіаграмотність, створення скоординованої системи реагування, використання технологій та інструментів моніторингу соціальних мереж, а також міжнародну співпрацю. Вивчаючи український досвід, інші країни можуть розробити ефективні стратегії протидії дезінформації та захисту своїх демократичних інститутів.

Насамкінець, відзначимо, що ініціатива «Правда і безпека», започаткована Міжнародною академією інформації у лютому 2022 року, стала одним із заходів об’єднання зусиль громадянського суспільства і державних органів України, а також експертизи зарубіжних партнерів Європейського Союзу, зокрема під час круглого столу «Взаємодія громадянського суспільства та уряду для боротьби з дезінформацією в умовах війни» [2].

Література

1. Закон «Про медіа» від 13 грудня 2022 року. [Електронний ресурс]. Режим доступу : https://zakon.rada.gov.ua/laws/show/2849-20#Text.

2. Академія дякує співорганізаторам круглого столу «Взаємодія громадянського суспільства та уряду для боротьби з дезінформацією в умовах війни» за підтримку ініціативи «Правда і безпека». [Електронний ресурс]. Режим доступу : https://interacademy.info/en/the-academy-thanks-the-co-organizers-of-the-

round-table-interaction-between-civil-society-and-state-bodies-for-countering-disinformation-at-wartime-for-the-support-of-the-public-init.

Орєхова А.О.
студентка НА СБ України
Науковий керівник:
Жевелєва І.С.
к.ю.н., доцент
доцент кафедри ОЗІОД ННІ ІБ СК НА СБ України

ТРАНСФОРМАЦІЯ БЮРОКРАТИЧНОЇ СИСТЕМИ УКРАЇНИ У КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Українська держава виникла на уламках радянської номенклатурної системи і увібрала в себе багато рис тодішнього тоталітарного суспільства. Це стосується, в першу чергу, методів керівництва, прийняття рішень та неефективне використання державних ресурсів, захистом данних та непотужною інформаційною системою. Нам імпонує підхід Макса Вебера до бюрократії та держави, а саме в його ідеях переважає принцип контролю над управлінцем та існує дисципліна посадових осіб, також Вебер уявляв бюрократію як сукупність висококваліфікованих спеціалістів, які пройшли гідну підготовку та гарантію якості роботи таких осіб, адже без таких принципів породиться корупція і буде уявний державний апарат, який буде існувати лише де-юре, а не де-факто [1, с. 67]. Проте сучасна інформаційна держава повинна забезпечувати «виклики» і запити, які є в суспільстві. «Пострадянське коріння», безумовно, до сих пір впливає на систему сучасної України. Нажаль, система управління інформаційною безпекою в Україні не відповідає потребам країни у проведенні комплексних реформ у різних сферах державної політики та її європейському виборі, а також європейським стандартам належного управління державою [2]. Однією з проблем впровадження ефективного електронного урядування в Україні є бюрократія (хоч бюрократія і має позитивні риси, такі як точне дотримання прописаних правил, слідування інструкціям та процедурам) [2].

Як позитивний приклад впровадження електронного урядування можна навести Естонію, країну, де бюрократія зведена до мінімуму, адже, вся адміністративна система переведена в електронний вигляд. Спілкування віч-на-віч між службовцями та громадянами в Естонії просто відсутнє, або зведене до виключень з правил, там діє електронне посвідчення особи, інтернет-голосування, електронна медична картка, електронний уряд. Невелика країна в Європі з населенням один мільйон триста тисяч осіб на шляху до побудови цифрової держави та за темпами діджиталізації вже обігнала багатьох світових

лідерів [3]. Зараз Литва і Латвія успішно наслідують приклад Естонії. Почалось все з того, що більше десятків років тому, Таллін взяв курс на розвиток сучасних інформаційних технологій. Спочатку уряд просто відмовився від паперів, замінивши електронну бюрократію на електронні файли в урядовій мережі. Потім ввели електронний підпис, громадяни отримали електронні ідентифікаційні картки. Також більше 90% податкових декларацій громадяни подають в електронному вигляді. Подолання бюрократіїї в Естонії – заслуга уряду [3]. Також, варто зазначити, що за даними міжнародної громадської організації Transparency International, Естонія – одна з найменш корумпованих країн, цього досягли завдяки наданню пріорітету підприємництву та інформаційній безпеці. Естонія взяла курс на розвиток малого та середнього бізнесу, податкові декларації подаються в електронному вигляді, а підприємницьку діяльність можна зареєструвати за 20 хвилин [3]. В Україні вся процедура, наразі, теж є швидкою та не займе більше ніж один день, якщо врахувати звернення до ЦНАП чи в «Дія», відкриття рахунку в банку, постановка на облік в податковій і це за умови, що особа має електронний цифровий підпис, якщо ж немає, то ситуація теж не займе багато часу, що значно зручно для реєстрації юридичної особи, ФОП тощо. Також ще одним цікавим фактом про Естонію є те, що іноземець може отримати «електронне громадянство», це дозволяє відкривати рахунки в естонських банках та реєструвати бізнес, знаходячись в будь-якій точці світу де є доступ до мережі Інтернет. Програма «е-Естонія» - це приклад подолання наслідків радянського минулого без значних ресурсів задля розвитку, орієнтуючись на сучасні технології. Наразі Латвія рівняється на Естонію в розвитку е-послуг. Жителі задоволені такими нововведеннями, адже можуть користуватись електронним цифровим підписом та іншими зручностями. Латвія пропонує своїм жителям більш ніж 300 різних електронних послуг, які дозволяють спілкуватись з державою через Інтернет, а не стояти в чергах [3]. Україна у співпраці з урядом Естонії запустили для громадян цієї країни застосунок mRiik, створений на основі українського додатку «Дія». Щонайменше п’ять країн вже заявили про намір створення власних цифрових додатків на основі українського застосунку.

28 жовтня 2022 року в газеті «Голос України» офіційно опубліковано Закон № 2654-IX «Про внесення змін до Податкового кодексу України та деяких інших законів України щодо особливостей оподаткування підприємницької діяльності електронних резидентів» [4]. Документ набирає чинності з 1 квітня 2023 року. Таким чином міжнародні ІТ-спеціалісти зможуть відкривати бізнес і сплачувати податки в Україні. Документом установлено, що електронний резидент (е-резидент) - іноземець, який досяг 18-річного віку, не є податковим резидентом України, отримав відповідні кваліфіковані електронні довірчі послуги та інформація про якого внесена до інформаційної системи "Е-резидент". Інформаційна система "Е-резидент" - інформаційна система, що є складовою

частиною Єдиного державного веб-порталу електронних послуг, у рамках якої здійснюється збирання, накопичення, обробка, захист, облік та надання інформації про електронного резидента (е-резидента). Іноземець має право набути статус електронного резидента (е-резидента) після подання ним через інформаційну систему "Е-резидент" заяви про набуття статусу електронного резидента (е-резидента), його ідентифікації та надання кваліфікованих електронних довірчих послуг.Е-резидент — це іноземець, який може отримувати кваліфіковані електронні послуги, відкривати банківські рахунки в Україні, має можливість зареєструвати себе фізичною особою-підприємцем та вести підприємницьку діяльність без необхідності перебувати в Україні. Для того, щоб стати е-резидентом, необхідно: зареєструватися у застосунку "Дія" та пройти фінансову та безпекову перевірку. Якщо перевірка пройде вдало, іноземець стає електронним резидентом — по факту, електронним платником єдиного податку на третій групі без ПДВ та отримує ЕЦП (електронно-цифровий підпис). Наступним кроком є відкриття дистанційного рахунку у банку. І саме банк буде податковим агентом для е-резидента. Іноземець матиме право працювати та сплачувати податок від доходів [5].

На нашу думку, аби впровадити ефективне електронне урядування в Україні, потрібно, в першу чергу, подолати негативні прояви бюрократії та мінімізувати корупцію, по-друге, залучити до впровадження передового зарубіжного досвіду неурядові громадські організації, по-третє, змінити сам підхід до публічного адміністрування, оптимізувати кількість державних службовців за принципом «від кількості до якості». Важливим при цьому буде моніторинг, оцінювання, планування роботи та звітування, впровадження інновацій, цей процес має відбуватись не лише на центральному рівні, але й на регіональному, в комплексі із впровадженням в обласних центрах РПР (Реанімайційного Пакету Реформ), лише так можна буде досягнути бажаного результату [6]. Проте варто звернути увагу на те, що будь-які реформи, інновації, покращення не повинні стати всупереч інформаційній безпеці держави, уряду чи спровокувати витік персональних данних громадян. Саме тому, держава забезпечити гарантії інформаційної безпеки. Варто також звернути увагу на нестабільну воєнну, політичну та економічну ситуацію в Україні, а саме з квітня 2014 року і по 1 травня 2018 року відбувалась Антитерористична операція (АТО), відтоді і до 24 лютого 2022 року проводилась Операція об’єднаних сил (ООС) на території Донецької і Луганської областей, а з 24 лютого 2022 року йде повномаштабна війна по всій території України, що загрожує правам та свободам людини. Що також загострює проблему захисту інформації в умовах збройної агресії з боку Росії. Тому тема проблеми управління інформаційною безпекою держави гостро постала перед Україною і потребує окремої уваги та негайного реагування.

Література

1. Макс Вебер. Соціологія. Загальноісторичні аналізи. Політика. К., 1998. С. 67-82. URL: http://litopys.org.ua/weber/wbs03.htm (дата звернення 19.02.2022).

2. Електронне урядування: проблеми, пріоритети, завдання *Ifactor Інтелектуальна бухгалтерська система знань*: веб-сайт. URL: https://i.factor.ua/ukr/journals/ds/2018/march/issue-3/article-34920.html (дата звернення 19.02.2022).

3. Эстония - государство, где победила электронная демократия *EUROUA.com Новости мира и Украины*: веб-сайт. URL: https://euroua.com/europe/eu/3949-estoniya-gosudarstvo-gde-pobedila-elektronnaya-demokratiya (дата звернення 19.02.2022).

4. Закон № 2654-IX «Про внесення змін до Податкового кодексу України та деяких інших законів України щодо особливостей оподаткування підприємницької діяльності електронних резидентів. URL: https://zakon.rada.gov.ua/laws/show/2654-20#Text (дата звернення 19.02.2022).

5. Верховна Рада проголосувала за електроне резидентство. Що це означає. Суспільне Новини. URL: https://suspilne.media/289532-verhovna-rada-progolosuvala-za-elektrone-rezidentstvo-so-ce-oznacae/ (дата звернення 19.02.2022).

6. Коаліція громадських організацій Реанімаційний Пакет Реформ розробила Дорожню карту реформ – оновлене експертне бачення пріоритетів реформування і розвитку країни на 2019-2023 роки у 21 сфері державної політики *Реанімаційний пакет реформ*: веб-сайт. URL: https://rpr.org.ua/news/dorozhnya-karta-reform-rpr-na-2019-2023-roky/ (дата звернення 19.02.2022).

Потенко О.С.
мол.наук.співр.,
Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова, Київ
Давиденко А.М.
д.т.н., пров.наук.співр.,
Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова, Київ

РОЗРОБКА ПРОГРАМНОГО ЗАСТОСУНКУ ВИБОРУ СКЛАДУ ПРОФІЛЮ ПРОТИДІЇ ЗАГРОЗАМ НА ОСНОВІ АНАЛІЗУ ВІРОГІДНОСТІ ЇХ РЕАЛІЗАЦІЇ

Задачі інформаційної безпеки в інформаційно-телекомунікаційних системах (ІТС), та побудови комплексних систем захисту інформації (КСЗІ) останнім часом привертає все більш серйозну увагу з боку фахівців, особливо, якщо таку систему використано на об’єктах критичної інфраструктури. Комплексна система захисту інформації – це сукупність організаційних та інженерно-технічних заходів, програмно-апаратних засобів, які забезпечують захист інформації в ІТС.

Необхідність створення КСЗІ в ІТС регламентується законодавством України. Оцінити наявність послуг безпеки в комп'ютерній системі дозволяють функціональні критерії, а критерії гарантій дозволяють оцінити коректність реалізації послуг. Щоб задовольняти певним вимогам захищеності інформації, яка обробляється в ІТС, комплекс засобів захисту (КЗЗ) обчислювальної системи повинен відповідати профілю захищеності, що являє собою перелік мінімально необхідних рівнів послуг.

З метою перевірки, аналізу та оцінки КСЗІ ІТС щодо їх відповідності вимогам нормативних документів з технічного захисту інформації та можливості їх використання для забезпечення технічного захисту інформації (далі - ТЗІ) проводиться державна експертиза у сфері технічного захисту інформації.

Однією із наукових задач яка вирішується для забезпечення процедури проведення державної експертизі у сфері технічного захисту інформації це вибір методу побудові складу профілю протидії загрозам на основі аналізу вірогідності їх реалізації

Для вирішення задачі проектування профілів, адаптивних загрозам за підкласами АС, пропонується використовувати метод динамічного програмування. Використовуючи класичний підхід [1], можна розробити прикладний алгоритм (методику) оцінки профілів, адаптивних загроз за підкласами автоматизованих систем АС-1, АС-2, АС-3, на кроки, на кожному із яких склад профілю буде покращено. Для цього необхідно провести дослідження реалізації вимог НД ТЗІ 2.5-004-99[2], НД ТЗІ 2.5-005-99[3] та визначити прикладний фізичний зміст, що дозволить розробити методику обчислення параметрів цільової функції під час оптимізації.

Крок 1: Введення початкових значень

Крок 2: Розрахунок цільової функції апроксимованого виду для n об'єктів

Крок 3: Знайти максимальне значення математичного очікування втрат на перших n об'єктах АС

Крок 4: Порівняти значення математичного очікування втрат із початковим. Якщо воно більше, то перейти к пункту 6. Якщо ні, то – до кроку 5.

Крок 5: Прийняти N=N+1 та перейти до кроку 2.

Крок 6: Знайти розподіл атакуючих потенційних загроз по n об'єктах захисту.

Для реалізації алгоритму розроблено програмний застосунок в системі Visual Studio Community Edition. Програмний застосунок написано на мові програмування C# з використанням програмної платформи Microsoft .NET Framework. Програмний застосунок здатний працювати в операційній системі Windows 10 та Windows 11. Реальний вигляд інтерфейсу застосунку наведено на рис. 1, де показана екранна форма з розрахунком максимального значення математичного очікування (МОЧ)

1 | F | Wi | y(N) | Mo

Максимальне значення МОЧ

N	1	2	3	4	5	6	7
1	0	0	0.032	0.032	0.032	0.032	0.032
2	0,072	0,072	0,072	0,072	0,072	0,072	0,072
3	0,1008	0,1008	0,104	0,104	0,104	0,104	0,104
4	0,1123	0,1123	0,1328	0,1328	0,1328	0,142	0,142
5	0,1169	0,168	0,168	0,184	0,184	0,184	0,184

Рис1. Екранна форма з розрахунком максимального значення математичного очікування (МОЧ)

Розроблено програмне забезпечення для реалізації методики обчислення параметрів цільової функції під час оптимізації, яке за рахунок використання методу динамічного програмування надає можливість реалізувати принцип оптимальності Р. Беллмана: з якого б етапу ми не почали визначати новий склад профілю для протидії загрозам в залежності від наявності ресурсів захисту щодо апаратного та програмного забезпечення (модернізація, удосконалення, переоснащення, нова політика безпеки тощо), то всі подальші етапи будуть більш оптимальними.

Тестування програмного забезпечення дозволило отримати аналітичні залежності для різних профілів протидії загрозам, що дозволяє оптимізувати процедуру вибору профілю в залежності від вимог до інформації яка обробляється.

Література

1. Гурин Л.С., Дымарский Я.С., Меркулов А.Д. Задачи и методы оптимального распределения ресурсов. - М.: Сов. радио, 1968. - 464 с.

2. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу, №22, 67с., 1999

3. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу, №22, 18с., 1999.

Розвадовський О.Б.
д.ю.н.,
доцент кафедри ОЗІОД ННІ ІБ СК НА СБ України

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ КУПАП У СФЕРІ ОХОРОНИ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

У сфері охорони державної таємниці та службової інформації інститут адміністративної відповідальності відіграє важливе значення, оскільки спрямований на зміцнення законності, запобігання правопорушенням, додержання Конституції і законів України, сумлінне виконання громадянами своїх обов'язків тощо.

Особливої актуальності вказані питання набувають в умовах російської агресії проти України, оскільки вимагають від органів державної влади, військового командування, військових адміністрацій, органів місцевого самоврядування, підприємств, установ та організацій в умовах воєнного стану вживати додаткових заходів щодо посилення охорони державної таємниці.

Проведений аналіз стану притягнення до відповідальності за статтями 212-2 (Порушення законодавства про державну таємницю), 212-5 (Порушення порядку обліку, зберігання і використання документів та інших матеріальних носіїв інформації, що містять службову інформацію) Кодексу України про адміністративні правопорушення (далі – КУпАП) вказує на недієвість адміністративної практики в сучасних умовах.

Зазначене насамперед стосується строків накладення адміністративних стягнень (стаття 38 КУпАП), оскільки через об'єктивні обставини, пов'язані з логістикою, небезпекою ракетних обстрілів, блекаутом, мобілізацією суддів, яким надано допуск до державної таємниці, тощо строки затягуються, засідання переносяться, а провадження закриваються у зв'язку із закінченням строків накладення адміністративних стягнень. Схожою є проблематика, пов'язана із визначеними строками складення адміністративних протоколів (стаття 254 КУпАП).

У разі закінчення строку притягнення особи до адміністративної відповідальності відповідно до пункту 7 статті 247 КУпАП провадження у справі про адміністративне правопорушення підлягає закриттю, якщо на момент розгляду справи закінчився строк, передбачений ст. 38 КУпАП. За цих підстав, згідно з вимогами ст. 247 КУпАП, суд не встановлює наявність вини особи у вчиненні адміністративного проступку.

Водночас, поєднання закриття провадження у справі з одночасним визнанням вини особи у вчиненні адміністративного правопорушення є взаємовиключними рішеннями і їх прийняття в одному судовому рішенні може розглядатись як порушення права громадянина на справедливий суд. Адже згідно з вимогами ст.

284 КУпАП рішенням, яке доводить вину особи, є постанова про накладення адміністративного стягнення або застосування заходів впливу, умовою якої є встановлення вини особи.

Таким чином, у разі спливу строку накладення адміністративного стягнення, суддя зобов'язаний припинити будь-які дії, спрямовані на притягнення особи до адміністративної відповідальності, незалежно від будь-яких інших обставин, що підлягають з'ясуванню саме під час розгляду справи, у тому числі й вини особи.

Вказане призводить до уникнення порушниками передбаченої законодавством відповідальності, нівелює виховну й профілактичну функції адміністративної відповідальності осіб (стаття 23 «Мета адміністративного стягнення» КУпАП) та негативно впливає на загальний стан охорони державної таємниці і службової інформації. Окреслене також стосується протоколів, складених за вчинення інших правопорушень, передбачених КУпАП.

У зв’язку з цим вважається за доцільне внесення змін до статті 38 (Строки накладення адміністративних стягнення) та статті 254 (Складення протоколу про адміністративне правопорушення) КУпАП в частині збільшення строків притягнення громадянина до відповідальності до 6 місяців та складення протоколу про адміністративне правопорушення у місячний термін, принаймні на час дії воєнного стану.

Солодка О.М.
кандидат юридичних наук,
старший науковий співробітник
НА СБ України

ЩОДО ПОТРЕБИ УДОСКОНАЛЕННЯ ЗАКОНОДАВСТВА У СФЕРІ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

Право на доступ до інформації є конституційним правом людини, яке передбачене і гарантоване статтею 34 Конституції України [1], а саме, право кожного на свободу думки і слова, на вільне вираження своїх поглядів і переконань; право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб на свій вибір. Здійснення цих прав може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров’я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя і зокрема реалізується в рамках формування інституту інформації з обмеженим доступом, що зумовлено

необхідністю захисту прав учасників інформаційних правовідносин на обмеження загального доступу до належної їм інформації.

Так, відповідно до ст. 20 Закону України "Про інформацію" [2] за порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом (ІзОД). Хоча на законодавчому рівні відсутнє визначення ІзОД, слід констатувати, що її притаманний особливий режим доступу, покликаний захищати ті відомості, вільний обіг яких може завдати шкоди правам й інтересам людини, суспільства, держави. Отже, характерною ознакою надання інформації статусу з обмеженим доступом є законодавчо визначена процедура її захисту та охорони як з боку держави, так і власника, однак стосовно загальних рис її класифікації слід зазначити, що достатньо чіткого поділу на види законодавцем не здійснено.

Так, зокрема інформація про стан банківських рахунків фізичної особи у правовідносинах, в яких приймає участь банк є банківською таємницею, яку банк зобов'язаний зберігати. В той же час для цієї фізичної особи такі дані є її конфіденційною інформацією, збереження чи розповсюдження якої відбувається саме на розсуд її власника. Схожа ситуація і з таємницею вчинення нотаріальних дій та таємницею усиновлення, які для окремої людини є її персональними даними. Крім того і змісту законодавчих визначень комерційної таємниці та конфіденційної інформації можна зробити висновок про належність комерційної таємниці власне до конфіденційної інформації, оскільки вона, як конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов.

У свою чергу дискусійним є співвідношення змісту понять «конфіденційна інформація про особу» та «персональні дані», адже в українському законодавстві одразу кілька законів регулюють питання їх обігу: Закони України «Про інформацію» [2] , «Про захист персональних даних» [3], «Про доступ до публічної інформації» [4], а одні й ті ж визначення не ідентичні, а навіть частково суперечать один одному, чим створюють проблеми із реалізацією особою свого права на захист власної інформації.

Система охорони державної таємниці та службової інформації є одним із найважливіших напрямів, за яким має здійснюватися реформування в частині об'єднання державної таємниці та службової інформації в єдину категорію інформації, доступ до якої обмежується виключно в інтересах, передбачених статтею 6 Закону України "Про доступ до публічної інформації" [4], та яка підлягає охороні державою, оскільки, наприклад, на сьогодні одна і та ж інформація в одних суб'єктів владних повноважень є відкритою, а у інших – віднесена до категорії службової інформації, що ускладнює кваліфікацію відомостей на предмет їх віднесення до ІзОД.

Загальним проблемним аспектом у сфері ІзОД є використання у законодавстві термінології, яка не відповідає законодавчо встановленій

класифікації ІзОД. Наприклад, в ухваленому Законі України «Про медіа» [5] у ст. 117 йдеться про те, що «Суб'єкти у сфері медіа та їх працівники не несуть відповідальності за поширення інформації, що містить таємницю, яка спеціально охороняється законом, якщо ці відомості не було отримано незаконним шляхом». Звідси можна зробити висновок, що існує ще таємниця, яка спеціально не охороняється законом, хоча відповідно до законодавства інформація стає таємною обов'язково і відповідно до закону, який зобов'язує всіх, хто причетний до її обігу вживати належних заходів її охорони, відтак факт законного отримання такого виду інформації не наділяє правом її розповсюдження.

Зважаючи на вище викладене, потребу оновлення законодавства у сфері ІзОД обумовлює, передусім, розвиток інформаційного суспільства, зокрема прискорена інформатизація, глобалізація інформаційних відносин, характер суспільних відносин. З огляду на те, що Україна – демократична держава, в якій інформаційні права людини та їх гарантії визначають зміст і спрямованість діяльності держави є необхідність внесення змін до чинного законодавства України з питань регулювання інформаційної сфери, зокрема в частині досягнення належного балансу між правом на доступ до інформації та обмеженням доступу до інформації шляхом належної правової регламентації системи інформації з обмеженим доступом у національному законодавстві України.

Література

1. Конституція України. URL : http://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80 (дата звернення: 11.01.2023).
2. Закон України «Про інформацію». URL : http://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 21.02.2023).
3. Закон України «Про захист персональних даних». URL : https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 12.03.2023).
4. Закон України «Про доступ до публічної інформації». URL : https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 11.03.2023).
5. Закон України «Про медіа». URL : https://zakon.rada.gov.ua/laws/show/2849-20#Text (дата звернення: 12.03.2023).

Стрельбіцький М. А.
д.т.н., професор
Равлюк В. В.
Ваврічен О. А.
Національна академія Державної прикордонної
служби України імені Б. Хмельницького

ПРИХОВАНІ КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ ДЕРЖПРИКОРДОНСЛУЖБИ УКРАЇНИ

Побудова сучасних інформаційних систем тісно пов’язана з проблемою забезпечення інформаційної безпеки. Разом із тим, на теперішній час розроблена та впроваджена в дію велика сукупність міжнародних та вітчизняних стандартів та нормативних документів у галузі інформаційної безпеки.

Інформаційна безпека - стан захищеності системи від загроз чотирьох основних типів: конфіденційності, цілісності, доступності та спостереженості [1]. Для опису процесу протидії зазначеним загроз розроблені математичні моделі, які формалізують засади розмежування доступу, контролю цілісності інформації, доступності даних та математично суворо визначають вимоги та умови безпечного функціонування інформаційної системи, або іншими словами, суворо обґрунтовують коректність і адекватність функціонування систем забезпечення інформаційної безпеки.

Одним із питань забезпечення конфіденційності інформації є проблема розмежування доступу до ресурсів інформаційної системи. В даний час існує достатня кількість підходів, що визначає доступ користувачів до тих або інших видів даних (ресурсів) інформаційної системи. При цьому основними з них є технології систем: дискреційного розмежування доступу; мандатного розмежування доступу; тематичного розмежування доступу; рольового розмежування доступу; суб'єктно-орієнтована технологія ізольованого програмного середовища.

Разом із цим, як показав аналіз вище перерахованих систем, розмежування доступу користувачів до інформації з різним ступенем секретності здійснюється на підставі раніше визначених категорій даних та рівнів доступу на конкретний момент часу або невеликий термін функціонування системи. Окремі моделі передбачають процедуру пониження конфіденційності даних, таким чином запобігають несанкціонованому витоку інформації. Варто зазначити, що існуючі інформаційно-комунікаційні системи прикордонного відомства експлуатуються досить тривалий час різними користувачами різного рівня доступу, при чому вимоги керівних документів, щодо грифу даних також змінюються. Таким чином, неврахування вищезазначених умов сприяє виникненню прихованого каналу витоку інформації.

З метою виявлення передумов несанкціонованого витоку конфіденційної інформації з інформаційно-комунікаційних систем необхідно провести аналіз надання допуску персоналу до конфіденційної інформації та процедури визначення грифа секретності матеріальних носіїв секретної інформації (МНСІ). Існуюча система надання доступу та допуску персоналу прикордонного відомства до конфіденційної інформації передбачає подання керівником організації запиту до СБУ яка надає допуск до МНСІ. Крім того, визначається також доступ до конкретного МНСІ. Таким чином, існуючу систему можна віднести до дискреційної системи розмежування доступу. Разом із тим, процес надання доступу до МНСІ описується мандатною моделлю доступу Бела ЛаПадули [2], а саме можливістю ознайомлення з документом, гриф секретності якого не вище допуску користувача.

Керівний документу, який визначає ступінь конфіденційності інформації, а саме «Звід відомостей, що становлять державну таємницю» (ЗВДТ) [3] визначає порядок присвоєння грифа секретності МНСІ, а саме відповідність інформації хоча б одному із пунктів цього документу є підставою для надання матеріальному носію інформації, що містить ці відомості, грифа секретності, який відповідає ступеню секретності, установленому для них у ЗВДТ.

Проведений аналіз розділів ЗВДТ показав наявність агрегованих пунктів з різними ступенями секретності, в окремих розділах більше 50%.

Під агрегованим пунктом ЗВДТ будемо розуміти пункт в якому ступінь секретності сукупності його складових відрізняється, а саме вищий від окремої складової. Існуючі моделі розмежування доступу не враховують наявність агрегованих пунктів з різними ступенями секретності.

Розглянемо можливі шляхи виникнення витоку інформації. З цією метою формалізуємо окремі поняття:

$\{O\}$ - об’єкти системи (користувачі або процеси, які виконуються від їх імені);

$\{S\}$ – суб’єкти системи (конфіденційна інформація);

$\{R\}$ – матриця доступів, рядки якої відповідають суб’єктам, а стовбці – об’єктам.

Зазначимо, що $\{O^{A}\} \cup \{O^{H}\} = \{O\}, \{O^{A}\} \cap \{O^{H}\} = \emptyset$

де: $\{O^{A}\}$ – агреговані об’єкти системи;

$\{O^{H}\}$ – не агреговані об’єкти системи.

Всі об’єкти та суб’єкти системи мають відповідний рівень допуску $l \in L$, де L – множина рівнів конфіденційності. Таким чином, суб’єкт S_l має доступ $A(S_l, O_k)$ (де А – предикат наявності доступу) до об’єкта O_k тоді і тільки тоді, коли $l \geq k$, тобто при домінуванні рівня допуску суб’єкта над об’єктом та наявності допуску $\{S_l, O_k\} \in R$.

Перший спосіб. У відповідності до моделей розмежування доступу та вимог керівних документів існує процедура пониження ступеня конфіденційності даних

(довірений суб'єкт – в термінах моделей, експерт – ЗВДТ). Таким чином, можлива ситуація з декласифікації окремих складових агрегованого об'єкту без врахування часу з подальшим наданням доступу користувачеві з відповідним рівнем допуску. Процес декласифікації складових об'єкту на нижчий рівень допуску. При умові пониження всіх складових об'єкта та надання суб'єкту даного рівня допуску до вказаних об'єктів виникає витік інформації. Таким чином, можливе виникнення прихованого каналу витоку інформації при деагрегації об'єкта при дотриманні вимог політики безпеки та керівних документів.

Другий спосіб. У відповідності до визначення поняття агрегованого об'єкта системи та відповідно до вимог ЗВДТ рівень його конфіденційності повинен стати вищий при наявності на МНСІ всіх його складових. Таким чином, можлива зворотна першому способу ситуація, коли суб'єкти у відповідності до політики безпеки формують на МНСІ сукупність агрегованого об'єкта з вищим ступенем конфіденційності.

У випадку доступу суб'єкта до МНСІ на якому агрегується сукупність об'єкта виникає прихований канал витоку інформації, так як порушується рівень доступу (рівень об'єкта переважає над рівнем суб'єкта).

З метою ліквідації зазначених прихованих каналів витоку інформації необхідно реалізувати відповідні механізми в політиці безпеки інформаційно-комунікаційних систем. Ліквідація першого способу прихованого витоку інформації передбачена моделлю Бела ЛаПадули, а саме «заборона запису вниз». Разом із тим в реальній системі реалізація цього принципу є проблемною, так як пониження рівня класифікації об'єктів передбачено керівними документами, зокрема ЗВДТ, при перевищенні терміну зберігання. Ліквідація другого способу прихованого витоку інформації при агрегації об'єкта не передбачена моделями розмежування доступу.

Вирішення наведених проблем можливе шляхом впровадження в інформаційно-комунікаційну систему тематичного розмежування доступу, який передбачає наявність механізму збереження історії надання доступів суб'єкта до об'єктів системи з початку реєстрації користувача та формування і підтримання тематичного класифікатора.

Як було зазначено вище, проблема прихованого витоку інформації виникає тільки при розгляді агрегованих об'єктів $\{O^A\}$, які відповідають певній тематиці ЗВДТ.

Визначимо тематичний класифікатор агрегованих об'єктів, як сукупність підмножин нижчого рівня $\{T^z\} = \{\tau_1^z, \tau_2^z, \dots \tau_n^z\}$, де z – індекс агрегованого об'єкту, n – кількість складових агрегованого об'єкту. Кожному елементу тематичного класифікатора та елементам підмножини визначається відповідний рівень конфіденційності, а саме відображення на множину рівнів конфіденційності $F: T^z \to L, \tau_i^z \to L$. Аналіз ЗВДТ показав, що складові z – го об'єкта мають однаковий рівень конфіденційності, але в загальному випадку це не є

обов'язковим. Запроваджується функція історії доступів $H(t)$ результатом якої є множина $\{O_k\}$ при умові $A(S_l, O_k)$ на момент часу t. Властивістю даної функції є $H(t) \subseteq H(t+1)$, тобто накопичення доступів в різні моменти часу всіх суб'єктів та об'єктів системи.

Таким чином, доступ суб'єкта S_l до об'єкта O_k можливий тоді і тільки тоді, коли рівень допуску суб'єкта домінує на рівнем допуску об'єкта $l \geq k$, суб'єкту надано доступ до об'єкта $\{S_l, O_k\} \in R$ і сукупність об'єктів, до яких мав доступ суб'єкт на момент часу t у сукупності з об'єктом O_k не входить в множину тематичного класифікатора T^z рівень доступу якого перевищує рівень суб'єкта $\{H(t), O_k\} \neq \mathrm{T}^z \ \forall z$.

В результаті аналізу керівних документів та існуючих моделей розмежування доступу визначені можливі канали прихованого витоку інформації без порушення політики безпеки. Запропоновано спосіб попередження несанкціонованого доступу суб'єктів інформаційної системи шляхом запровадження тематичного класифікатора та функції історії доступів.

Література

1. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу НД ТЗІ 2.5-004-99.

2. Bell D.E., LaPadula L.J. Unified Exposition and Multics Interpretation MITRE Corporation. Secure Computer System: (1976). URL: http://csrc.nist.gov/ publications/history/bell76.pdf (дата звернення: 15.03.2023).

3. Про затвердження Зводу відомостей, що становлять державну таємницю. Офіційний вебпортал парламенту України : веб-сайт. URL : https://zakon.rada.gov.ua/go/z0052-21 (дата звернення: 12.03.2023).

Суржко В.О.
студентка П-211 групи
Навчально-наукового інституту інформаційної безпеки
НА СБ України

ЗАХИСТ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ В УМОВАХ ЗБРОЙНОЇ АГРЕСІЇ рф

Особливо в сьогоднішніх умовах дослідження питання щодо захисту інформації, зокрема, інформації з обмеженим доступом є актуальним.Основним напрямком в захисті інформації є правовий захист інформації, актуальність якого зростає в умовах побудови інформаційного суспільства, зокрема в умовах збройної агресії рф. Правовий захист інформації визнаний як на міжнародному (міжнародні договори, угоди, конвенції, декларації тощо), так і на державному

рівні. На державному рівні правовий захист регулюється державними та відомчими нормативно-правовими актами. Система законодавчих актів та розроблених на їх базі нормативних та організаційно-розпорядчих документів повинна забезпечувати організацію ефективного нагляду за їх виконанням та забехзпеченням захисту інформації з обемеженим доступом.

У ст. 34 Конституції України закріплено право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово чи будь-яким іншим способом і на свій вибір [1]. Будь-яка інформація є відкритою, крім тієї, яка відноситься законом до інформації з обмеженим доступом. Згідно зі п. 1 ст. 20 ЗУ «Про інформацію», в залежності від порядку доступу інформація поділяється на відкриту та інформацію з обмеженим доступом [2]. Інформація з обмеженим доступом - це відомі тільки певному колу осіб відомості, дані та знання, які мають особливу цінність, щодо яких вживаються заходи, спрямовані на обмеження вільного доступу третіх осіб, поширення яких може принести істотну шкоду заінтересованим особам [3]. Це відомості конфіденційного або таємного характеру, правовий статус яких передбачений законодавством України, визнаних такими відповідно до встановлених юридичних процедур і доступ до яких обмежений власником таких відомостей [4].

Переходячи безпосередньо до самого дослідження деяких питань захисту інформації з обмеженим доступом в умовах збройної агресії рф, хочу нагадати що питання щодо обмеження доступу до інформації регулюються різними нормативно-правовими актами України, серед яких: Конституція України, Закони України «Про інформацію», «Про доступ до публічної інформації».

Отже, пропоную розібратись в представлених проблемних питаннях захисту інформації з обмеженим доступом в умовах збройної агресії рф та можливі шляхи їх вирішення:

Які технічні та організаційні заходи можуть бути використані для захисту інформації від несанкціонованого доступу в умовах збройної агресії рф?

Технічні заходи для захисту інформації включають в себе використання різноманітних методів шифрування, резервного копіювання інформації, регулярне оновлення програмного забезпечення, контроль доступу до мережі і обмеження прав користувачів. Організаційні заходи можуть включати навчання працівників з питань кібербезпеки, створення відповідальної підзвітної команди з кібербезпеки та впровадження процедур реагування на інциденти.

Які виклики ставить перед військовими та державними структурами захист інформації від збройної агресії рф, зокрема щодо обмеження доступу до конфіденційної інформації?

Військові та державні організації стикаються з багатьма проблемами щодо захисту інформації від збройної агресії рф. Одним з найбільш серйозних є необхідність обмеження доступу до конфіденційної інформації. Витік такої інформації може викликати серйозні наслідки для національної безпеки. Інші

виклики включають-забезпечення безпеки інформаційних систем, захист від кібератак, боротьба з розповсюдженням фейкової інформації, контроль за доступом до інформації тощо.

Які наслідки можуть виникнути внаслідок порушення захисту інформації обмеженим доступом в умовах збройної агресії рф та як їх уникнути?

-Розголошення важливої військової та державної інформації: Якщо інформація з обмеженим доступом потрапляє до рук зловмисників, військова чи урядова інформація може бути використана проти країни, потенційно підриваючи безпеку країни.

-Пошкодження репутації: Розголошення конфіденційної інформації про країну може завдати шкоди репутації цієї країни, особливо якщо інформація містить негативні факти чи дії.

Як я вже зазначала, захист інформації з обмеженим доступом є особливо важливим в умовах збройної агресії рф, тому в такому випадку забезпечення захисту такої інформації є ще більш відповідальним засобом. Зокрема, такими є:

-Захист інформації під час передачі. Умови збройної агресії можуть бути перешкодою для забезпечення безпечної передачі інформації, особливо якщо йдеться про конфіденційні дані. Необхідно вжити заходів для забезпечення конфіденційності та запобігання несанкціонованому доступу під час передачі.

-Забезпечення цілісності інформації. Умови збройної агресії можуть призвести до спроб порушити цілісність інформації з метою зміни чи підробки її змісту. Для захисту цілісності інформації використовуються електронні підписи, шифрування та інші методи.

-Фізичний захист інформації. Фізичний доступ до пристроїв, що містять конфіденційну інформацію, може бути обмежено під час збройних нападів. Важливо забезпечити безпеку пристроїв та інформації на об’єктах і приміщеннях, які можуть бути атаковані.

Як можуть бути захищені критичні об'єкти від кібератак та інших форм вторгнення з боку рф?

Захист критичних об'єктів від кібератак та інших форм вторгнення є задачею, яка потребує комплексного підходу та взаємодії різних суб'єктів. Деякі можливі заходи для захисту критичних об'єктів від кібератак та інших форм вторгнення з боку рф можуть включати:

-Захист інфраструктури: Фізичний захист критично важливих об'єктів, таких як електростанції та транспортні вузли, є критично важливим.Також необхідно забезпечити захист від хакерських атак, що можуть бути спрямовані на збір інформації або виконання злочинної діяльності.

-Підвищення кваліфікації персоналу: у сфері кібербезпеки та використання сучасних технологій важливо забезпечити належну кваліфікацію персоналу критичних об’єктів. Крім того, співпраця зі службами безпеки.

Підсумовуючи викладене, ще раз наголошу, ці питання та їх вирішення є актуальними, оскільки рф веде активну війну проти нашої держави України та здійснює агресивну зовнішню політику. Одним з аспектів цієї агресії є кібератаки та інші форми кіберагресії, що створюють загрозу для безпеки інформації та кібербезпеки.

Крім того, ситуація, яка склалась нині вимагає підвищення заходів безпеки і захисту інформації з обмеженим доступом. З метою захисту державних та комерційних секретів, необхідно використовувати сучасні методи інформаційної безпеки, такі як шифрування, аутентифікація користувачів, контроль доступу та інші заходи. Також необхідно розробляти і використовувати спеціальні системи захисту інформації з обмеженим доступом, які забезпечують надійний захист інформації від несанкціонованого доступу.

Отже, необхідно забезпечити належний рівень освіти з питань інформаційної безпеки для працівників, які мають доступ до інформації з обмеженим доступом. Це допоможе підвищити свідомість та уважність у працівників, які мають доступ до цієї інформації, та зменшити ризик її витоку.

Література

1. Конституція України від 28.06.1996 р. №254к/96-ВР:
[URL:https://www.president.gov.ua/ua/documents/constitution/konstituciya-ukrayini-rozdil-ii].
2. Закон України «Про інформацію» від 02.10.1992 р. № 2657-ХП:
[URL.: http://https//zakon.rada.gov.ua/laws/show/2657-12#Text].
3. Кулініч О. О. Університетські наукові записки. «Інформація як об’єкт цивільних прав».2005. № 3. С. 126-128.
[URL: http://nbuv.gov.ua/UJRN/Unzap_2005_3_24].
4. Інформаційне право: Доступ до інформації: Навчальний посібник:/ за заг. ред: Марущак А. І. КНТ. 2007. 24 с.

Тимофєєв Д.С.
Кручінін О.В.
НТУ «Дніпровська політехніка»

ВПРОВАДЖЕННЯ АРХІТЕКТУРИ НУЛЬОВОЇ ДОВІРИ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ ЗАКЛАДІВ ВИЩОЇ ОСВІТИ УКРАЇНИ

Функціонування інформаційно-комунікаційних систем (ІКС) закладів вищої освіти (ЗВО) України в сучасних умовах характеризується рядом особливостей пов’язаних із багатофакторним впливом значної кількості процесів глобального та локального характеру. Домінантним на поточному етапі є реалізація заходів

прискорення інтеграції системи освіти та науки України до Європейського та Євро-Атлантичного просторів в умовах збройної агресії рф. Процеси інтеграції охоплюють одночасне реформування нормативно-правової, організаційної та програмно технічної складових зокрема у галузі інформаційної та кібербезпеки ЗВО, що призводить до необхідності запровадження актуальних та стійких методів та засобів забезпечення сталого розвитку інфраструктури підтримки та супроводу наукової та освітньої діяльності.

Особливостями ЗВО, як об'єкта інформаційної діяльності, є багатопрофільний характер, велика кількістю форм і методів навчальної роботи, просторове розгалуженням інфраструктури (філії, представництва), дистанційна взаємодія учасників процесів. Сюди ж можна віднести і різноманіття джерел фінансування, наявність розвиненої структури допоміжних підрозділів і служб (будівельна, виробнича, господарська діяльність), необхідність адаптації до мінливого ринку освітніх послуг, потреба в аналізі ринку праці, відсутність загальноприйнятої формалізації ділових процесів, необхідність електронної взаємодії з регуляторними та аудиторськими організаціями та установами, часта зміна статусу співробітників, студентів та партнерів, зокрема міжнародних. У результаті зростання кількості злочинів у сфері інформаційних технологій з'являється велика кількість вимог до захисту ресурсів обчислювальних мереж навчальних закладів і виникає потреба у постановці завдання побудови власної інтегрованої системи безпеки. Її рішення припускає наявність нормативно-правової бази, формування концепції безпеки, розробку заходів, планів і процедур щодо безпечної роботи, проектування, реалізацію і супровід технічних засобів захисту інформації в рамках освітнього закладу.

Типовою ситуацією в ІКС ЗВО України є використання гетерогенного програмно-технічного забезпечення, поєднання високотехнологічного обладнання та новітніх глобальних інформаційних сервісів, отриманих за грантовими програмами та пільговими, або безкоштовними академічними ліцензіями з застарілими автономними системами автоматизації діяльності з архаїчною архітектурою підтримки адміністративної, освітньої та науково-дослідної роботи.

Основними ризиками при використанні інформаційних ресурсів закладів вищої освіти варто відзначити такі: неконтрольований доступ до інформаційних ресурсів, низька захищеність від внутрішніх та зовнішніх загроз, незаконне копіювання інформації, порушення технологій обробки інформації, запуск програм-вірусів, знищення та модифікація даних в інформаційних системах, викрадення інформації з бібліотек, архівів, баз даних, перехоплення інформації в технічних каналах її витоку [1]. До цього додається досить низький рівень освіченості в питаннях інформаційної та кібербезпеки значної кількості співробітників та студентів, особливо молодших курсів.

Трохи зменшує проблему те, що ЗВО є стабільною, ієрархічною за функціями управління системою, що володіє всіма необхідними умовами життєдіяльності,

яка діє на принципах централізованого управління (останнє означає, що в управління завданнями інформатизації може активно використовуватися адміністративний ресурс) та певною автономією у прийнятті рішень.

Забезпечення кіберзахисту ІКС ЗВО потребує комплексного підходу з використанням кращих практик, як з точки зору організації, так і використання сучасних програмно-технічних комплексів та криптографічних систем здатних інтегрувати рішення лідерів ринку інформаційних послуг та технологій забезпечення кібербезпеки з урахуванням наявної бази та фінансових обмежень.

Враховуючи вищевикладене, особливої актуальним є питання удосконалення процесу управління при використанні інформаційних ресурсів з впровадженням гнучких технологій ідентифікації та контролю користувачів та сервісів ІКС ВНЗ в умовах динамічних змін конфігурації та складових об'єкту захисту.

Значну кількість означених проблем має змогу вирішити запровадження принципів та компонентів архітектури нульової довіри. За визначенням компанії Gartner [2] доступ до мережі з нульовою довірою (ZTNA) це продукти та послуги, які створюють межу логічного доступу на основі ідентифікації та контексту, які охоплюють корпоративного користувача та внутрішні додатки або набір додатків. Додатки приховано від виявлення, а доступ обмежено через довірчий брокер до множини названих об'єктів. Посередник перевіряє особу, контекст і дотримання політики зазначених учасників, перш ніж дозволити доступ, і мінімізує бічні переміщення в інших місцях мережі. ZTNA усуває надмірну неявну довіру, яка часто супроводжує інші форми доступу до додатків, такі як застаріла VPN. ZTNA разом із брокерами безпечного доступу до хмарних сервісів (CASB) та шлюзами мережної безпеки (SWG) є однією з основних технологій, які складають ринок послуг безпеки.

Відповідно до NIST SP 800-207 [3] Архітектура нульової довіри має бути розроблена та розгорнута з дотриманням наступних основних положень:

1. Ресурси. Організації слід захищати всі свої дані, послуги та пристрої. Якщо користувачі мережі можуть отримувати доступ до ресурсів організації з власних пристроїв, такі аксесуари теж підпадають під захист підприємства.

2. Комунікації. Всі комунікації, як усередині, так і за межами мережі, повинні оброблятися однаково та захищатися найбезпечнішим із доступних методів.

3. Посесійний доступ. Кожне підключення до критично важливого ресурсу чи організації має встановлюватись окремо для кожного сеансу.

4. Динамічні політики. Доступ до ресурсів організації має надаватися відповідно до правил політики організації та за принципом найменших привілеїв. Така політика має визначати ресурси організації, користувачів та права доступу для цих користувачів.

5. Моніторинг. Для забезпечення належного захисту даних та корпоративних ресурсів організації повинні здійснювати моніторинг цих ресурсів.

6. Аутентифікація та авторизація. Перед наданням доступу до будь-якого корпоративного ресурсу організація має забезпечити динамічну аутентифікацію та авторизацію.

7. Безперервне поліпшення. Організація повинна збирати інформацію про поточний стан мережних активів, інфраструктуру та з'єднання, щоб поліпшити стан безпеки мережі.

В ІКС ЗВО проблематично та недоцільно застосовувати відразу всі сім принципів проектування відповідної архітектури. Реалізацію можна впроваджувати послідовно, з урахуванням наявних ресурсів та технологій, що дасть змогу в першу чергу мінімізувати найбільші ризики.

Розпочинаючи планування архітектури необхідно визначитись з наявними технологіями у корпорацій - постачальників сервісів в конкретному ЗВО. На даний час більшість провідних постачальників, як то Google, Microsoft, CISCO, Cloudflare та інші вже мають комплексні пропозиції з впровадження відповідних технологій для інфраструктури організацій та установ, у тому числі науково-освітніх. Кожне з цих рішень дозволяє поетапно реалізувати ряд переваг:

- ідентифікація, класифікація та моніторинг наявних мережевих ресурсів, що забезпечить прозорість та керованість інфраструктури, швидкість реагування на інциденти;
- управління доступом з урахуванням централізованих чітко визначених політик та правил, що мінімізує ризики несанкціонованого доступу;
- мікросегментація – дозволить розбити охоронний периметр на менші зони, що мінімізує швидкість розповсюдження атаки та наслідки її реалізації.

Основні проблеми впровадження в архітектури нульової довіри в ІКС ЗВО: відсутність формалізації бізнес-процесів, низьке фінансування, застарілі та гетерогенні архітектури ІКС, недостатня кваліфікація та кількість фахівців з кібербезпеки та інформаційних технологій, неможливість застосування суворих протоколів для окремих категорій користувачів.

Література

1. Ільїн О.О. Аналіз уразливості інформаційного ресурсу вищого навчального закладу та класифікація загроз інформаційної безпеки // Ільїн О.О., Сєрих С.О., Вишнівський В.В. Сучасний захист інформації.- №1, 2017, с.66-72.

2. What is Zero Trust Network Access? [Електронний ресурс]. – Режим доступу: https://www.gartner.com/reviews/market/zero-trust-network-access

3. NIST Special Publication 800-207 «Zero Trust Architecture». [Електронний ресурс]. – Режим доступу: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

Толкачов М.Ю.
кафедра Системи інформації ім. В.О. Кравця Інституту комп'ютерного моделювання, прикладної фізики та математики Національного технічного університету «Харківський політехнічний інститут»
Дженюк Н.В.
кафедра Системи інформації ім. В.О. Кравця Інституту комп'ютерного моделювання, прикладної фізики та математики Національного технічного університету «Харківський політехнічний інститут»

ПОБУДОВА БАГАТОКОНТУРНОЇ СИСТЕМИ БЕЗПЕКИ МЕРЕЖ ЗА ВПЛИВУ СОЦІОЛОГІЧНИХ СКЛАДОВИХ НАВАНТАЖЕННЯ

На сьогоднішній день гібридні атаки, які реалізуються з ймовірністю 95%, становлять основну загрозу. Тому що вони комплексні та націлені на результат. Ці погрози мають кілька каналів впливу. Вони можуть впливати на певні послуги безпеки, а також можуть отримувати ефект синергії. Не просто складання загроз, отримання доступу або заподіяння шкоди, а це в кілька разів збільшений ефект та вплив на всі складові послуг безпеки.

Одним із каналів впливу є вплив штучного інтелекту на стійкість захисту різних систем. Системи штучного інтелекту також несуть із собою низку ризиків, які повною мірою не враховуються за допомогою існуючих структур і підходів до управління ризиками. З іншого боку, при належному контролі системи штучного інтелекту можуть пом'якшувати загрози безпеці, їх наслідки та керувати ними [1].

У новій реальності викликів, де перетинаються безпрецедентний гібридний вплив, загроза неефективного застосування існуючих алгоритмів та безперервне впровадження штучного інтелекту, необхідний новий підхід до формування безпосередньо систем безпеки. Цей підхід використовує багатоконтурні системи безпеки.

Метою роботи є розробка моделі побудови багатоконтурної системи безпеки мереж. В основу взаємодії в системі запропоновано підхід Zero Trust Security. Такий підхід дозволить сформувати систему безпеки мереж, що охоплює весь стек мережної безпеки.

Для зовнішнього контуру системи безпеки можна виділити доступ до служб, ресурсів, до яких не потрібні облікові дані (наприклад, загальнодоступна веб-сторінка). У цьому випадку принципи Zero Trust Architecture не використовуються безпосередньо. Складність контролю трафіку зростає коли необхідні активи, не належать підприємству і містять згенеровані штучно компоненти соціологічного впливу. У цих випадках підприємство обмежене щодо того, які внутрішні політики кібербезпеки можуть застосовуватись. У цьому випадку вживаються додаткові, більш глибокі, ресурсомісткі заходи. Ці заходи можуть бути як додаткова сегментація та інтелектуальний аналіз навантаження трафіку [2].

Для комплексних викликів безпеки для внутрішнього та зовнішнього контуру запропоновано модель взаємодії компонентів програмно-визначеної інфраструктури та окремо компонентів периметра мережі. Модель визначає базові відносини між компонентами та їх взаємодіями. Точка ухвалення рішення про застосування політики розбита на два логічні компоненти: механізм політики та адміністратор політики. Логічні компоненти Zero Trust Architecture використовують для зв'язку окрему площину управління, тоді як дані додатків передаються у площині даних.

Механізм політик використовує політику підприємства, вхідні дані із зовнішніх джерел (наприклад, систем CDM, служб аналізу загроз), а також ієрархії уявлень об'єктів, згенерованих штучним інтелектом як вхідні дані для алгоритму довіри. Механізм політик пов'язаний із компонентом адміністратора політик.

Адміністратор політик відповідає за встановлення, маркування та поділ навантаження за ознаками, включаючи соціологічний аналіз. Він тісно пов'язаний з механізмом політик і залежить від його вирішення, яке подання застосувати до фрагмента навантаження [3].

Пропонований підхід не має на увазі довіри до всієї передбачуваної передачі навантаження, а встановлює довіру для кожного фрагмента навантаження, отриманого в результаті сегментації на основі алгоритму довіри. Сегментація навантаження здійснюється на основі політик та за алгоритмами, розробленими на основі семіотичного аналізу.

Література

1. NIST AI 100-1 Artificial Intelligence Risk Management Framework (AI RMF 1.0) (January 2023). https://doi.org/10.6028/NIST.AI.100-1.

2. Rose, S. et al. (August 2020). Zero Trust Architecture, National Institute of Standards and Technology (NIST) Special Publication 800-207, Gaithersburg, Md., https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

3. Zhang J.J., Wang F.Y., Wang X., Xiong G., Zhu F., Lv Y., Hou J., Han S., Yuan Y., Lu Q., et al. Cyber-physical-social systems: The state of the art and perspectives. IEEE Trans. Comput. Soc. Syst. 2018;5: 829–840. doi: 10.1109/TCSS.2018.2861224.

Толстяков Є.О.
Національна академія Служби безпеки України

РОЗПОВСЮДЖЕННЯ НЕПЕРЕВІРЕНОЇ ІНФОРМАЦІЇ ЧЕРЕЗ ЛОКАЛЬНІ ГРУПИ МЕСЕНДЖЕРІВ ТА ВИКОРИСТАННЯ КРИТИЧНОГО МИСЛЕННЯ ЯК ЗАХОДУ ПРОТИДІЇ

Якщо виділяти за загрозами, то одним з основних напрямів інформаційної безпеки є захист від розповсюдження неправдивої інформації. На сьогодні одним із найпопулярніших сервісів за допомогою якого можливо масово розповсюджувати інформацію стають так звані канали у популярних месенджерах таких як Whatsapp, Viber, Telegram. За даними сервісу Apptopia станом на березень 2023 року найбільш популярним месенджером в України із функціоналом створення публічних каналів та локальних груп за кількістю скачувань є Telegram (3 місце у загальному рейтингу безкоштовних додатків проти 8-го у Viber та 10-го у Whatsapp для iOS та 2 місце проти 4-го у Whatsapp та 17-го у Viber для пристроїв на базі Android).

Навіть у глобальному рейтингу за останні 5 років Telegram випередив Facebook Messenger і став найпопулярнішим хмарним додатком для обміну повідомленнями. Зараз Telegram поступається лише WhatsApp і з кожним роком скорочує розрив, про що заявив у лютому 2023 року П. Дуров, засновник Telegram, у своєму каналі. Тож канали на його платформі стають потужним елементом інформаційного впливу, конкуруючи із класичними засобами масової інформації (ЗМІ).

Козубцов І.М. та Козубцова Л.М. у своєму переліку об’єктів критичної інфраструктури (ОКІ) відносять соціальні мережі спілкування, до системи *соціального* значення. Як можливі наслідки негативного впливу на них виділяють суспільний колапс, можливі маніпуляції суспільною думкою, викривлення подій в людському сприянні, реалізація психологічного тиску на суспільство для підготовки та ведення гібридної війни.

Канали є інструментом для трансляції повідомлень широкій аудиторії. Людина яка адмініструє канал може залишатися анонімною, хоча існує система верифікації, за допомогою якої та чи інша публічно відома особа може підтверджувати, що інформація виходить дійсно від неї.

Разом із публічними каналами, як зручний засіб комунікації із родичами, друзями, колегами широкого розповсюдження набули групи у месенджерах. Мета створення таких груп – це, зазвичай, необхідність у швидкому доведенні необхідної інформації визначеному колу осіб, її обговорення та звітування.

Групи ідеально підходять для обміну матеріалами з друзями та родиною або для співпраці в невеликих командах. Але групи також можуть бути дуже великими (у Telegram є можливість підтримувати спільноти до 200 000 учасників).

Якщо розглядати робочі групи, в них часто керівником проекту чи іншою особою, якій делеговані комунікативні функції з окремих питань, доводиться необхідна інформація, як то робочі завдання, повідомлення про зміни графіку, кадрові рішення тощо.

Серед іншого, в умовах повномасштабної збройної агресії рф, часто у робочих групах повідомляються про протоколи особистої та корпоративної безпеки, що є цілком виправданим в умовах змін у тактиці ворога та створення нових засобів протидії їй.

З урахуванням того, що робочі групи часто створюються як допоміжний інструмент інформування на ентузіазмі колективу, порядок їх використання не протоколюється, що призводить до тих чи інших зловживань. Такими зловживаннями можуть бути безневинні повідомлення особистого характеру (привітання зі святами, посилання на розважальні ресурси, веселі меми), шкода від яких полягає лише у відволіканні від робочого процесу. Або ж це може бути розповсюдження неперевіреної інформації соціально-значущого для учасників групи характеру, яка може впливати на прийняття управлінських рішень та морально-психологічний клімат у колективі.

У системі розповсюдження інформації завжди приймають участь дві сторони: *адресант* та *адресат*, тобто відправник та отримувач повідомлення. В робочих групах організацій з чіткою ієрархією службових відносин, зазвичай керівник (або уповноважена особа), виступає в ролі адресанта, що, з врахуванням ієрархічності системи, може додавати повідомленням додаткового авторитету. Така інформація часто сприймається без достатньої критичної оцінки, спираючись на надійність джерела за замовчуванням.

Відсутність у месенджерах надійної внутрішньої або сторонньої системи перевірки інформації призводить до того, що вся відповідальність за її якість лягає на членів спільноти (тих хто розповсюджує та отримує її). Тож нерідко ми зіштовхуємся з переважанням емоційного підходу над раціональним при прийнятті рішень про розповсюдження повідомлень, що, поряд з широким використанням інформаційно-психологічного впливу ворога, може призвести до небажаних наслідків. Основною метою такого впливу зазвичай ставиться створення хаосу та морального дисбалансу. Побічним негативним наслідком може стати оприлюднення інформації з обмеженим доступом, якщо до інформаційно-психологічної складової додати елементи соціальної інженерії (психологічне маніпулювання людьми з метою здійснення певних дій або розголошення конфіденційної інформації).

Однією з основних причин за яких стає можливим неконтрольоване розповсюдження неперевіреної інформації стає відсутність чітких вимог щодо порядку її розповсюдження у робочих групах.

Яким чином можна завадити негативному впливу неправдивої інформації у локальних групах в месенджерах? Перш за все, пропонується використовувати ті

стандарти (як зі сторони адресанта, так і адресата), які є загальноприйнятими в інституціях, масове розповсюдження інформації якими є основним видом їх діяльності, тобто ЗМІ.

Підхід до оприлюднення отриманої інформації напрацьовувався у ЗМІ весь час їх існування та складається з декількох елементів, серед яких провідне місце посіла перевірка на правдивість викладених фактів або факт-чекінг (fact-checking).

Є дві загальноприйняті формули перевірки фактів: 5W+H та IMVAIN.

Перша – це система питань, які ви можете ставити до вхідної інформації. W та H позначають перші літери спеціальних питань в англійській мові: What? – Що сталося? Why? – Чому це сталось? Who? – Хто про це повідомив? Where? – Де це сталося? When? – Коли сталося? How? – Як це відбулося?

Друга - це властивості, якими має володіти надійне *джерело*. Метод названий за першими буквами цих властивостей: Independent - незалежне, Multiple - множинне, Verify - перевірене, Authoritative - авторитетне, Named – назване.

Питання IMVAIN потрібно ставити лише до джерела, а не інформації загалом. Якщо є відповіді на всі питання і вони вас влаштовують, то джерелу можна довіряти. Якщо не можна відповісти хоча б на два запитання, цій інформації рекомендують недовіряти.

Поширення неперевіреної інформації може стати серйозною проблемою, оскільки це може призвести до поширення неправдивої інформації, яка може негативно вплинути на окремі групи людей та суспільство в цілому. Щоб запобігти цьому, можна вжити кілька заходів.

Перш за все, важливо розвивати критичне мислення у себе та оточення, навчитися аналізувати інформацію, перевіряти її достовірність та переконуватися у її правдивості перед тим, як її поширювати.

Другим заходом може стати попередження людей про небезпеку поширення неперевіреної інформації, це може бути небезпечним та сприяти негативним наслідкам. Таким чином, вони можуть стати більш уважними та обережними при обміні інформацією.

Третім заходом може стати активне використання інформаційних ресурсів (довідкові сайти, відомі новинні портали, наукові видання тощо). Це може допомогти знайти достовірну інформацію та переконатися у її правдивості перед поширенням.

Література

1. Організація захисту інформації з обмеженим доступом, Гуз А.М., Довгань О.Д., Марущак А.І. та ін. ; за заг. ред. Є.Д. Скулиша. - К. : Наук.-вид. відділ НА СБ України, 2011. - 378 с.

2. Козубцов І.М., Козубцова Л.М., Прогноз можливих наслідків настання «колапсу інформаційних систем спеціального призначення» // Збірник тез

наукових доповідей (Київ, 26 березня 2021 року) – С. 50-53. URL: https://academy.ssu.gov.ua/uploads/p_57_53218641.pdf (дата звернення 18.03.2023).

3. Рейтинг додатків Apptopia URL: https://apptopia.com/store-insights/top-charts/itunes-connect/social-networking/ukraine (дата звернення 18.03.2023).

Тугарова О.К.
кандидат юридичних наук, доцент
Національна академія Служби безпеки України

СВОБОДА СЛОВА В УМОВАХ ВОЄННОГО СТАНУ: ПИТАННЯ ПРАВОВОГО РЕГУЛЮВАННЯ

Широкомасштабне вторгнення російської федерації наприкінці лютого минулого року створило перед українським суспільством проблему реалізації права на свободу слова і визначення чіткого балансу між можливістю вільно збирати, зберігати, використовувати і поширювати інформацію засобами масової інформації (медіа) та захистом інтересів держави у воєнний час.

Одним із перших нормативно-правових актів, який визначив межу допустимого обмеження свободи слова та вільного обігу інформації, став Указ Президента України «Про введення воєнного стану в Україні» [2], норми якого закріпили положення щодо тимчасового (на період дії правового режиму воєнного стану) обмеження конституційного права на свободу думки і слова, на вільне вираження своїх поглядів і переконань (ст. 34 Конституції України) [1]. Це положення зумовило внесення змін у роботу засобів масової інформації та медійний ландшафт країни.

Нагальним питанням стало вирішення проблеми щодо можливості вітчизняних та іноземних медіа оперативно, достовірно і повно оприлюднювати суспільно необхідну інформацію про стан бойових дій в країні і недопущенням розголошення відомостей, які потенційно можуть вплинути на стан захищеності окремих територій, завдати ризик життю і здоров'ю цивільних і військових.

Наказом Головнокомандуючого Збройних Сил України № 73 від 03.03.2022 року «Про організацію взаємодії між Збройними Силами України, іншими складовими сил оборони та представниками засобів масової інформації на час дії правового режиму воєнного стану» (далі - Наказ) [3] було визначено перелік інформації, на яку встановлено заборону поширення посадовими або службовими особам під час спілкування з представниками медіа, а саме:

- відомості (інформація) з обмеженим доступом, що підпадають під дію Зводу відомостей, що становлять державну таємницю, затвердженого наказом Центрального управління Служби безпеки України від 23 грудня 2020 року № 383, зареєстрованого в Міністерстві юстиції України 14 січня 2021 року № 52/35674;

- відомості (інформація) з обмеженим доступом, що включені до Переліку відомостей Збройних Сил України, що становлять службову інформацію, затвердженого наказом Генерального штабу Збройних Сил України від 22 листопада 2017 року № 408.

Крім того, Наказом затверджено перелік інформації, розголошення якої може призвести до обізнаності про дії Збройних Сил України, інших складових сил оборони, негативно вплинути на хід виконання завдань за призначенням правового режиму воєнного стану, зокрема:

1) найменування військових частин (підрозділів) та інших військових об'єктів в районах виконання бойових (спеціальних) завдань, географічні координати місць їх розташування;

2) чисельність особового складу військових частин (підрозділів);

3) кількість озброєння та бойової техніки, матеріально-технічних засобів, їх стан та місця зберігання;

4) описи, зображення та умовні позначки, які ідентифікують або можуть ідентифікувати об'єкти;

5) інформація щодо операцій (бойових дій), які проводяться або плануються;

6) інформація щодо системи охорони та оборони військових об'єктів та засобів захисту особового складу, озброєння та військової техніки, які використовуються (крім тих, які видимі або очевидно виражені);

7) порядок залучення сил та засобів до виконання бойових (спеціальних) завдань;

8) інформація про збір розвідувальних даних (способи, методи, сили та засоби, що залучаються);

9) інформація про переміщення та розгортання своїх військ (найменування, кількість, місця, райони, маршрути руху);

10) інформація про військові частини (підрозділи), форми, методи, тактику їх дій та способи застосування за призначенням;

11) інформація про проведення унікальних операцій із зазначенням прийомів та способів, що використовувались;

12) інформація про ефективність сил і засобів радіоелектронної боротьби противника;

13) інформація про відкладені або скасовані операції;

14) інформація про зниклий або збитий літак, літальний апарат, зникле судно та пошуково-рятувальні операції, які плануються або проводяться;

15) інформація про планування та проведення заходів забезпечення безпеки застосування військ (дезінформація, імітація, демонстративні дії, маскування, протидія технічним розвідкам та захист інформації);

16) відомості про проведені інформаційно-психологічні операції, ті, що проводяться, а також плануються;

17) інформація, яка має на меті пропаганду або виправдання широкомасштабної збройної агресії Російської Федерації проти України (Додаток 2 до Наказу) [3].

Місяць тому до Наказу було внесено зміни, які доповнили й оновили правила роботи журналістів в прифронтових зонах. Відтак, в новій редакції визначено зони для перебування представників медіа:

- *зелена* (дозволяється робота акредитованих представників ЗМІ без супроводу офіцера зі зв'язків з громадськістю, або іншої, визначеної командиром посадової особи);
- *жовта* (дозволяється робота акредитованих представників ЗМІ лише у супроводі офіцера зі зв'язків з громадськістю або іншої, визначеної командиром посадової особи);
- *червона* (робота акредитованих представників ЗМІ заборонена) (п.1 Додатку 2 Наказу). Зазначені нововведення є спробою спростити доступ журналістів до прифронтових територій, на яких вже не ведуться бойові дії.

Крім того, в новій редакції встановлено заборону посадовим або службовим особам, які виконують бойові (спеціальні) завдання, давати інтерв'ю або коментарі представникам медіа; у виключних випадках така можливість надається за умови наявності дозволу відповідних керівників, командирів (начальників) виключно після проходження інструктажу щодо недопущення поширення інформації з обмеженим доступом та вимог законодавства України у цій сфері (п.3. Наказу).

Змінені і правила отримання журналістами акредитації: запроваджено прескарту журналіста нового зразка, встановлено заборону на використання інших, додаткових акредитацій для представників медіа, визначено підстави відповідальності за порушення вимог, визначених у документі.

Утім, не зважаючи на такі обмежувальні заходи, слід відзначити, що норми Наказу закріплюють *обов'язок* командувачів складових сил оборони на час дії правового режиму воєнного стану забезпечувати у районах проведення бойових дій роботу акредитованих представників засобів масової інформації, у тому числі іноземних (п.2 Наказу). Такий підхід свідчить про розуміння важливості роботи представників засобів масової інформації в зонах проведення бойових дій, про усвідомлення державою вагомої ролі мас медіа у формуванні думки вітчизняної і закордонної аудиторії, і, зрештою, про реальний рівень цивілізованості українського суспільства.

Література

1. Конституція України : офіц. текст. Київ : КМ, 2019. 96 с

2. Про введення воєнного стану в Україні: Указ Президента України від 24.02. 2022 р. № 64/2022. URL: https://zakon.rada.gov.ua (дата звернення: 19.03.2023)

3. Про організацію взаємодії між Збройними Силами України, іншими складовими сил оборони та представниками засобів масової інформації на час дії правового режиму воєнного стану: Наказ Головнокомандуючого Збройних Сил України від 03.03.2022 р. № 73 (із змінами, внесеними згідно з наказом № 196 від 12.07.2022; № 266 від 03.10.2022; № 49 від 27.02.2023).URL: https://www.mil.gov.ua (дата звернення: 19.03.2023)

Шепета О.В.
кандидат юридичних наук, доцент
ННІ ІБ СК НА СБ України

ОСНОВНІ ПРИНЦИПИ ОРГАНІЗАЦІЇ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ В УМОВАХ ВІЙСЬКОВОЇ АГРЕСІЇ рф

У сучасному діловому світі інформація вважається одним із найцінніших активів організації. Захист інформації є найважливішим аспектом політики безпеки будь-якого підприємства, який забезпечує конфіденційність, цілісність і доступність інформації. На даний момент Україна переживає військову агресію російської федерації, а як ми всі знаємо, військові конфлікти можуть завдати значних збоїв бізнесу та призвести до втрати цінних інформаційних ресурсів. Тому під час військових конфліктів підприємства повинні вживати заходів для захисту своєї інформації від крадіжки, втрати чи знищення. Так для захисту інформації на підприємстві розглянемо ключові принципи, методи та підходи, які повинні застосовуватися підприємствами для захисту своїх інформаційних активів під час військового конфлікту.

Перший принцип, якого слід дотримуватися, це комплексна оцінка ризику. Підприємства повинні проводити ретельну оцінку ризиків, щоб визначити потенційні загрози своїм інформаційним активам. Це може включати аналіз потенційних вразливостей, таких як незахищені мережі чи незашифровані дані, а також оцінку потенційного впливу злому. Результати цієї оцінки повинні стати основою для розробки ефективної політики безпеки.

Політика безпеки – другий принцип, якого слід дотримуватися. Політика безпеки повинна чітко визначати заходи, які підприємства вживатимуть для захисту своїх інформаційних активів під час військового конфлікту. Ця політика повинна включати структуру для впровадження заходів безпеки, таких як брандмауери, системи виявлення вторгнень і шифрування. Політика також

повинна включати вказівки щодо поведінки співробітників, як-от управління паролями, обробка даних і віддалений доступ.

Третій принцип – розвиток міцної культури безпеки. Підприємства повинні створити культуру безпеки, яка підкреслює важливість захисту інформаційних активів. Цього можна досягти за допомогою навчальних програм, інформаційних кампаній і регулярних оцінок. Співробітників слід навчити найкращим методам безпеки, таким як виявлення фішингових електронних листів і уникнення публічних мереж Wi-Fi. Крім того, підприємства повинні проводити регулярні оцінки безпеки, щоб виявити потенційні слабкі місця в інфраструктурі безпеки та завчасно їх усунути.

Нарешті, четвертий принцип — проактивний підхід. Підприємства повинні застосовувати проактивний підхід до захисту інформації, регулярно оцінюючи стан безпеки та впроваджуючи заходи безпеки напередодні потенційної атаки. Це може включати регулярне сканування вразливостей і тестування на проникнення, а також впровадження заходів безпеки, таких як шифрування та резервне копіювання даних.

Підсумовуючи, організація захисту інформації на підприємстві в умовах військової агресії російської федерації вимагає комплексного підходу, що включає оцінку ризиків, ефективну політику безпеки, міцну культуру безпеки та проактивний підхід. Дотримуючись цих основних принципів, підприємства можуть краще захистити свої інформаційні активи та зменшити ризики, втрати або крадіжки інформації в період військової агресії.

Шиян І.О.
Національна академія СБ України

ПРОБЛЕМНІ ПИТАННЯ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ В УМОВАХ ЗБРОЙНОЇ АГРЕСІЇ рф

Кіберпростір використовується як один з інструментів війни між Україною та рф. Росія активно використовує кібератаки та кібершпигунство, щоб отримати перевагу в інформаційній та технологічній сфері.

Сторона рф використовує кібератаки для здійснення шпигунства, розповсюдження дезінформації, крадіжки даних з обмеженою інформацією та підриву кіберінфраструктури України. Наприклад, 23 лютого 2022 року, за день до російського вторгнення в Україну, відбулися чергові атаки на державні та банківські сайти. Приблизно о 16:00, було пошкоджено сайти Верховної Ради, Кабінету Міністрів України та Міністерства закордонних справ, СБУ та інші [1].

Українська ж сторона використовує, у свою чергу, кіберпростір для захисту від кібератак, для контратак та шпигунства. Українська армія створила спеціальні підрозділи з кібербезпеки (війська зв'язку та кібербезпеки Збройних сил України), які займаються виявленням та протидією кібератакам, як на цивільні, так і на об’єкти критичної інфраструктури. Також Україна використовує кіберпростір для збору інформації про дії противника та розповсюдження власної інформації на територіях рф [2].

Базовими принципами інформаційної безпеки є забезпечення цілісності інформації, її конфіденційності і водночас доступності для всіх авторизованих користувачів. Із цього погляду основними випадками порушення безпеки інформації можна назвати такі: несанкціонований доступ; витік інформації; втрата інформації; підробка інформації; блокування інформації; порушення роботи інформаційної системи [3].

Причинами витоку інформації з обмеженим доступом в умовах збройної агресії рф можуть бути збої обладнання; некоректна робота програмного забезпечення; навмисні дії сторонніх осіб; помилки обслуговуючого персоналу та користувачів – випадкове знищення або змінювання даних; некоректне використання програмного та апаратного забезпечення, яке призводить до порушення нормальної роботи системи, виникнення вразливих місць, знищення або змінювання даних, порушення інтересів інших законних користувачів тощо; неефективно організована система захисту; втрата інформації через неправильне зберігання архівних даних тощо); навмисні дії обслуговуючого персоналу та користувачів.

Як видно з описаного вище, однією з основних та непередбачуваних проблем захисту інформації з обмеженим доступом в умовах збройної агресії є людський фактор – недостатня кваліфікація персоналу, який має доступ до інформації з обмеженим доступом. Наприклад, працівники можуть не мати достатніх знань і навичок щодо захисту інформації або не дотримуватися правил безпеки. Це може призвести до порушення конфіденційності та розкриття інформації. Крім того, якщо співробітники не знають, як правильно поводитися з обмеженою інформацією, вони стають легкою мішенню для кібератак і шахрайства [4]. Тому необхідне проведення інформування персоналу підприємства про правила поводження з конфіденційною інформацією.

Щоб запобігти подібним ситуаціям, необхідно забезпечити належне навчання співробітників правилам захисту інформації та безпеки. Крім того, повинна діяти система контролю та моніторингу, яка допоможе виявити факти недотримання правил безпеки та забезпечить швидке реагування на порушення.

Ще одним важливим аспектом для захисту інформації з обмеженим доступом є існування ефективної системи інформаційної безпеки з чітким розумінням та визначенням загроз інформації, що охороняється. У свою чергу, створення системи інформаційної безпеки є масштабною роботою, яка вимагає серйозних

зусиль: ідентифікації найбільших ризиків, які існують для інформаційної безпеки підприємства; розроблення додаткових заходів щодо забезпечення безпеки; розроблення і введення простої системи класифікації ступеня конфіденційності інформації, що обробляється [5].

Отже, важливо встановити якісний та ефективний механізм перевірки кваліфікації кожного працівника, який має доступ до обмеженої інформації, щоб гарантувати, що вони мають необхідні знання та навички для роботи з цією інформацією.

Для забезпечення якісного навчання співробітників захисту інформації необхідні регулярні тренінги та семінари. Це допоможе переконатися, що співробітники розуміють загрози, які можуть виникнути при роботі з обмеженою інформацією, і знають, як діяти в таких ситуаціях.

Крім того, слід забезпечувати належну захищеність інформації, щоб зменшити ризики її витоку. Для цього можна використовувати різні методи захисту, шифрування даних, обмеження доступу до інформації по рівнях та за допомогою паролів та ідентифікаційних кодів, а також захист від кібератак, тощо.

Література

1.Закон України “Про інформацію” від 2 жовтня 1992 року // Із змінами, внесеними згідно із Законами N 2756-VI (2756-17) від 02.12.2010, ВВР, 2011, N 23, ст.160.

2. Гуз А.М. Організація захисту інформації з обмеженим доступом : Підручник / [А.М. Гуз, О.Д. Довгань, А.І. Марущак та ін.; за заг. ред. Є.Д.Скулиша]. – К. : Наук.-вид. відділ НА СБ України, 2011. – 378 с.

3. Хорошко В. О. Методичне забезпечення підготовки та перепідготовки спеціалістів з інформаційної безпеки / Хорошко В. О., Орєхова І. І. // Сучасна спеціальна техніка, №3, 2011. – С. 22-27.

4. Лісовська Ю.П. Кібербезпека: ризики та заходи. Кондор. 2019. 272 с.

5. Гулак Г.М. (2020) Методологічні засади побудови гарантоздатних захищених інформаційних систем дистанційного навчання закладів вищої освіти // Математичні машини і системи. 2020. № 4. С. 148–162.

СЕКЦІЯ 4
ПРІОРИТЕТНІ НАПРЯМКИ РОЗВИТКУ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ ЗА ОЦІНКАМИ МОЛОДИХ ВЧЕНИХ, ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Александров Р.О.
Чечко А.Р.
Національна академія СБ України

ПРОБЛЕМИ ПРОТИДІЇ ІНФОРМАЦІЙНИМ, ПСИХОЛОГІЧНИМ ВПЛИВАМ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ НА ОСОБОВИЙ СКЛАД ЗБРОЙНИХ ФОРМУВАНЬ СТРУКТУР СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

Протидія інформаційним та психологічним впливам Російської Федерації на особовий склад збройних формувань структур сектору безпеки і оборони України є важливою проблемою, яка потребує уваги та дієвих заходів

Однією з найбільших загроз є інформаційна війна, що проводиться Росією, з метою дискредитувати, дезінформувати та дестабілізувати українські військові структури. Це може бути досягнуто шляхом розповсюдження фейкових новин, спекуляції на чутках, використання соціальних мереж для поширення пропагандистського матеріалу тощо.

Крім того, необхідно розробити та впровадити ефективну систему моніторингу та аналізу інформаційних та психологічних впливів з боку Росії на особовий склад збройних формувань, цього можна досягнути шляхом проведення спеціальних тренувань та психологічних підготовок, які допоможуть зберегти бойовий дух та збільшити віру в свої сили. Це дозволить швидко реагувати на можливі загрози та приймати ефективні заходи для захисту від них.

Також важливо вживати заходів для забезпечення військової безпеки та захисту від можливих вторгнень з боку Росії. Для цього потрібно забезпечити належний рівень забезпечення військової техніки, озброєння та спеціального обладнання, проводити регулярні тренування та практичні заняття, забезпечувати високий рівень професійної підготовки військовослужбовців.

Окрім цього, важливо розробити та впровадити ефективні заходи з кадрової політики та внутрішнього контролю, щоб запобігти можливим впливам з боку Росії на внутрішні процеси військових структур.

Також необхідно забезпечити взаємодію та координацію між різними структурами сектору безпеки та оборони, зокрема між військовими та цивільними структурами. Це дозволить ефективніше протистояти загрозам з боку Росії та забезпечити військову безпеку України в цілому.

Узагалі, ефективна протидія інформаційним та психологічним впливам Росії

на особовий склад збройних формувань структур сектору безпеки і оборони України потребує комплексного підходу, який включає в себе різноманітні заходи з підвищення рівня професійної підготовки військовослужбовців, кадрової політики, забезпечення військової безпеки та взаємодії між різними структурами.

Відсутність ефективної інформаційної політики в Україні може стати однією з причин, що сприяють впливу фейків з боку Російської Федерації на військовослужбовців. Інформаційна політика повинна забезпечувати доступ до достовірної та об'єктивної інформації для військових, а також сприяти формуванню правильних уявлень про реальні загрози та ситуацію в країні.

Фейки з боку Росії можуть викликати певні відчуття незахищеності та невпевненості серед військовослужбовців, а також дискредитувати українську владу та військові структури. Це може призвести до зниження морального духу військовослужбовців, зменшення їхньої бойової готовності та забезпечення військової безпеки країни в цілому.

Для протидії впливу фейків з боку Російської Федерації на військовослужбовців необхідно розробити та впровадити ефективну інформаційну політику, яка має на меті забезпечення доступу до достовірної та об'єктивної інформації. В рамках цієї політики необхідно проводити регулярні інформаційні кампанії, тренінги та семінари, які мають на меті формування правильних уявлень про реальні загрози та ситуацію в країні.

Також важливо розробити та впровадити систему раннього попередження впливу фейків на військовослужбовців, яка дозволяє швидко виявляти та реагувати на негативні інформаційні впливи. Для цього можна використовувати різні інструменти, такі як моніторинг соціальних мереж та засобів масової інформації, аналіз та оцінку інформації з боку Росії, швидку розсилку відповідної інформації військовим структурам тощо.

Крім того, важливо забезпечити військовослужбовців інформаційними ресурсами, які містять достовірну та об'єктивну інформацію про ситуацію в країні, стратегічні та тактичні завдання збройних сил України, а також про підтримку військовослужбовців з боку суспільства та держави.

Крім того, для зменшення впливу ворожих інформаційних операцій на особовий склад потрібно проводити спеціалізовані тренінги чи консультації, а також надавати військовослужбовцям психологічну підтримку.

Загалом, для протидії інформаційним та психологічним впливам Російської Федерації на особовий склад збройних формувань структур сектору безпеки і оборони України, необхідно вирішувати комплексну проблему, яка передбачає розробку та впровадження ефективної інформаційної та психологічної політики, підвищення морально-психологічної стійкості військовослужбовців, забезпечення їхнього психологічного здоров'я та підтримки з боку суспільства та держави.

Використання іноземних ЗМІ Російською Федерацією для дестабілізації ситуації в Україні є одним зі засобів інформаційної війни. Російські ЗМІ з метою

впливу на настрої українців можуть створювати та поширювати фейкові новини, дезінформацію та пропаганду.

Для протидії цьому необхідно в першу чергу забезпечити своїх громадян інформаційною безпекою. Держава має створити спеціальні служби, які б відслідковували та аналізували інформацію, що поширюється через іноземні ЗМІ, та проводили б інформаційну контррозвідку.

Для ефективної протидії інформаційній війні також необхідно розвивати національні ЗМІ, які мають високу довіру серед громадян та здатні швидко та ефективно реагувати на фейкові новини та дезінформацію.

Крім того, необхідно проводити інформаційну роботу серед населення, пояснюючи, як розпізнавати фейкові новини та дезінформацію та як бути обережними при роботі з інтернет-ресурсами. Також важливо підвищувати рівень медіаосвіти серед населення та забезпечувати широкий доступ до об'єктивної та достовірної інформації.

Узагалі, для протидії використанню іноземних ЗМІ Російською Федерацією для дестабілізації ситуації в Україні необхідно вирішувати комплексну проблему, яка передбачає розробку та впровадження ефективно ї інформаційної політики, забезпечення доступу до надійних джерел інформації, підвищення рівня медіаосвіти населення, розвиток національних ЗМІ, залучення фахівців з інформаційної безпеки, забезпечення координації дій між відповідними державними структурами та інші заходи.

Також важливо звернути увагу на міжнародну співпрацю в цьому напрямі. Україна має підтримувати партнерські стосунки з іншими країнами та міжнародними організаціями з метою координації дій із захисту від інформаційної війни та спільної боротьби проти дезінформації та пропаганди.

Українські ЗМІ та організації громадянського суспільства також можуть використовувати свої ресурси для виявлення та розповсюдження об'єктивної та достовірної інформації, а також для розкриття фейків та дезінформації.

Отже, протидія використанню іноземних ЗМІ Російською Федерацією для дестабілізації ситуації в Україні потребує комплексного підходу та співпраці всіх відповідних структур, міжнародної співпраці та підтримки громадськості. Тільки таким чином можна забезпечити інформаційну безпеку та захист національних інтересів.

Андрощук В.В.
студент Національної академії СБ України

СПРОСТУВАННЯ МІФУ ЩО УКРАЇНЦІ Й РОСІЯНИ ОДИН НАРОД

Попри весь трагізм подій 24 лютого 2022 року, вони мали один ключовий

аспект для української і, завдяки глобалізації, світової історії. А саме, відчайдушний спротив українських збройних сил і простих людей відкрив для світу Україну й українців. І хоча зараз нам в це важко віриться, та для більшості світу, й навіть для значної частини європейців до 24 лютого 2022 року, українці й росіяни були одним народом, навіть незважаючи на події 2014 року. Проте ціна, яку досі платить Україна, продемонструвала кардинальні відмінності між росіянами і українцями на всіх ціннісних рівнях.

Та незважаючи, на це, для більшості населення нашого ворога ми все ще «один народ», і таке невизнання українців як окремої самостійної нації ставить з одного боку серйозну загрозу нашій національній безпеці, а з іншого - завдання для українських сил безпеки і оборони довести протилежне.

По-перше, варто зазначити, що саме поширення цього міфу в медіа не дуже корелюється з іншою пропагандою на російських ЗМІ та в заявах їхніх офіційних осіб. Адже судячи з останніх з заяв президента рф він продовжує говорити, що росіяни і українці - один народ, роз'єднаний двома кранами. Проте коли він говорить про війну, він і далі стверджує що «ми не воюємо з народом України» (наприклад, остання його пресконференція), тим самим визнаючи існування українського народу. Такий стан в науці називається амбівалентність – коли люди одночасно вірять у дві взаємовиключні твердження. Якщо ж гіпотетично припустити що росіяни і українці один народ тоді, за такою логікою те що називається в рф «СВО» мало б називатися громадянська війна, оскільки воює «один народ», але так ніхто війну не називає. І в результаті ми отримуємо що, з одного боку, український народ і українці існують коли вони бомблять самі себе, а з іншого - росіяни і українці -це один народ і нам треба об'єднуватися адже «ми прийшли вас рятувати».

Наукове підґрунтя вказаного міфу рф починає ще з історії Київської Русі, мовляв, українці і росіяни від самого початку були одним цілим, а тому ніякої української нації не існує і просто ніколи не існувало.

Проте коли ми говоримо про минуле, варто пам'ятати, що не слід його розглядати з точки зору сучасності. Тобто середньовічну державу Київську Русь не можна порівнювати з Україною чи Росією використовуючи теперішні критерії, адже в ті часи це були окремі племена, вони не мали паспортів, національності і не називали себе українцями чи росіянами.

Про утворення національних держав можна говорити починаючи лише з 19 століття, а як міжнародний термін це поняття утвердилося лише після Першої світової війни. Тому сперечатися про те, чиєю національною державою була Русь, має стільки ж сенсу, як і з'ясовувати, чиєю державою була інша середньовічна імперія – імперія Каролінгів, на протилежному, західному кінці Європейського континенту.

Крім того, зв'язок Київської русі і Московської держави, а потім Російської імперії, СРСР та рф росіянам був необхідний лише для обґрунтування

територіальної експансії на захід і завоювання нових територій. Тому використовувався як інформаційна кампанія під гаслами про «збирання руських земель».

Мова - це ще один аргумент про «один народ», адже українська і російська мови походять від одного джерела, лексично близькі і значна частина українців розмовляє російською. Але якщо говорити з наукової точки зору, до української найближчою є білоруська мова (84 % спільної лексики), потім польська (70 % спільної лексики), словацька (68 % спільної лексики) і тільки потім російська мова (62 % спільної лексики). А те що, багато українців говорять і розуміють російську, пов'язано з значним періодом русифікації і тривалою забороною української мови (славнозвісні Емський указ і Валуєвський циркуляр). Крім того, навіть в коротких періодах коренізації України в СРСР, російська залишалася головною, як мова кар'єрного росту і роботи у державних структурах, тому українці змушені були її використовувати.

Та незважаючи на всі ці негативні тенденції в минулому, повномасштабне вторгнення 2022 року врази пришвидшило процес українізації, тепер більшість російськомовних українців переходять на українську. Також зараз в Україні не стоїть питання української мови, вона без сумніву є державною, а російську як мову кар'єрного росту поступово замінює англійська, як мова міжнародного спілкування у зв'язку з Євроатлантичною інтеграцією України.

Окрім того, що росія просто насаджує і використовує свої псевдо-історичні факти для підтвердження свого міфу та ігнорує інші факти.

Чи не найяскравіший приклад - це Українська революція 1917-1921 років, коли після Першої світової війни українці створили чомусь не російську чи Руську народну республіку, а УНР, і це сталося також і на Заході України з утворенням ЗУНР, без попередньої згоди чи якихось зв'язків між державами під час утворення. Вони використовували як державні атрибути синьо-жовтий прапор, тризуб, гімн «Ще не вмерла Україна» і українську мову (а не триколор, двоголового орла чи російську мову). Що ще раз підтверджує існування двох абсолютно різних народів, зі своїми атрибутами цінностями та культурою. І хоча українська державність в той час не змогла довго протриматися під тиском зовнішніх ворогів і внутрішніх чвар, вона заклала ґрунт і державотворчий досвід в історичну пам'ять українців. Що дозволило в 1991 році здобути незалежність держави Україна, яку, до речі, на міжнародному рівні визнала і російська федерація.

Отже, враховуючи всі зазначені фактори, можна зробити висновок що твердження що росіяни та українці один народ, немає під собою ніякого історичного, і логічного підґрунтя. І всі розумні люди цей міф не сприймають серйозно, проте проблема полягає у тому, що у рф таких людей не багато, і основна маса досі вірить всьому що кажуть у телевізорі. Тому для ефективної інформаційної взаємодії необхідно не тільки спростовувати міфи росіян, а й самим

здійснювати інформаційний вплив на населення рф і нагадувати їм що Крим, до анексії, 23 роки перебував в Україні (а до того майже півстоліття в УРСР), що ніяких народів так званих Л/ДНР ніколи не існувало і так далі здійснювати інформаційно медійні операції на інші болючі точки в режимі на росії.

Література

1. Шпорлюк З. Формування модерних націй: Україна – Росія – Польща. Київ: Дух і Літера, 2013. 552 с.

2. Когут З. Коріння ідентичности. Студії з ранньомодерної та модерної історії України. Київ: Критика, 2004. 351 с.

3. Грицак Я.Й. Подолати минули: глобальні історія України. Київ: Портал, 2022. 416 с.

4. Як російська пропаганда впливає на суспільну думку в Україні // Media Sapiens. 2017. 13 лютого. URL: http://osvita.mediasapiens.ua/mediaprosvita/research/yak_rosiyska_propaganda_vplvae_na_suspilnu_dumku_v_ukraini_doslidzhennya (дата звернення 10.03.2023).

Антонюк А.А.
студент Національної академії СБ України

ЧОМУ ІНФОРМАЦІЯ ПРО ПОТУЖНІСТЬ РОСІЙСЬКОГО ФЛОТУ Є МІФОМ: АНАЛІЗ СУЧАСНОГО СТАНУ

Міф про потужність російського флоту залишається однією з найпоширеніших ідей в міжнародних відносинах, багато держав навіть довгий час спиралися на цей міф у побудові відносин з рф. Однак, часом міфи можуть бути далекі від реальності. Аналіз сучасного стану російського флоту демонструє, що хоча він має свої потужні аспекти, це не означає, що він є непереможним, зокрема:

по-перше, російський флот має значні потужності, які дозволяють йому домінувати у своїй зоні впливу. Проте, його потужності є обмеженими і не дозволяють йому конкурувати зі світовими лідерами в морських війнах та конфліктах. Війна з Україною і втрата флагману Чорноморського флоту крейсера «Москва» цьому показовий приклад;

по-друге, стан російського флоту сьогодні далекий від ідеального. Застарілі кораблі та обмежена кількість сучасних бойових кораблів ускладнюють його здатність до бойових дій;

по-третє, більшість міфів про російський флот є переважною пропагандою, що має на меті підвищити престиж росії на міжнародній арені.

Отже, хоча російський флот має свої потужні аспекти, міф про його непереможність та потужність є лише міфом. Російський флот не може

конкурувати з флотами більш розвинутих країн світу, таких як США та Китай, які мають значно більші бюджети на військову сферу. Згідно з даними Stockholm International Peace Research Institute, росія займає третє місце за розміром військового бюджету у світі, проте ці кошти розподіляються між різними видами зброї, включаючи ядерну. Більшість суден в російському флоті є застарілими і потребують значних витрат на модернізацію.

Також необхідно враховувати те, що сучасні військові конфлікти з використанням високоточних ракет, авіації, та безпілотників, не залишають майже жодних шансів для російського флоту у реальному бою. Тому, розуміючи сучасні реалії, можна стверджувати, що майбутнє у російського флоту надзвичайно туманне і дуже коротке.

Література

1. Global Firepower - 2023 World Military Strength Rankings. *Global Firepower - 2023 World Military Strength Rankings*. URL: https://www.globalfirepower.com (дата звернення 1.03.2023).

2. Stockholm International Peace Research Institute. URL: https://www.sipri.org (дата звернення 1.03.2023).

3. Janes | The trusted source for defence and security intelligence. *Janes.com*. URL: https://www.janes.com/ (дата звернення 1.03.2023).

Апаренков І.В.
Гупало Є.А.
Іванчук П.І.
курсанти першого курсу
Національної академії СБ України
групи НБ-222

АНАЛІЗ НОРМАТИВНИХ ДОКУМЕНТІВ ЩОДО ОРГАНІЗАЦІЇ ЗАХИСТУ WEB-РЕСУРСІВ ВІД НСД В ІКС

Професійна підготовка фахівців з питань управління інформаційною безпекою та технічного захисту інформації потребують інтеграції цілої низки вимог різноманітних нормативних документів з питань захисту інформації, які раніше вважалися самостійними і не пов'язаними між собою.

У зв’язку з цим істотно зростає роль системних знань, необхідних для ефективного використання вимог різних нормативних документів з метою вирішення нових, нестандартних проблем організації захисту інформації з обмеженим доступом.

Тому методологія систематизації, іншими словами - аналізу знань, потребує

розробки нової технології їхньої формалізації та використання в навчальному процесі Академії.

Отже, розробка нових методик та інструментів аналізу (систематизації) знань у тому числі з питань організації захисту інформації з обмеженим доступом є актуальним науковим завданням.

З метою використання в навчальному процесі Академії стосовно підготовки фахівців за напрямом «Організація захисту інформації з обмеженим доступом» запропоновано методика систематизації знань на прикладі аналізу документів НД ТЗІ щодо захисту WEB-ресурсів в інформаційно-комунікаційних системах.

Для проведення аналізу знань використано системний та об'єктно-орієнтований підхід а також матричну модель загальної безпеки.

Розглянуто теоретичні й практичні питання реалізації системного та об'єктно-орієнтованого підходів для вирішення конкретних навчальних завдань щодо захисту WEB-ресурсів в інформаційно-комунікаційних системах на підставі вимог нормативних документів НД ТЗІ.

Запропоновано методичні та практичні рекомендації щодо аналізу та систематизації знань з питань організації захисту інформації з обмеженим доступом.

Література

1. Закон України «Про інформацію».

2. Закон України «Про основні засади забезпечення кібербезпеки України».

3. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу;

4. Домарєв В.В. «Система ситуаційного управління: теорія, методологія, рекомендації» - К. Знання України, 2017. – 347 с.

5. Домарєв В.В., Скворцов С.О. - Організація захисту інформації на об'єктах державної та підприємницької діяльності. – К: Європейський університет, 2006.-165с. Затверджено Міністерством освіти і науки України як підручник для студентів вищих навчальних закладів (лист №14/18-Г-602 від 31.07.2006р.)

6. Браіловський М.М., Головань С.М., Домарєв В.В., Коженевський С.Р. - Технічний захист інформації на об'єктах інформаційної діяльності. – К: ДУІКТ, 2007.-178с. Затверджено Міністерством освіти і науки України як підручник для студентів вищих навчальних закладів (лист №14/18-Г-1476 від 06.09.2007р.).

Бобровська С.А.
студент Національної академії СБ України

АКТУАЛЬНІ ПИТАННЯ МОРАЛЬНО-ПСИХОЛОГІЧНОГО ЗАБЕЗПЕЧЕННЯ В УМОВАХ ЗБРОЙНОЇ АГРЕСІЇ рф ПРОТИ УКРАЇНИ

Триваюча агресія російської федерації проти України, а особливо етап повномасштабного її вторгнення, призвів до суттєвого ускладнення морально-психологічного стану мешканців України, як цивільних, так і військовослужбовців. Так, згідно з інформацією, отриманою Міністерством охорони здоров'я України внаслідок опитування українців у вересні 2022 року, понад 70% наших співгромадян перебувають у стресовому стані – 71% опитаних відчували останнім часом стрес або сильну знервованість, а половина осіб, що взяли участь у цьому дослідженні - тривожність і напруження. Українські психологи також наголошують на наявності таких проблем і підтверджують збільшення звернень за консультаціями, що стосуються тривожних та депресивних станів, неконтрольованої агресії чи навіть суїцидальних думок, що супроводжуються переживанням втрати: близьких, дому, ідентичності [1].

Безумовно, наявність таких проблем серед цивільного населення України лише підтверджує їхню актуальність і для військовослужбовців. У межах ініціативи першої леді Олени Зеленської зі створення Всеукраїнської програми ментального здоров'я було проведено аудит потреб та ресурсів системи надання послуг у сфері психічного здоров'я. За його результатами, стан психічного здоров'я військовослужбовців значно гірший, ніж серед решти населення. Тривожні розлади трапляються серед військових удвічі частіше в порівнянні з рештою населення. Результати дослідження ГО «Безбар'єрність», оприлюднені у 2023 році [2] свідчать, що великий депресивний розлад значно поширеніший серед військових, ніж серед решти населення (4,8 % порівняно з 3,63% відповідно).

Активні бойові дії призводять і до бойового стресу. В умовах активного ведення бойових дій, бойовий стрес як явище є неминучим. Дослідження показують, що в добре підготовлених і згуртованих підрозділах з хорошим командуванням, лише один із десяти бійців страждає від бойового стресу навіть в умовах важких боїв. Інші військовослужбовці, навіть за умови впливу бойового стресу на них, адаптуються до нової реальності. У випадках вдалого подолання бойового стресу військові вдаються до позитивної поведінки в умовах бойових дій, ознаками якої є групова згуртованість, вірність побратимам та командирам, відчуття власної значимості та бачення сенсу у тій меті, що поставлена перед бійцями. В таких підрозділах військовослужбовці схильні до бадьорості і нижчої тривожності, в них спостерігається зростання сили волі, витривалості, терпіння до труднощів, дискомфорту та навіть поранень. Бійці відчувають укріплення віри в себе, свої дії та свою місію у війні, стають хоробрими та жертовними [3, 68-75].

Але для того щоб в умовах сучасної війни справді досягти таких результатів, командири та їхні підлеглі мають розділити тягар, вирішити внутрішні конфлікти, збудувати згуртований підрозділ і зменшити стрес. Такі дії, а також дотримання дисципліни і законів ведення війни, запобігають неправомірній поведінці, спричиненій стресом.

Дослідження показали, які саме ситуації і стресові фактори спричиняють бойову втому. Деякі з них можуть контролюватися хорошим лідером. Інші ситуації чи події проконтролювати не можна, проте знання, які з них збільшують стрес і бойову втому, дозволяють командиру компенсувати їх вплив зменшенням інших факторів стресу і здійсненням корекційної роботи. Командир також повинен мати план забезпечення належної допомоги постраждалим від бойового стресу і враховувати його під час виконання основних завдань.

Окрім наявності цього плану і слідуванню йому, важливим є і дотримання універсальних заходів, які знижують бойовий стрес, а відповідно і бойову втому, та запобігають втратам від них, а також допомагають зменшити девіантну поведінку, спричинену стресом.

До таких «універсальних заходів» першочергово належить чітке декларування стандартів поведінки. Командир має наголошувати, що сили оборони повинні неухильно дотримуватись закону та кожного разу підкреслювати ці стандарти, особливо коли вони порушуються супротивником, або при перших ознаках порушень нашими військами. Деякі ранні ознаки можуть включати в себе розмови про порушення закону, власну їх інтерпретацію чи порушення закону в зоні активних бойових дій, де такі правопорушення не можуть бути задокументованими. В певних випадках корисно підкреслювати національну, військову гордість і гордість підрозділу за те, що наші військові слідують стандартам навіть при провокаційних умовах, регулярно пояснювати етичні, правові, практичні та тактичні причини, чому ми слідуємо встановленим правилам. Окрім розмов, варто дотримуватися встановлених порад і на практиці: сам командир має встановити особистий приклад правильної поведінки, повідомляти про всі порушення та передавати всіх перевірених порушників у відповідні інстанції, та безумовно, карати проступки і порушення військових в мирний час, щоб встановити стандарт того, що негідна поведінка не допускається [4].

Окремо слід звернути увагу на те, що в українських збройних силах на 400-500 військовослужбовців працює один психолог, а українські нормативно-правові акти встановлюють, що допустиме навантаження на офіцера-психолога може бути не більше 7 осіб на день, що звертаються за психологічною консультацією та реабілітацією та не більше 4 осіб, що звертаються із серйозними розладами. У той же час, в армії, наприклад, Ізраїлю, один психолог відповідальний за 70-90 військовослужбовців. [2] І це при тому, що наразі Ізраїль не веде масштабних воєнних дій, що були би співставні за інтенсивністю з бойовими діями, що

відбуваються на території України. Крім того, методологічні рекомендації та посібники щодо морально-психологічного забезпечення військовослужбовців [5] [6], випущені Міністерством оборони та Генеральним штабом переважно у 2014-2016 роках, коли умови ведення бойових дій та роботи військових психологів суттєво відрізнялись від нинішніх. Це зумовлює необхідність оновити наявні рекомендації, а також збільшити чисельність комплектування військовими психологами військових частин.

Виконання наведених рекомендацій призведе до суттєвого підвищення морально-психологічного стану серед військовослужбовців, а відповідно полегшить адаптацію останніх до нових умов, нівелюватиме схильність до дисфункціональної поведінки.

Література

1. Результати соціологічного дослідження «Психічне здоров'я та ставлення українців до психологічної допомоги під час війни» проведеного у вересня 2022 р. соціологічною службою «Gradus research company» на замовлення Міністерства охорони здоров'я України. 2022. URL: https://gradus.app/documents/308/Gradus_Research___Mental_Health_Report_short_version.pdf (дата звернення: 09.03.2023).
2. Медведенко Л. Стан психічного здоров'я військовослужбовців значно гірший, ніж серед решти населення. 2023. URL: https://armyinform.com.ua/2023/02/28/stan-psyhichnogo-zdorovya-vijskovosluzhbovcziv-znachno-girshyj-nizh-sered-reshty-naselennya/ (дата звернення: 09.03.2023).
3. Білошицький В.І., Гангал А.В., Стукан С.О., Бех С.М. Морально-психологічне забезпечення у Збройних Силах України: навчально-методичий посібник. 2-ге видання, доповнене і перероблене. Київ: НТУУ "КПІ імені Ігоря Сікорського", 2020. 138 с.
4. А. О. Кобзар, В. Т. Марценківський, П. М. Слюсаренко та ін. Морально-психологічне забезпечення підрозділів Збройних Сил України: підручник. Київ.: НУОУ ім. Івана Черняховського, 2018. 404.
5. Алгоритм роботи військового психолога щодо психологічного забезпечення професійної діяльності особового складу Збройних Сил України (методичні рекомендації) / Міністерство оборони України, Наук.- дослід. центр гуманітар. проблем Збройних Сил України: Н.А. Агаєв, О.Г. Скрипкін, А.Б. Дейко, В.В. Поливанюк, О.В. Еверт. – Київ: НДЦ ГП ЗС України, 2016. 147 с.
6. Формування психологічної готовності військовослужбовців до виконання завдань антитерористичної операції (порадник для офіцерів та сержантів) / Штаб антитерористичної операції в Донецькій та Луганській областях, відділ по роботі з особовим складом, 2014. 22 с.

Балдич А.В.
студентка групи Н-223мз ННІ ІБ СК НА СБ України
Науковий керівник:
Жевелєва І.С.
к.ю.н., доцент
доцент кафедри ОЗІОД ННІ ІБ СК НА СБ України

ЕВОЛЮЦІЯ РОСІЙСЬКИХ ПРОПАГАНДИСТСЬКИХ НАРАТИВІВ У ЛЮТОМУ-ЖОВТНІ 2022 РОКУ

Пропаганда стала важливим методом ведення інформаційної війни, який широко використовується для підтримки воєнних операцій. За своїм значенням пропаганда – це спосіб поширення потрібної інформації для впливу на суспільну думку з метою подальшого маніпулювання свідомістю населення [1]. На сьогодні фундаментальну залежність всіх сфер життєдіяльності від пропаганди можна прослідкувати в політиці провідних країн світу [2, с. 69]. За видами пропаганда поділяється на білу, сіру та чорну [3], де чорна – це пряме спотворення реальності. Прямим прикладом чорної пропаганди є інформаційний потік російської федерації в ході повномасштабного вторгнення російських військ на територію України.

Це підтверджується тим, що новини, думки політичної еліти Кремля, судження політологів та військових аналітиків стали діяти з новою силою, збільшуючи донесення завідома неправдивої інформації до цільової аудиторії за допомогою інших методів, які підкріплювались старими наративами. Основний прикладом, задля підтвердження судження можна виділити суспільно-політичне ток-шоу «60 хвилин» з Ольгою Скабєєвою та Євгенієм Поповим.

Повертаючись до вищесказаного, тематика лютневої пропаганди не являється її початком, тому і у програмі «60 хвилин» вона має своє продовження, адже і до цього моменту там велося щоденне обговорення українських та західних подій. Натомість, після 24 лютого їх пропаганда стала діяти за жорстокішими методами, які передбачають абсолютне спотворення ситуацій для створення більшого резонансу серед глядачів, викликаючи при цьому підтримку дій влади, що спровоковано страхом, шоковим станом та неможливістю перевірення достовірності інформації. Іншими методами стали: уособлення російських збройних сил з непереможними римськими воїнами; багаторазовість повторення інформації (метод Геббельса) [3]. Поєднання цих методів дозволило російським пропагандистам поширити теми, які стали гаслами війни в Україні для їх глядачів: **денацифікація та демілітаризація України, геноцид російськомовного населення з боку української влади, захист власної державності, звільнення території від «нацистів» та «бандерівців»** та інші [4].

Окрім цього, варто звернути увагу на те, що їх пропагандистські помисли діють не лише на громадян росії, але й на значну частину закордонної аудиторії.

Це зумовлено насамперед тим, що їх засоби та методи донесення інформації свідчить про сильний вплив на свідомість людей шляхом викривлення, перекручування фактів, повністю знебарвленням чи навпаки додаванням яскравості в певні тематичні новини [5], маніпулюючи не лише на зміну уявлення про українців та Україну, але й провокуючи на дії, які несуть в собі негативний вплив на світове бачення ситуації. Правильно підібраний шлях донесення дезінформації до міжнародної аудиторії дозволив отримати значну підтримку угорських, сербських, німецьких та інших народів [5]. Не без уваги залишається факт використання політичними лідерами європейських країн постулатів російських ток-шоу. Зокрема, президент Франції Е. Макрон висловився в одному із звернень про «братські народи», що може говорити про дієву пропагандистську риторику російських ЗМІ на закордонних глядачів.

Не дивлячись на те, що ґрунт російської пропаганди формувався 8 років, вони зуміли від 24 лютого видати нові теми для обговорення. Першим таким наративом виявилось те, що росія не мала іншого виходу, як почути «**прохання жителів Донбасу про допомогу через постійні обстріли з градів та загрозу їхньому життю»** [4]. Це стало одним із офіційних заяв кремлівської влади, які були озвучені і в «60 хвилин». Окрім цього, наратив, який, так само як і інші, розвіявся з першими тижнями війни був про «**слабкість української армії, про їхню масову здачу в полон та про великі втрати складу».** Всі ці слова постійно підтримувались реплікою, що населення України робить вибір самостійно, де та в складі якої країни перебувати.

Початковими наративами також виступали «**створення в Україні за допомогою НАТО та Америки біолабораторій та ядерної зброї»**, що стає прямою загрозою існуванню держави росії. Не дивлячись на те, що росіяни і самі щиро вірять в свою пропаганду, вони намагаються себе нею ще й заспокоїти, адже з самого початку ще одним пропагандистським наративом виступає **порівняння Зеленського з Саакашвілі та «безпорадність»**, яка їх пов'язує. Така «безпорадність» визначається не тільки заявами про втечу Зеленського в Польщу, але й «**відмовами західних країн в підтримці України».**

Останнім з яскравих початкових наративів, введеним в життя пропагандистами, став лозунг **«все йде за планом»** [4], він використовується і по нині, як захисна реакція на відведення військ з Київського, Харківського та Херсонського напрямків. Хоча після кожного такого відступу аргументів по такому відходу в них стає дедалі менше.

Наступним етапом пропагандистських наративів в ток-шоу «60 хвилин» є збільшення екранного часу для обговорення, нібито **постачання російської нафти** США та країнам Європи [4]. Це дало можливість підкормлювати публіку вигадками про безвихідне становище НАТО та швидкої відмови їх в допомозі українській владі. Окрім цієї тематики все частіше з'являються розмови про

«дружній Китай» та «**створення власного альянсу»**, до якого входитимуть росія, Китай, Іран, Аргентина та Туреччина.

Без уваги російських пропагандистів не залишилась і події на фронті, де ключовими тезами стали заяви про слабкість української армії, **масову мобілізацію до української армії** не тільки цивільних, але й ув'язнених, які без військової підготовки відправляються на передову, як «гарматне м'ясо» [4]. Окрім цього все частіше лунають теми про «**іноземних найманців»**, які воюють на стороні українців. Пропаганда виправдовує відступи російських військ зі своїх позицій тим, що вони «**не можуть воювати проти 50 країн»**. Також частим є наратив, що, нібито, **війну росія веде не з Україною, а з НАТО** [4].

Змін зазнала і риторика щодо **бажаного обсягу території України**, яку росія планує «звільнити». Якщо раніше в їх плани входили території лівобережжя до річки Дніпро, то зараз, за словами російських «військових аналітиків», які є частими гостями в пропагандистських програмах, варто брати під контроль всю територію України, оскільки залишена частина території завжди буде загрозою для так званої «великої держави» [4].

Ще одним напрямком пропаганди, яку поширюють Скабєєва та Попов, є **ядерна зброя** та **вибори в парламент Вашингтону**. Пропагандисти та кремлівська влада сподіваються на нейтральну позицію США щодо ситуації в Україні після можливої зміни президента та уряду на чергових виборах та припинення поставок зброї.

Отже, сучасні російські пропагандистські наративи є продовженням старої кампанії, яка була заснована на твердженнях про «нацистів» та «бандерівців» на території України, та висвітлення негативного відношення до країн Європи та США. Характерною особливістю російської пропаганди є те, що одні пропагандистські наративи продовжують інші, заповнюють весь інформаційний простір і відволікають увагу суспільства від важливих тем та реальної оцінки ситуації. Як наслідок, через відсутність інформаційної гігієни, пострадянський менталітет, низький рівень освіченості, велика кількість цільової аудиторії починає вірити в пропагандистські тези.

Література

1. Ознаки та методи пропаганди. Ілларіон Павлюк. *Освітня асамблея*. URL: https://www.ea.org.ua/2016/11/16/propaganda-pavliuk/ (дата звернення: 18.03.2023).

2. Жевелєва І.С. Пропаганда як загроза інформаційній безпеці суспільства. *Information Security of the Person, Society and State*, 2011. № 2. С. 69–75.

3. 8 методів пропаганди: як люди перетворюються на зомбі. *Газета "Закон і Бізнес". Законодавство, влада, права людини*. URL: https://zib.com.ua/ua/151037.html (дата звернення: 18.03.2023).

4. 60 минут. URL: https://smotrim.ru/ (дата звернення: 18.03.2023).
5. Бєлкін Л. та ін. Контрпропаганда vs пропаганда в умовах широкомасштабного збройного вторгнення Російської Федерації в Україну. *Юридичний науковий електронний журнал,* 2022. № 6. URL: http://www.lsej.org.ua/6_2022/52.pdf (дата звернення: 19.03.2023).

Богданович І.О.
курсант
Національної академії СБ України
Головко О.Я.
старший викладач
кафедри романо-германських мов
Національної академії СБ України

DIRECTIONS OF STATE INFORMATION SECURITY DEVELOPMENT

Introduction. Protecting its information interests, each state must take care of its information security. The strengthening of Ukrainian statehood also requires the same. A balanced state information policy of Ukraine is formed as an integral part of its socio-economic policy, based on the priority of national interests and threats to the country's national security. From a legal point of view, it is based on the principles of a legal democratic state and is implemented through the development and implementation of relevant national doctrines, strategies, concepts and programs in accordance with current legislation.

Conducting a successful information policy can significantly affect the resolution of domestic, foreign, and military conflicts. Information security is one of the essential components of the country's national security, its provision thanks to the consistent implementation of a well-formulated national information strategy would greatly contribute to ensuring success in solving tasks in political, social, economic and other spheres of state activity.

Modern scientists such as I. Aristova, G. Pocheptsov, and others are engaged in the study of ways of forming the information security of society. A number of publicists, V. Suprun, V. Yarochkin, developed the basic principles of ensuring information security. At the same time, structural and functional aspects of the process of guaranteeing information security require a separate study [1, с. 123-126].

The purpose of the study is to identify and analyze the main directions of the state information policy in order to protect the national information space and guarantee information security.

Firstly, we consider it necessary to analyze the term "state information policy". In this connection, we will try to define the meaning of the concept of "politics". We

believe that this term should be considered as a set of mutually agreed and mutually determined concrete conceptual ideas, built taking into account the interests and needs of citizens, society and the state in a certain sphere of life. It should be emphasized that politics can differ in its objects, subjects, goals and means. So, for example, the object of information policy is the national information sphere with all its components. As for the state information policy, as M. Ivanchenko notes, it should be understood as a set of main directions and methods of the state's activity in obtaining, using, distributing and storing information.

It is necessary to pay attention to the opinion of I.R. Berezovska, who, analyzing the concept of "state information policy", indicates that such a policy should lay the foundations for solving the fundamental tasks of the development of society, the main of which is the formation of a unified information space of Ukraine and its entry into the world information space, guaranteeing information security of the individual, society and the state [5, c. 181-195].

The main information threat to national security is the threat of another party's influence on the country's information infrastructure, information resources, society, consciousness, subconsciousness of the individual, with the aim of imposing on the state a desired (for the other party) system of values, views, interests and decisions in vitally important spheres of social and state activity, to manage their behavior and development in the desired direction for the other party. Actually, this is a threat to the sovereignty of Ukraine in vital spheres of public and state activity, which is implemented at the informational level.

Strategic information confrontation is an independent and fundamentally new type of confrontation capable of resolving a conflict without the use of armed forces in the traditional sense.

State information policy should reflect urgent issues that have arisen in the international sphere and the sphere of information security, etc. It is necessary to ensure legislative protection of the rights and interests of all subjects of information relations [3].

Studying the works of modern scientists, analyzing the articles of students, we can conclude that the main emphasis of the state information policy, in their opinion, should be based on ensuring the right to reliable, complete and timely information, freedom of speech and information activity, prevention of interference in the content and internal organization of information processes, except cases determined by legislation in accordance with the Constitution of Ukraine; preservation and improvement of the domestic national information product and technologies, provision of information and national-cultural identification of Ukraine in the world information space; guaranteeing state support and development of resources for scientific and technical products and information technologies.

As for the priority directions of the state information policy, the Law of Ukraine "On Information" includes the following among them:

- ensuring everyone's access to information;
- ensuring equal opportunities to create, collect, receive, store, use, distribute, protect, and protect information;
- creating conditions for the formation of an information society in Ukraine;
- ensuring the openness and transparency of the activities of subjects of power;
- creation of information systems and information networks, development of electronic governance;
- constant updating, enrichment and storage of national information resources;
- ensuring information security of Ukraine;
- promoting international cooperation in the information sphere and Ukraine's entry into the global information space [3].

Attention should also be paid to the position of M. Ivanchenko, who, considering the issue of directions of the state information policy, proposes to single out the following main directions: ensuring citizens' access to information; creation of national information systems and networks; strengthening the material, technical, financial, organizational, legal and scientific foundations of information activities; ensuring effective use of information; promotion of constant updating, enrichment and preservation of national information resources; creation of a general information protection system; promoting international cooperation in the field of information and guaranteeing the information sovereignty of Ukraine; assistance in meeting the informational needs of Ukrainians abroad [2, c. 113-117].

Conclusion. Therefore, given that the state information policy is aimed at protecting the information environment from information and communication challenges and threats, ensuring information security in this sense is an extremely important element of the country's national security. That is why, maximum attention should be focused on strengthening the participation of state authorities in eliminating problems related to the informatization of society and ensuring proper integration of the Ukrainian information space into the European one.

Література

1. Безштанько В. Цикл впровадження системи управління інформаційною безпекою. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2006. Вип. 2 (13). С. 123–126.

2. Гбур З. В. Методи та принципи державного управління економічною безпекою. Інвестиції: практика та досвід. 2017. № 24, груд. С. 113–117.

3. Чубаєвський В. Методи управління корпоративною інформаційною безпекою. Економіка та суспільство. 2022. № 43. URL: https://doi.org/10.32782/2524-0072/2022-43-49 -(дата звернення: 17.03.2023).

4. About information. The official website of the Parliament of Ukraine. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (date of application: 03/17/2023).

5. Berezovska I. Unlawful use of personal data contained in social media as a threat to informational and national security of ukraine. Visnyk of the lviv university. series law. 2014. № 60. С. 185–191. URL: https://doi.org/10.30970/vla.2014.60.288 (дата звернення: 17.03.2023).

Бондаренко С.Ю.
студент групи П-211
ННІ ІБ СК НА СБ України

СПОСОБИ ГЛОБАЛЬНОЇ ДЕЗІНФОРМАЦІЇ ЯК ПРОВІДНА ЗАГРОЗА, ВИЗНАЧЕНА В СТРАТЕГІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Після прийняття рішення РНБО України від 29 грудня 2016 року «Про Доктрину (далі – Доктрина) інформаційної безпеки України» (Указ Президента України від 25 лютого 2017 року № 47/2017) була прийнята доволі довгоочікувана для всього українського суспільства Стратегія інформаційної безпеки (далі – Стратегія), яка була введена в дію Указом Президента України від 28 грудня 2021 року № 685/2021 [1,2].

На відміну від доктрини як документа, що має не лише законодавчим способом, а й філософо-культурним підґрунтям уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу російської федерації в умовах розв'язаної нею гібридної війни (тобто напрямки, цілі, мета, опис ситуацій, що склалися), стратегія як документ, що визначає актуальні виклики та загрози національній безпеці України в інформаційній сфері, а також стратегічні цілі та завдання, спрямовані на протидію таким загрозам, захист прав осіб на інформацію та захист персональних даних (тобто вже чіткі практичні кроки, шляхи та способи вирішення проблемних питань, які були зазначені у доктрині).

У загальних положеннях Стратегії окреслено аналіз кола загроз та викликів інформаційній безпеці, серед яких міститься (відразу перша, що свідчить про одну з найбільш небезпечних) збільшення кількості глобальних дезінформаційних кампаній.

Законодавець трактує так це явище: «Глобальні дезінформаційні кампанії, що інспіруються авторитарними урядами та активістами радикальних рухів для маніпулювання свідомістю окремих людей та груп населення, стали повсякденною практикою, яка загрожує демократичному розвитку держав та міжнародній стабільності» [2]. Треба бути дуже сильно проросійською людиною, колаборантом (відповідальність за ст.111-1 КК України), пособником держави-агресору (відповідальність за ст.111-2 КК України), зрадником своєї Батьківщини (відповідальність за ст. ст.111 КК України), чи особистістю з політичною

інфантильністю аби не сприйняти таке твердження як, на жаль, реалії сучасності всього українського (і не тільки) суспільства. На нашу думку, зростання масштабів дезінформації – симптом «глобальних проблем», що підривають суспільну довіру.

Із розвитком технологій у сфері масової комунікації Україна і світ постають перед новими викликами. Одним із найскладніших і найпідступніших сьогодні є дезінформація. Бо чи не несе загрози отримана мільйонами людей «новина» про «розп'ятого хлопчика» на Донбасі, про армію дресированих гусей, бджіл, кіз, про безпечність чи взагалі відсутність коронавірусу, про те, що конкурент на виборах — наркоман, алкозалежний тощо? Дезінформація виникає в умовах політичного розчарування, економічної нерівності чи соціальних заворушень. Дезінформація процвітає, коли громадянське суспільство, журналісти, правозахисники та вчені не можуть вільно працювати, збиратися та говорити. Коли дезінформацію підживлюють чиновники (як у нашому випадку – російська пропагандистська система (у тому числі й «влада», нібито «незалежні ЗМІ» тощо)), вона може призвести до злочинів на ґрунті ненависті та насильства.

Ті представники влади, які вдаються до дезінформації, щоб заглушити неугодні висловлювання або залякування і переслідування критично налаштованих осіб, повинні бути притягнуті до відповідальності.

Поговоримо про найбільш відомі способи дезінформування. Серед форм поширення дезінформації можна виділити текстову, відеоконтент, аудіальний контент, а серед способів — координована неавтентична поведінка, таргетинг, діпфейки тощо.

Дезінформація у формі тексту найпростіша у створенні, адже написати і поширити текст може практично кожен. Не потрібно фахових навичок монтажу, дизайну, щоб створити маніпулятивне текстове повідомлення. Більшість публікацій у Facebook, Telegram, на сайтах інтернет-видань, у друкованих матеріалах є текстовими.

Відеоконтент також набув набагато простіших форм, ніж раніше. Якщо колись відео потребувало вираження виключно на телебаченні чи в кінотеатрах, що вимагало часу і витрат на його створення, то зараз відеоблогінг на найпростішому рівні цього не потребує: достатньо мати смартфон та доступ до інтернету.

Звісно, з поширенням конкуренції на ринку відеоконтенту, блогери теж значно більше вкладають у свій продукт для залучення більшої кількості користувачів. Водночас, навіть найпростіші відеоблоги можуть стати популярними і небезпечними в контексті дезінформації. Яскравим прикладом цьому є пропагандист Анатолій Шарій, який почав із звичайного знімання своїх висловлювань на суспільно-політичні теми, а зараз має доволі широку аудиторію, політичну партію і ймовірне фінансування проросійськими політичними силами.

Одним із поширених способів поширення дезінформації є координована неавтентична поведінка. Як повідомляється у звіті Facebook, такий спосіб

використовується для створення маніпуляцій навколо важливих для громадськості тем. Цей спосіб полягає у створенні багатьох фейкових акаунтів (часто під прикриттям медіа чи іншої публічної сторінки), які залучають якомога більше користувачів і в однаковий період поширюють однакові тези, посилаючись один на одне чи на однакове джерело. Найчастіше це нібито сенсаційна інформація або ж чийсь коментар, поданий під гучним заголовком. Мета такої діяльності — створити для читачів усіх цих фейкових акаунтів інформаційну завісу, в якій вони читають тільки те, що треба авторам дезінформаційних повідомлень, а інформація з інших джерел туди не потрапляє.

До прикладу, у травні цього року Facebook зафіксував координовану неавтентичну поведінку десятків сторінок, пов'язаних із наближеним до президента Росії бізнесменом Євгеном Прігожиним. Вони поширювали інформацію про те, що у Судані блокують гуманітарні поставки з Росії, організовані самим Прігожиним. Таким чином, усі ці сторінки працювали на створення позитивного іміджу Росії і дискредитацію невигідних для Росії сил у Судані. Варто зазначити, що Прігожин вже давно курує інтереси Росії в африканських країнах. Для цього він використовує, зокрема, так звану "фабрику тролів", тобто сотні акаунтів, які розповсюджували фейки, розпалювали ворожнечу і маніпулювали суспільною думкою.

Проте мало хто знає, що це доволі не повний набір (далеко не повний) засобі для дезінформування. Неперевірена чи навмисно хибна інформація, опублікована у засобах масової інформації з корисливою чи іншою метою, часто називається «газетною качкою». Це досить інтернаціональний вислів: у більшості мов брехливу інформацію в ЗМІ називають «газетною качкою». Вираз «газетна качка» виник у XVII столітті в Німеччині. На таких матеріалах, які являли собою журналістську вигадку, тогочасні газетярі ставили позначку «NT» (non testaur — не перевірено, що на слух сприймалося як «енте», що німецькою означає «качка»).

Прикладом такої інформації можемо назвати те, що у 1986 році, у Парижі, у газеті Le Parisien йшлося про демонтаж Ейфелевої вежі, яку перевезуть у Діснейленд, що будується, і зберуть заново. Таке рішення уряд пояснював зручністю розташування для будівництва нового стадіону майбутньої Олімпіади 1992 року. Реакція була негайною. Парижани зітхнули з полегшенням, коли дізналися, що це лише розіграш.

Недостовірне або хибне твердження (неперевірене або свідомо невірне), яке наділяється в форму достовірного та видається за достовірне; опубліковане офіційне повідомлення, яке приймається за істину як результат самого факту появи його у пресі; інформація, публікація, недостойна довіра, або подія сумнівної істинності, що сприймається повсюдно за правду називається фактоїд.

Дезінформація залишається одним із важливих викликів, який постає перед державами, громадянським суспільством та населенням країн (як менш розвинених, так і високорозвинених). Огляд прикладів дезінформації підтверджує,

що її вплив не можна переоцінити: вона відображається на суспільній думці, виборах, безпеці держави і людей, здоров'ї та житті, кар'єрі тощо.

Розвиток інформаційних технологій хоч і дає нові можливості у розвитку державного управління, інформування населення, залученості громадян у розбудову держави, проте підвищує ризики дезінформації. За допомогою алгоритмічних систем і штучного інтелекту фейки можуть бути більш переконливими і призначатися саме для тої аудиторії яка має більшу ймовірність повірити в них.

У зв'язку з цим світова спільнота намагається розробити нові політики і рекомендації щодо протидії дезінформації, але при цьому не порушити право на вільне вираження поглядів. Для ефективної протидії дезінформації в Україні необхідне вдосконалення законодавства, виконання європейських рекомендацій щодо підвищення медіаграмотності, розвиток інституцій у сфері боротьби з дезінформацією. При цьому і міжнародні практики не можуть стояти на місці, адже технології змінюються. В ідеалі нові політики мають ставати передбаченням і запобіжником небезпек, проте зараз вони є скоріше реакцією.

Література

1. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки" : Указ Президента України; Стратегія від 28.12.2021 № 685/2021 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/685/2021 (дата звернення: 15.03.2023)

2. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України; Доктрина від 25.02.2017 № 47/2017 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/47/2017 (дата звернення: 15.03.2023)

Войтович А.О.
здобувач вищої освіти
Навчально-наукового гуманітарного інституту
Національна академія Служби безпеки України, Україна

НАПРЯМИ РОЗВИТКУ КОМУНІКАЦІЙ У КОЗАЦЬКОМУ СЕРЕДОВИЩІ

Під козацьким середовищем ми зазвичай розуміємо соціокультурну спадщину та традиції, пов'язані зі становленням та існуванням козацтва в Україні від XVI до XVIII століття. Козацьке середовище характеризується певними

цінностями, які стали основою для формування козацької ідентичності, такими як свобода, гідність, мужність, чесність, справедливість та інші.

У козацькому середовищі відбувалися різноманітні події та явища, які допомогли сформувати культурну спадщину, пов'язану зі степовою культурою та воєнними традиціями. До таких подій можна віднести заснування козацьких військ, битви та походи козаків, побутові традиції козацького суспільства, козацьку поезію та інші аспекти козацького життя та культури.

У сучасному контексті козацьке середовище може розглядатися як частина національної ідентичності України та символ національного героїзму та патріотизму. Також козацьке середовище може бути розглянуто як частина культурної спадщини та туристичної атракції для відвідувачів.

Вивчення козацького середовища з точки зору сучасності є важливим з кількох причин.

По-перше, знання про козацьке середовище допомагає збагатити культурний та історичний багаж нації.

По-друге, козацьке середовище може слугувати прикладом мужності, гідності та патріотизму для сучасного суспільства. Україна проходить складний період в своїй історії, тому вивчення історії козацтва та його цінностей може допомогти сформувати позитивні національні ідеали та розуміння важливості самостійності та свободи.

По-третє, вивчення козацького середовища може мати практичне застосування у сучасному житті. Наприклад, козацькі традиції та цінності можуть бути використані для формування позитивної робочої атмосфери та зміцнення взаємин у колективі.

Козацьке середовище було дуже специфічним і вимагало від козаків високого рівня комунікативних навичок для ефективної взаємодії з іншими людьми. На думку фахівців, однією з найбільш поширених форм комунікації в козацькому середовищі було листування. Це пояснюється тим, що козаки жили на великих територіях, і зустрічалися рідко, тому листування було найзручнішим способом зв'язку між ними. Козаки використовували листи як засіб для передачі повідомлень та інформації між собою та з іншими важливими особами [1].

Ще однією важливою формою комунікації були духовні наради або сходи (збори, які проводилися з метою вирішення релігійних, моральних, культурних, соціальних та політичних питань, що стосувалися життя козацької громади). Ці збори дозволяли козакам ділитися інформацією, приймати рішення та координувати свої дії [2].

Також можна виділити деякі конкретні комунікативні технології, які були особливо ефективними в козацькому середовищі. Перш за все, це було усне спілкування. Козаки досить часто збиралися в групи, щоб обговорювати плани, домовлятися про спільні дії, робити важливі оголошення тощо. Усне спілкування дозволяло швидко і ефективно обмінюватися інформацією [4].

Другим ефективним комунікативним засобом було використання посланців або кур'єрів. Це було ефективним в козацькому середовищі не тільки під час війни, а й у мирний час. Посланці відігравали важливу роль у комунікації між різними козацькими військами та громадами. Вони передавали повідомлення, інформацію про рішення нарад, про зустрічі та переговори. Також, вони були залучені до посередницької діяльності, наприклад, при укладанні договорів між козацькими військами або при вирішенні конфліктів.

У часи війн, посланці були особливо важливими, оскільки вони передавали важливу інформацію про рух військ супротивника, про його плани та наміри. Вони також виконували завдання з забезпечення зв'язку між військовими підрозділами та допомагали у виконанні розвідувальних завдань. Козаки часто використовували цей метод для передачі важливих повідомлень або документів, особливо коли це потребувалося зробити на великі відстані [3].

Третім ефективним комунікативним засобом була військова сигналізація, така як вогні, димові сигнали, тривоги тощо. Цей метод дозволяв швидко повідомляти про початок або закінчення бою, наступ або відступ військ, зустріч зі своїми військами, надання допомоги [5].

Крім цього, важливим було використання символіки та інших знаків, які мали спеціальний зміст для козаків. Наприклад, різні кольори, герби, прапори, хрести тощо використовувалися для ідентифікації козацьких загонів або для позначення важливих подій. Прапор з чорним орлом на золотому тлі став символом козацької Січі та був використаний на багатьох бойових стягах козацьких полків. Такі символи мали не лише декоративну функцію, але й сприяли формуванню ідентичності козацького народу та укріпленню внутрішньої єдності.

Ще одним важливим комунікаційним засобом була література, яка мала свої особливості та відображала історію та культуру козацтва. Такі літописи, як «Історія Русів», літописи Величка і Граб’янки були важливими джерелами інформації про козацтво, його традиції та історію. У козацькому літописі «Історія Русів» є багато записів про князівство Київське та його військо, а також про козацькі загони, які приймали участь у багатьох війнах того часу. Літописи Велички та Граб'янки детально описують життя козаків та події, пов'язані з війнами, які вони вели проти Туреччини, Польщі та Московської держави.

З урахуванням зазначеного, козацьке середовище було дуже різноманітним і складним, але в основному комунікативні засоби були спрямовані на такі цільові аудиторії:

1. Козаки. Комунікативні засоби мали за мету підвищити їхню військову дисципліну, виховувати любов до Батьківщини, інформувати їх про важливі події та підтримувати їхній дух бойового братерства.

2. Жителі сусідніх земель та народностей, тобто на іноземців або тих, хто не належав до козацької спільноти. Козаки спілкувалися з ними для вирішення питань торгівлі, дипломатії, воєнних дій та інших справ.
3. Запорозька Січ, тобто на козацьку спільноту, яка об'єднувала козаків в певних територіальних межах. На Запорозькій Січі комунікативні засоби використовувалися для координації дій козаків, обговорення важливих питань спільноти, прийняття рішень та вирішення конфліктів. На Запорозькій Січі використовувалися різноманітні жанри народної творчості, такі як пісні, оповіді, легенди, що передавали козацьку історію та культуру. Також на Січі були свої власні символіки, яка також використовувалась як комунікативний засіб для ідентифікації козаків та їхньої спільноти.

Козацькі комунікативні засоби мали на меті підвищити патріотичні почуття та національну свідомість у козаків. Для досягнення цієї мети використовувалися різноманітні засоби, такі як літературні твори, публічні виступи, музика, обряди та інші культурні інструменти. Також велика увага приділялася вихованню в козаків моральних та етичних цінностей, таких як чесність, відвага, відданість Батьківщині та інших козацьких ідеалів.

Засоби комунікації, спрямовані на жителів сусідніх земель, зазвичай були побудовані на основі пропаганди козацьких ідеалів та досягнень. Козаки намагалися відображати своє суспільство як приклад для наслідування та демонструвати свої досягнення в боротьбі за волю та незалежність.

Комунікативні засоби, спрямовані на запорізьку Січ, зазвичай мали за мету укріпити внутрішню єдність козацького середовища та підвищити його вплив на сусідні землі та держави.

Отже, комунікативні технології в козацькому середовищі були досить ефективними, забезпечували необхідний рівень взаємодії та співпраці між козаками та цільовими аудиторіями. Однак, важливо зазначити, що в той час комунікативні технології були значно менш розвиненими, ніж сьогодні, тому в деяких ситуаціях комунікація могла бути неефективною. Також козацьке середовище було досить розкиданим територіально, і козаки жили в досить важких умовах. Цей чинник ускладнював комунікацію та обмін інформацією. Загалом, визначені комунікативні технології у козацькому середовищі відповідали історичним реаліям того часу та забезпечували необхідний рівень взаємодії та співпраці між козаками з метою досягнення різних цілей, таких як захист території, управління спільнотою та взаємодія з іншими народами та державами.

Література

1. Гаврилюк М. Козацьке листування як джерело інформації про життя та діяльність козаків // Козацтво і сучасність, 2017. С. 18-22.

2. Єрмоленко В. Козацькі збори та наради: суспільно-політична та культурна спадщина // Наукові записки Інституту історії України, 2016. Т. 34. С. 42-52.

3. Карпов В. Козацькі кур'єри: роль і місце в армії // Вісник Харківського національного університету імені В. Н. Каразіна. Серія "Історія", 2013. Вип. 52. С. 43-47.

4. Мірошниченко В. В. Козацьке усне мовлення як джерело культури// Наукові записки. Серія: Філологічні науки, 2011. Т. 116, Вип. 1. С. 121-124.

5. Шмульків О. Військова сигналізація козацької доби // Історія науки і техніки, 2011. Т. 2, № 2. С. 32-38.

Глобенко С.В.
аспірант кафедри державного управління у сфері цивільного захисту
Інституту державного управління та наукових досліджень з цивільного захисту

ЄВРОПЕЙСЬКИЙ КОНЦЕПТ ПРОТИДІЇ ДЕЗІНФОРМАЦІЙНИМ ПРОЯВАМ У ДЕРЖАВНОМУ ІНФОРМАЦІЙНОМУ ПРОСТОРІ

Сьогодні сфера інформаційної діяльності й захисту інформаційного простору держави загалом, а також в умовах загрози чи виникнення надзвичайних і кризових явищ зокрема набуває особливої ваги, адже інформаційні чинники в публічному управлінні на шляху до забезпечення сталості розвитку держав світу характеризуються значним як консолідуючим, так і дестабілізуючим потенціалом. Недооцінювання чи нехтування ними може призвести до непоправних втрат – ресурсних, іміджевих, репутаційних тощо.

Розуміючи важливість і складність порушених питань, держави світу намагаються віднаходити дієві інструменти й вживати ефективних заходів задля забезпечення захисту власного інформаційного простору.

Зокрема, Європейська комісія [1, с. 7–8] вважає такими наступне.

По-перше, має бути забезпечена максимальна прозорість як щодо походження інформації, так і щодо того, яким чином вона генерується, ким спонсорується, поширюється та націлюється, аби надати можливість громадянам краще розуміти контент і виявляти ймовірні спроби маніпулювання чи дезінформування.

По-друге, сприяння різноманітності інформації, аби громадяни могли приймати обґрунтовані рішення на основі критичного аналізу (зокрема шляхом просування високоякісної журналістики, підвищення рівня власної медіаграмотності та зменшення дисбалансу у відносинах між творцями та розповсюджувачами інформації).

По-третє, підвищення рівня достовірності інформації шляхом надання доказів її надійності (зокрема через довірених інформаторів) і кращого відстеження та автентифікації впливових постачальників інформації.

По-четверте, пошук інклюзивних, комплексних рішень. Ефективні

довгострокові рішення вимагають підвищення обізнаності, рівня медіаграмотності, широкого залучення зацікавлених сторін і співпраці між представниками державного й недержавного секторів.

Окрім вже згаданих підходів, окремі країни здійснюють заходи регіонального рівня, спрямовані на забезпечення ефективного функціонування власного державного інформаційного простору. Так, зокрема, відповідно до Постанови Ради міністрів про заснування посади Урядового уповноваженого з питань безпеки інформаційного простору Республіки Польща [2] до завдань відповідної посадової особи віднесено:

1. Координацію діяльності органів державного управління, до компетенції яких входить виявлення, моніторинг та нейтралізація інформаційних загроз інтересам держави, у сфері розпізнавання та нейтралізації загроз безпеці інформаційного простору держави та реагування на них. До таких загроз, зокрема, належать:

– виявлення та аналіз інформаційної діяльності, основним фокусом якої є безпека, інтереси та імідж Республіки Польща;

– ідентифікація суб'єктів, особливо іноземних, які організовують та провадять інформаційну діяльність всупереч інтересам Республіки Польща;

– відстеження проявів інформаційно-психологічних операцій, які проводяться в інформаційному просторі проти держави;

– проведення заходів, спрямованих на нейтралізацію виявлених загроз безпеці інформаційного простору Республіки Польща;

– реалізація заходів щодо підвищення стійкості інформаційного простору держави шляхом:

а) публікації досліджень з питань забезпечення безпеки інформаційного простору держави;

б) провадження інформаційної діяльності, спрямованої на зміцнення безпеки, інтересів та іміджу держави;

в) координації інформаційно-комунікативної діяльності установ, відповідальних за формування інформаційної політики Республіки Польща.

2. Розроблення рекомендацій для Ради міністрів задля пошуку системних рішень, метою яких є підвищення здатності Республіки Польща протистояти інформаційним загрозам.

Аналіз повноважень Урядового уповноваженого з питань безпеки інформаційного простору Республіки Польща свідчить, що подібна посадова особа за своїми функціональними обов'язками охоплює досить широкий контекст щодо захисту інформаційного простору держави як загалом, так і в умовах загрози чи виникнення надзвичайних і кризових явищ зокрема. Це дає підстави зробити припущення, що заснування подібних посад в інших державах і поширення позитивного досвіду окремих країн у рамках загального підходу Європейського співтовариства може призвести до суттєвих позитивних зрушень у напрямку

забезпечення національної стійкості в інформаційній сфері держави.

Література

1. Bekämpfung von Desinformation im Internet: ein europäisches Konzept: Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen. COM (2018) 236 final. 26.04.2018. Brüssel, 2018. 21 S.

2. Rozporządzenie Rady Ministrów w sprawie ustanowienia Pełnomocnika Rządu do spraw Bezpieczeństwa Przestrzeni Informacyjnej Rzeczypospolitej Polskiej z dnia 11 sierpnia 2022 r. *Dziennik Ustaw Rzeczypospolitej Polskiej*. 17 sierp. 2022 r. Poz. 1714. S. 1–2.

Голодюк Ю.І.
Євтушик М.М.
студенти першого курсу
Національної академії СБ України
група НБ-221

ЕКСПЕРТНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ПРОЦЕСІВ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Вступ

Нові можливості сучасних інформаційних технологій створюють виклик традиційним системам генерування, розповсюдження та передачі знань, тобто системам науки й освіти.

Потужні бази даних і знань відіграють роль гігантських «сховищ» для нескінченних фактів і базових даних у тому числі з питань управління інформаційною безпекою, а глобальні комп’ютерні мережі стають потужними інструментами для високошвидкісного доступу до цієї інформації з будь-якого куточка світу.

У зв’язку з цим істотно зростає роль методологічних, системних, міждисциплінарних знань людини, необхідних для раціонального й осмисленого оперування з різноманітними знаннями і даними з метою вирішення нових, нестандартних проблем.

Виникає необхідність відходу від класичних підходів, що ґрунтуються на вивчені конкретних дисциплін, та переходу до проблемно орієнтованих методів формування знань, а також зменшення дистанції між фундаментальними і прикладними дослідженнями.

У цій новій парадигмі найголовніше місце відводиться формування аналітичних здібностей вченого, педагога чи студента, тобто його спроможності

шукати і знаходити необхідну інформацію, точно формулювати проблеми і гіпотези, вбачати в сукупностях даних певні закономірності, знаходити розв’язок складних міждисциплінарних задач.

Отже, розробка нових методик та інструментів отримання знань, у тому числі з питань управління інформаційною та кібернетичною безпекою, є актуальнім науковим завданням.

Основна частина.

У відповідь на появу нових сфер науки і технологій потребують змін традиційні університетські дисципліни. В результаті виникають міждисциплінарні програми навчання.

Професійна підготовка фахівців з питань управління інформаційною безпекою та дослідження в інших сферах знань потребують інтеграції цілої низки дисциплін, які раніше вважалися самостійними і не пов'язаними між собою.

Тому методологія систематизації знань має створюватися з урахуванням їхньої подальшої реалізації комп’ютерними засобами, що, в свою чергу, потребує їхньої формалізації та розробки нової технології навчального процесу.

З метою використання в навчальному процесі Академії запропоновано модель навчально-методичного комплексу (далі – НМК) для підготовки фахівців за напрямом «Організація захисту інформації з обмеженим доступом» та розглянуто можливості її реалізації у вигляді програмного забезпечення.

НМК — це інформаційно-методичний інструмент управління знаннями з питань інформаційної безпеки, який є простим, універсальним і ефективним засобом перетворення окремих відомостей в знання шляхом аналізу та синтезу потоків інформації з питань управління інформаційною безпекою.

В якості прикладу для аналізу інформації обрано зміст міжнародного стандарту ISO/IEC 27001 «Практичні правила менеджменту інформаційної безпеки». Стандарт ISO 27001 містить загальні принципи і практику впровадження, забезпечення і оптимізації управління інформаційною безпекою на всіх етапах життєвого циклу інформаційно-комунікаційних систем.

Висновки

Надані методичні та практичні рекомендації щодо організації захисту інформації з обмеженим доступом з використанням НМК в якості інформаційно-методичного інструменту синтезу знань з питань управління інформаційною безпекою.

Розглянуто теоретичні й практичні питання реалізації системного, об’єктно-орієнтованого та процесного підходів для вирішення конкретних навчальних завдань забезпечення управління інформаційною безпекою.

Запропоновано системне рішення для організації інформаційної взаємодії науковців, викладачів та студентів в навчальному процесі.

Література
1. Закон України «Про інформацію».
2. Закон України «Про основні засади забезпечення кібербезпеки України».
3. Стандарт ISO/IEC 27001 «Практичні правила менеджменту інформаційної безпеки».
4. Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури, затверджені постановою Кабінету Міністрів України від 19 червня 2019 року № 518.
5. Домарєв В.В. Система ситуаційного управління: теорія, методологія, рекомендації Київ: Знання України, 2017. – 347 с.

Дашковська О.В.
к.хім.н., доц.,старший науковий співробітник,
Погребняк В.П.
к.т.н., проф., старший науковий співробітник
ДНУ «Інститут модернізації змісту освіти»

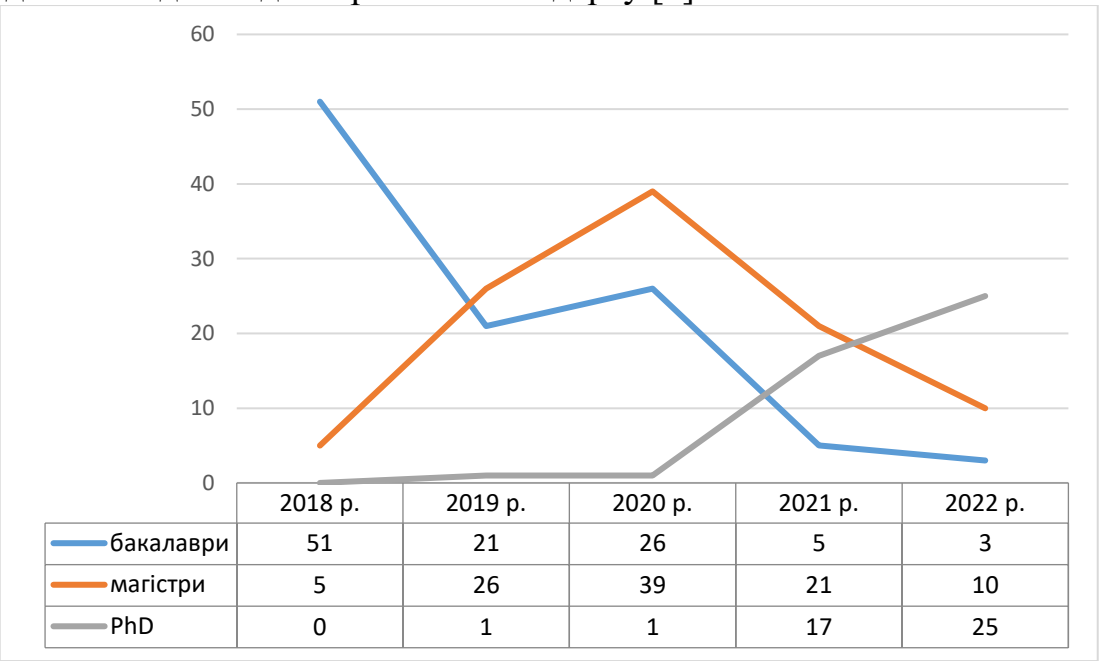
СТАНДАРТИ ВИЩОЇ ОСВІТИ ТА ОСВІТНІ ПРОГРАМИ: ОСОБЛИВОСТІ ТА РЕЗУЛЬТАТИ УПРОВАДЖЕННЯ В УМОВАХ ВОЄННОГО СТАНУ

Аналізується стан упровадження стандартів вищої освіти (далі СВО) та освітніх програм, здійснений у передвоєнний період, та досліджуються особливості організації і результати цієї діяльності в умовах воєнного стану в країні.

Зазначається, що СВО - це нове покоління освітніх стандартів, що замінило галузеві стандарти вищої освіти, які діяли у 2002-2014 роках. СВО розроблялись і впроваджувались в освітній процес згідно з положеннями Закону України «Про вищу освіту» [1] (далі Закон), спрямованими на модернізацію структури і змісту вищої освіти, та відповідають Національній рамці кваліфікацій, гармонізованій з Рамкою кваліфікацій Європейського простору вищої освіти і оновленому переліку спеціальностей [2].

До початку широкомасштабної агресії рф проти України Міністерство освіти і науки України оновило персональний склад Науково-методичної ради, оголосило конкурс до сектору вищої освіти, частково поповнило склад науково-методичних комісій (далі НМК), не завершивши їх планову ротацію. Внесено зміни та доповнення до деяких СВО бакалаврського та магістерського рівнів в частині форм атестації здобувачів вищої освіти: вони доповнені єдиним державним кваліфікаційним іспитом [3]. Станом на кінець 2022 року в установленому порядку було затверджено і введено в дію 106 бакалаврських, 101 магістерських

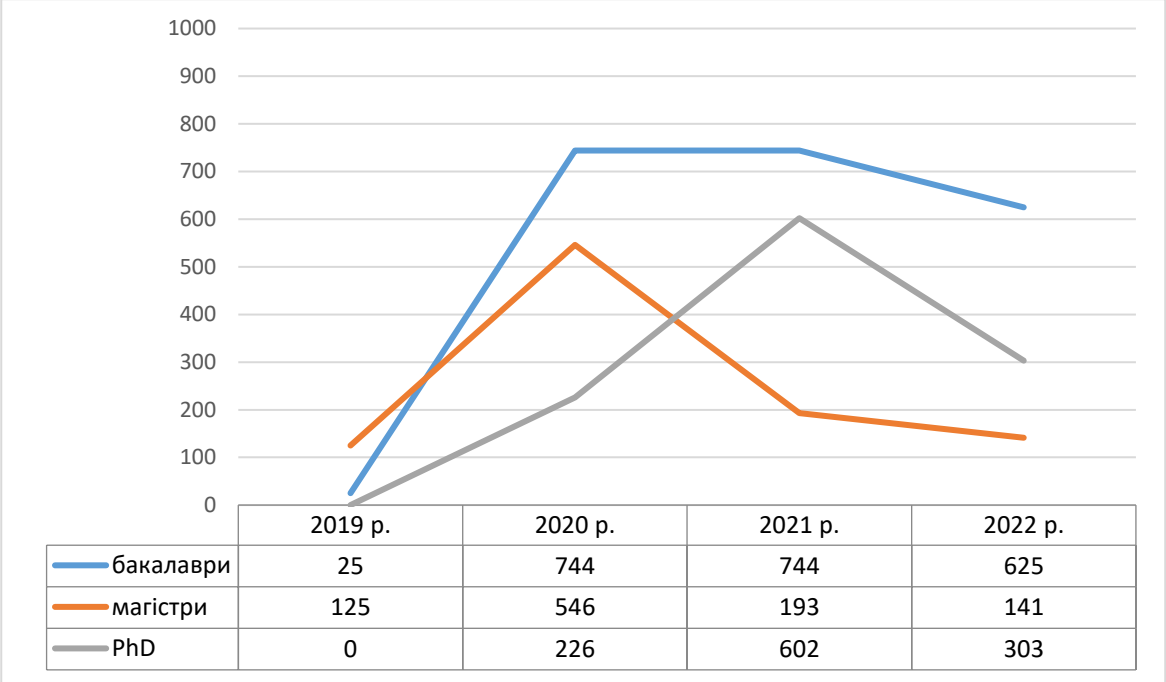
та 44 докторських стандартів (рис. 1). Слід зазначити, що у 2023 році не було затверджено жодного докторського стандарту [4].



	2018 р.	2019 р.	2020 р.	2021 р.	2022 р.
бакалаври	51	21	26	5	3
магістри	5	26	39	21	10
PhD	0	1	1	17	25

Рисунок 1. Затверджено стандартів вищої освіти.

З 2019 року запрацювало Національне агенство із забезпечення якості вищої освіти (далі НАЗЯВО), що фактично завершило формування у вищій освіті цілісної системи забезпечення якості: внутрішнього і зовнішнього забезпечення якості вищої освіти, забезпечення якісної діяльності самого національного агенства. Одночасно в законодавче поле було введено процес акредитації освітніх програм. З цього ж року акредитація освітніх програм здійснювалась НАЗЯВО в основному відповідно до вимог чинних законодавчо-нормативних актів. За даними НАЗЯВО [5] на кінець 2022 року акредитовано 4274 освітні програми: бакалавра - 2138, магістра - 1005, доктора філософії - 1131 (рис. 2). Порівняльний аналіз переліків акредитованих програм і списку затверджених СВО свідчить, що майже половина докторських освітньо-наукових програм акредитувалась без наявності затверджених СВО.



	2019 р.	2020 р.	2021 р.	2022 р.
бакалаври	25	744	744	625
магістри	125	546	193	141
PhD	0	226	602	303

Рисунок 2. Акредитовано освітніх програм

Введення в країні воєнного стану суттєво вплинуло на практику акредитації освітніх програм та термін дії акредитаційних документів. За зверненням НАЗЯВО уряд своєю постановою [6] дозволив агенству тимчасово проводити акредитацію освітніх програм у віддаленому (дистанційному) режимі, а також ухвалювати рішення про умовну (відкладену) акредитацію без проведення або з частковим проведенням акредитаційної експертизи без оплати ЗВО вартості акредитації. Також продовжено до 1 липня року, наступного за роком припинення або скасування воєнного стану в Україні, термін дії сертифікатів ЗВО (наукових установ) про акредитацію спеціальностей та сертифікатів про акредитацію освітніх програм, що були чинними на 24 лютого 2022 року.

НАЗЯВО, керуючись цією постановою, визначило Тимчасовий порядок акредитації освітніх програм в умовах воєнного стану [7]. Згідно з ним усі освітні програми, починаючи з 17 березня 2022 року, проходять процес акредитації за однією із двох процедур:

1) у віддаленому (дистанційному) режимі, відповідно до Положення про акредитацію освітніх програм, за якими здійснюється підготовка здобувачів вищої освіти [8];

2) за спрощеною процедурою з ухваленням рішення про умовну (відкладену) акредитацію без проведення або з частковим проведенням акредитаційної експертизи без оплати вартості акредитації закладом вищої освіти.

НАЗЯВО може ухвалити рішення про умовну (відкладену) акредитацію за спрощеною процедурою у разі наявності обґрунтування закладом вищої освіти неможливості проведення акредитації освітньої програми у віддаленому (дистанційному), змішаному режимах або в загальному порядку через

ушкодження внаслідок бойових дій. У такий спосіб, починаючи з травня 2022 року, акредитовано 892 освітні програми, з них 377 - бакалаврських, 264 - магістерських і 257 - доктора філософії.

Висновки

1. У вітчизняній вищій освіті створена необхідна нормативно-правова база і реалізуються відповідні організаційні заходи для забезпечення акредитації освітніх програм та дії акредитаційних документів в умовах воєнного стану в країні.
2. Уповільнився процес введення в дію стандартів освітньо-наукового/освітньо-мистецького рівнів вищої освіти. Враховуючи, що кількість затверджених «докторських» стандартів складає біля 50 відсотків від можливої, значна їх частина акредитується за відсутності затверджених стандартів.
3. Практика застосування СВО, переобтяженість матеріалами методичного характеру, вилучення із системи вищої освіти ставить проблему їх модернізації та спрощення з перенесенням змістовного навантаження на освітні програми.

Література

1. Про вищу освіту. Закон України від 01.07.2014 №1556-VII. URL: http://zakon2.rada.gov.ua/laws/show/1556-181.

2. Про внесення змін у додаток до постанови КМУ від 23.11.2011 №1341. Постанова КМУ від 25 червня 2020 року №519. URL: https://zakon.rada.gov.ua/laws/show/519-2020-%D0%BF#Tex

3. Про внесення змін до деяких стандартів вищої освіти. Наказ МОН від 13.01.2022 №26.

4. Затверджені стандарти вищої освіти. URL: https://mon.gov.ua/ua/osvita/visha-osvita/naukovo-metodichna-rada-ministerstva-osviti-i-nauki-ukrayini/zatverdzheni-standarti-vishoyi-osviti

5. Протоколи засідань. Офіційний сайт НАЗЯВО. URL: http://naqa.gov.ua.

6. Про особливості акредитації освітніх програм, за якими здійснюють підготовку здобувачів вищої освіти, в умовах воєнного стану. Постанова КМУ від 16 березня 2022 №295. URL: https://zakon.rada.gov.ua/laws/show/295-2022-%D0%BF#Text

7. Тимчасовий порядок акредитації освітніх програм, за якими здійснюється підготовка здобувачів вищої освіти, в умовах воєнного стану.URL:https://naqa.gov.ua/wp-content/uploads/2022/10/4_%D0%94%D0%BE%D0%B4%D0%B0%D1%82%D0%BE%D0%BA-%D0%B4%D0%BE-%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB-%E2%84%9619-%D0%B2%D1%96%D0%B4-25.10.2022-%D0%A2%D0%B8%D0%BC%D1%87%D0%B0%D1%81%D0%BE%D0%B2%D0%B8%D0%B9-1.pdf.

8. Про затвердження Положення про акредитацію освітніх програм, за якими здійснюється підготовка здобувачів вищої освіти. Наказ МОН від 11.07.2019 № 977. URL: https://mon.gov.ua/ua/npa/pro-zatverdzhennya-polozhennya-pro-akreditaciyu-osvitnih-program-za-yakimi-zdijsnyuyetsya-pidgo

Дацюк М.В.
Федірко Д.А.
курсанти Національна академія СБ України

ДЕСТРУКТИВНА ІНФОРМАЦІЙНА КАМПАНІЯ рф НА ТИМЧАСОВО ОКУПОВАНИХ ТЕРИТОРІЯХ УКРАЇНИ

Рішенням Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» визначено основні Національні виклики та загрози які на той момент стосувались періоду окупованих територій після 2014 року, до яких входили територія Донецької, Луганської областей та Автономної Республіки Крим, які включають:

Інформаційний вплив російської федерації як держави-агресора на населення України. російською федерацією використовуються нові активні заходи, у тому числі міжнародного характеру, щодо легітимізації спроби анексії Автономної Республіки Крим та міста Севастополя, заперечення своєї участі у війні на території Донецької та Луганської областей та посилення адвокаційної кампанії за зняття санкцій, запроваджених у зв'язку з порушенням російською федерацією суверенітету і територіальної цілісності України. Задіяння у цьому процесі російською федерацією всіх її політичних, інформаційних, економічних, розвідувальних та інших спроможностей. https://www.president.gov.ua/documents/6852021-41069

Інформаційне домінування російської федерації як держави-агресора на тимчасово окупованих територіях України. У результаті тимчасової окупації у 2014 році державою-агресором частини території України були захоплені розташовані на цій території об'єкти інформаційної інфраструктури, зокрема й об'єкти Концерну радіомовлення, радіозв'язку та телебачення.

Державою-агресором застосовуються методи тотального придушення свободи слова, контролю над редакційною політикою засобів масової інформації та інших інформаційних ресурсів, що функціонують на цих територіях.

На тимчасово окупованих територіях, у районах здійснення заходів із забезпечення національної безпеки і оборони, відсічі і стримування збройної агресії Російської Федерації у Донецькій та Луганській областях розгорнуто безпрецедентну інформаційну кампанію. Використовуючи також регулярне постачання на тимчасово окуповані території потужного передавального

обладнання та блокування українських інформаційних ресурсів, російська федерація намагається створити альтернативну викривлену інформаційну реальність, побудовану на наративах держави-агресора. Придушення будь-яких спроб інакомислення посилюється регулярними репресіями стосовно незалежних журналістів на тимчасово окупованій території Автономної Республіки Крим та міста Севастополя, а також переслідуванням за перегляд українського контенту, що є характерним для тимчасово окупованих територій Донецької та Луганської областей.

Інформаційний тиск, що здійснюється державою-агресором, негативно відображається й на дітях, які проживають на тимчасово окупованих територіях, адже через свій вік вони є особливо вразливими для впливу інформаційних кампаній. https://www.president.gov.ua/documents/6852021-41069

Обмежені можливості реагувати на дезінформаційні кампанії. Деструктивна пропаганда, поширення дезінформації як ззовні, так і всередині України застосовуються державою-агресором з метою підриву стійкості суспільства та інформаційної дестабілізації держави. https://www.president.gov.ua/documents/6852021-41069

Спроби маніпуляції свідомістю громадян України щодо європейської та євроатлантичної інтеграції України. Переважна більшість громадян підтримує реалізацію європейського та євроатлантичного курсу України. Водночас здійснюються спроби маніпуляції свідомістю громадян України шляхом поширення міфів та дезінформаційних (деструктивних) стереотипів щодо ЄС і НАТО з метою послаблення консолідації суспільства щодо зовнішньополітичного курсу України, гальмування проведення реформ, що негативно впливає на загальну суспільно-політичну ситуацію в державі. https://www.president.gov.ua/documents/6852021-41069

Доступ до інформації на місцевому рівні. Інформаційні потреби на місцевому рівні належним чином не задовольняються, зокрема через низьку спроможність забезпечення населення послугами з доступу до Інтернету.

Альтернативні джерела споживання інформації місцевого рівня, зокрема місцеві друковані засоби масової інформації, зазвичай є політично заангажованими від місцевих еліт. https://www.president.gov.ua/documents/6852021-41069

Недостатній рівень інформаційної культури та медіаграмотності в суспільстві для протидії маніпулятивним та інформаційним впливам. Відсутність належного рівня інформаційної культури та медіаграмотності в суспільстві в умовах стрімкого розвитку цифрових технологій створює підґрунтя для маніпулювання громадською думкою, проведення стрімких деструктивних інформаційних операцій, що зумовлює існування потенційних та реальних загроз інформаційній безпеці України. https://www.president.gov.ua/documents/6852021-41069

З початком окупації і анексії Криму та опору України військовій агресії рф на

території Донецької і Луганської областей, інформаційна політика росії перетворилася на тотальну військову дезінформаційну агресію, спрямовану на те, аби демонізувати в очах споживачів цієї інформації керівництво України.

6 березня 2014 р. на сайті телеканалу ATR проведено інтернет-референдума, під час якого можна було висловити свою думку щодо приєднання Криму до рф. Більшість людей, що взяли участь у голосуванні, висловилась проти. Тому вже 7 березня російські військовики у Криму відімкнули від інтернету перший кримськотатарський телеканал ATR. Того самого дня вони зупинили ефірне аналогове мовлення українського телеканалу «Інтер», на частотах якого транслюється НТВ.

В кінці вересня – початку жовтня 2023 року рф заявляла, що на території тимчасово окупованій Запорізькій області відбудуться референдуми щодо приєднання області до складу рф, звісно ж всі розуміли, що це все фейк, проте росія це масово розповсюджувала через свої внутрішні та зовнішні пропагандистські ЗМІ. «За даними ГУР МО України російські пропагандисти в різних місцях створювали постановочні сюжети. Завозили людей із ростовської області та Криму для того, щоб створити так звану масовку. Показати наскільки люди радіють, наскільки вони дружно йдуть голосувати. Цю картинку будуть показувати російському глядачу і будуть намагатися переконати Європу, що це відбулося відповідно до міжнародного права. Але ми розуміємо, що це фейк. Це чергова потужна інформаційна кампанія, які проводить рф, покриваючи свої злочини», – цитує Скібіцького пресслужба ГУР

Висновок. Все вище вказане, знову ж таки, стосувалось подій після 2014 року, але зараз ми бачимо, що це є актуальним на сьогодення. Тактика рф інформаційної війни порівняно з 2014 до 2023 року зовсім не змінилась, спочатку вони кажуть, що не будуть нападати, а через деякий час вже просувають свою пропагандистську інформацію використовуючи всі наявні і можливі методи, починаючи із ретрансляції на тимчасово окупованих територіях російських телепередач симоньян та скабєєвої і закінчуючи це агітацією з надписами «росия здесь навсегда і т.д.». Так 6 березня на території АРК відімкнули телеканали «1+1» і 5-ий. Ще раніше російський телеканал «россия 24» захопив ефірні частоти кримської приватної «Чорноморської телерадіокомпанії». Було також заблоковано державну телерадіокомпанію «Крим» у Сімферополі особами у камуфляжній формі без зброї. Генеральний директор ТРК Степан Гулеватий викликав міліцію, але вона не реагувала на виклик.

Література

1. Інформаційні операції РФ: як дискредитували Україну в інтернеті у грудні. URL: https://www.ukrinform.ua/rubric-world/3651143-informacijni-operacii-rf-ak-diskredituvali-ukrainu-v-interneti-u-grudni.html (дата звернення: 16.03.2023)

2. ГУР: Росія провела потужну інформаційну кампанію при проведенні

фейкового дійства – «референдумів». URL: https://detector.media/infospace/article/203308/2022-09-30-gur-rosiya-provela-potuzhnu-informatsiynu-kampaniyu-pry-provedenni-feykovogo-diystva-referendumiv/ (дата звернення: 16.03.2023)

3. УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №685/2021 «Про рішення Ради національної безпеки і оборони України» від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки". URL: https://www.president.gov.ua/documents/6852021-41069 (дата звернення: 16.03.2023)

Домарєв В.В.
к.т.н., доцент,
доцент кафедри ТЗІ ННІ ІБ СК НА СБ України
Комарова Л.О.
д.т.н., професор

ЕКСПЕРТНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ПРОЦЕСІВ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ

Вступ

Нова парадигма інформаційної безпеки, як концептуальна схема (модель) постановки і рішення проблеми, випливає з підвищених вимог до живучості інформаційно-комунікаційних систем, що характеризуються високим ступенем розподілу ресурсів і практично повною відсутністю централізованого керування.

Аналіз сучасного стану управління безпекою в інформаційній сфері національної безпеки України вказує на недостатню ефективність експертно-аналітичного забезпечення державних управлінських рішень щодо реагування суб'єктів сектора безпеки і обороні України на виклики і загрози в інформаційній сфері особливо в умовах військового стану [1].

Процеси експертно-аналітичного забезпечення (далі – ЕАЗ) спрямовані на підвищення ефективності управлінських рішень в умовах дефіциту часу, суперечності або недостовірності вхідної інформації.

На сьогодення питання управління ІБ (КБ) є актуальними для багатьох сфер національної та державної безпеки, а їх дослідженням займаються фахівці різних галузей наукових та спеціальних знань [2].

З огляду на таке існує необхідність удосконалення таких важливих процесів, як аналіз, прогнозування і планування заходів інформаційної безпеки, особливо що стосується питань покращення взаємодії між експертами сектору безпеки і оборони України.

Отже розробка та оптимізація технологій експертно-аналітичного забезпечення управлінських рішень суб'єктів сектору безпеки і оборони України в

галузі управління ІБ, а також питання організації взаємодії експертів державних, наукових та навчальних установ **є *актуальною науковою задачею*.**

Основна частина

Більшу частину ЕАЗ складають задачі системного аналізу. Це задачі декомпозиції, побудови математичних та системних моделей різного класу, комплексування проектних рішень, аналізу коректності впроваджених рішень тощо.

Складність й різнорідність сучасних процесів управління ІБ потребує використання системно-процесного та об’єктно-орієнтованого підходів до вирішення проблем експертно-аналітичного забезпечення процесів управління ІБ у спосіб розвитку методологічних, технологічних та організаційних основ.

Ефективність управління ІБ (КБ) залежить від спроможності суб’єктів сектора безпеки і оборони правильно працювати з інформаційними потоками та адекватно ухвалювати рішення на основі їх аналізу.

Експертно-аналітична діяльність - це робота, пов'язана з виконанням завдання компенсації неповноти або надмірності даних про стан і процеси гарантування національної безпеки.

Завдання експертно-аналітичного забезпечення управлінської діяльності полягає в інтелектуальній підтримці процесів ухвалення рішень, а саме:

забезпечення процедур використання неформалізованих знань експертів для підготовки колегіальних рішень та їх процедурна підтримка;

вироблення інформаційних технологій та затвердження системи показників для оцінки, аналізу і прогнозування стану ІБ (КБ);

вироблення та затвердження методології та практичних рекомендацій щодо використання існуючих в органах державного управління експертно-аналітичних систем для підтримки ухвалення управлінських рішень в умовах військового стану;

створення інструментарію експертно-аналітичної підтримки процесу моніторингу стану ІБ (КБ) та ухвалення стратегічних рішень тощо.

Високий рівень ефективності ЕАЗ досягається за рахунок скоординованої, законодавчо регламентованої діяльності експертів державних, наукових та навчальних установ, яка спрямована на захист національних цінностей й інтересів інформаційній сфері та кіберпросторі [3].

Логіка технологій ЕАЗ щодо набуття та узгодження знань в галузі управління ІБ (КБ) полягає в наступному [4]:

1. Визначається предметна галузь знань з питань управління ІБ (КБ).
2. Проводиться системній аналіз та створюються моделі обраної предметної галузі.
3. Розробляються методики та алгоритми використання моделей.

4. З використанням єдиних (універсальних) моделей, методик та алгоритмів здійснюється узгоджена діяльність експертів державних, наукових та навчальних установ.

Для дослідження, створення та використання технологій ЕАЗ використано такі наукові підходи: системний, процесний, об’єктно-орієнтований, а також нечіткі логіка (fuzzy logic) та множини, що перетинаються. А також запропоновано логіко-лінгвістичну матричну модель загальної безпеки (рис.1) та алгоритм її використання (рис.2) в якості науково-методичного апарату організації взаємодії експертів [4].

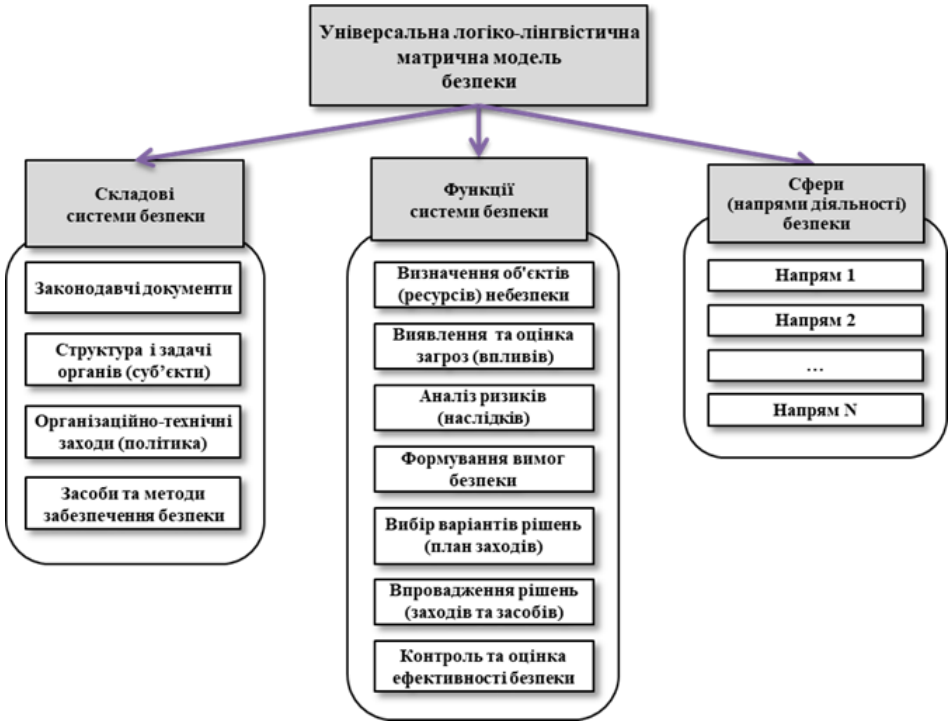


Рис.1 Логіко-лінгвістична матрична модель загальної безпеки

Висновки

За результатами аналізу проблемних питань організації експертно-аналітичного забезпечення процесів управління ІБ (КБ) запропоновано методичний підхід щодо організації взаємодії експертів державних, наукових та навчальних установ з метою підвищення ефективності експертно-аналітичного забезпечення процесів управління ІБ (КБ) на державному рівні.

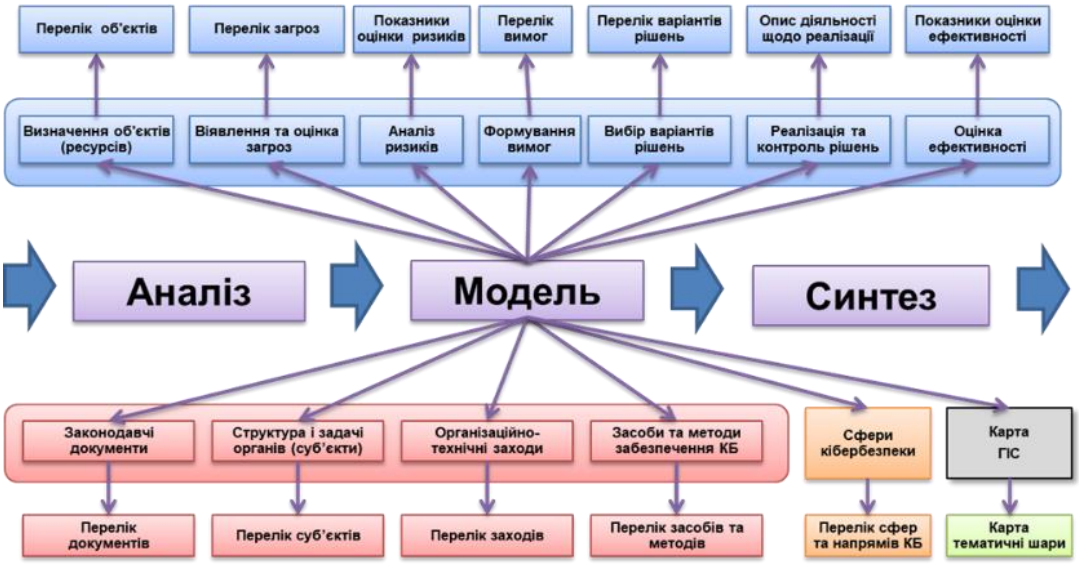


Рис.2 Алгоритм використання логіко-лінгвістичної матричної моделі

Використано системно-процесний та об’єктно-орієнтований підхід а також логіко-лінгвістична матрична модель які дозволяють підвищити ефективність ЕАЗ у залежності від того, наскільки якісно обґрунтовані та втілені системні логіко-функціональні зв’язки між компонентами моделі.

Запропоновано технології експертно-аналітичного забезпечення які спрямовані на забезпечення діяльності осіб, що ухвалюють рішення в умовах дефіциту часу, суперечності або недостовірності вхідної інформації.

Література

1. Закон України Про інформацію.

2. Закон України Про основні засади забезпечення кібербезпеки України.

3. Загальні вимоги до кіберзахисту об’єктів критичної інфраструктури, затверджені постановою Кабінету Міністрів України від 19 червня 2019 року № 518.

4. Домарєв В.В. Система ситуаційного управління: теорія, методологія, рекомендації, Київ: Знання України, 2017. 347 с.

Загика М.В.
студентка,
Навчально-науковий інститут інформаційної безпеки та стратегічних комунікацій Національної академії Служби безпеки України

КІБЕРЗАХИСТ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: ПОШУК ПРОБЛЕМ ТА ШЛЯХІВ ЇХ ВИРІШЕННЯ

Кінцевою метою хакерів, як правило є збагачення. Відрізняються тільки шляхи досягнення кінцевої мети: шифрування даних на кінцевих пристроях користувачів з метою вимагання коштів за розшифрування, фішинг, викрадення баз даних з персональними або будь-якими іншими даними, за які можна отримати кошти тощо. Однак, ситуація в українському кіберпросторі дещо інша. Кількість кібератак та кіберінцидентів із початком повномасштабного вторгнення різко зросла. Крім того, кібератаки часто передують або ж корелюють із кінетичними атаками ворога. Стає зрозуміло, що за більшістю кібератак стоять російські спецслужби та хактивісти, що працюють на уряд російської федерації, адже більшість атак було спрямовано на державний сектор та сектор безпеки і оборони.[1][2][3]

Метою російської федерації є українська інформаційна інфраструктура: її знищення чи отримання доступу до українських державних інформаційних ресурсів. Варто розуміти, що кібератаки можуть бути допоміжним інструментом за допомогою якого ворог проводить його інформаційно-психологічні операції з метою створення панічних настроїв та поширення пропаганди й дезінформації. Свідченням цього можуть бути розсилання інформаційних повідомлень із шкідливим програмним забезпеченням, в тому числі із скомпрометованих електронних скриньок органів державної влади, – збільшення кібератак на засоби масової інформації.[4][5][6][7] Але, варто розуміти, що кібератаки становлять серйозну загрозу інформаційній безпеці держави. Атаки на логістичний сектор та державні інформаційні ресурси, ресурси органів державної влади, телекомунікаційну сферу – можуть спричинити не просто панічні настрої, а ускладнити функціонування та взаємодію між суб'єктами важливими для функціонування держави.[7][8][9][10]

З початком повномасштабного вторгнення на армію та державу почали посилено працювати об'єкти критичної інфраструктури, а отже стали пріоритетною ціллю для ворога, в тому числі й у кіберпросторі. Захист таких об'єктів у кіберпросторі є складовою національної безпеки держави. Однак, наразі лише розпочато процес формування реєстру об'єктів критичної інфраструктури, категоризацію об'єктів критичної інфраструктури у секторах і досить тривалий період займе процес реалізації усіх вимог з організації заходів безпеки на цих об'єктах. Одним із напрямків забезпечення безпеки об'єкта критичної

інфраструктури є його кіберзахист.

На сьогодні основними суб'єктами національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України. Кожен із цих суб'єктів виконує свої завдання із забезпечення кібербезпеки держави. Зрозуміло, що ці структури взаємодіють та обмінюються інформацією щодо кіберзагроз між собою, а в певних випадках і з міжнародними партнерами. Однак, процес захисту об'єктів критичної інфраструктури лише розпочався, що стосується як законодавчої частини, так і реалізації заходів вже на фізичному та технічному рівнях.

Вже в умовах воєнного стану під триваючими кінетичними та кібернетичними атаками різко збільшилась кількість об'єктів, яким необхідно забезпечити кіберзахист. Процес побудови захисту об'єктів критичної інфраструктури вже в умовах воєнного стану вимагає швидких дій, що також може чинити певний негативний вплив, оскільки для кожного об'єкту необхідно створити індивідуальний комплекс заходів, що вимагає більше часу, ніж розробка типових стандартних рекомендацій чи положень для усіх об'єктів загалом. Треба також зазначити, що відповідно до постанови Кабінету Міністрів України від 9 жовтня 2020 року № 1109 «Деякі питання об'єктів критичної інфраструктури» до об'єктів критичної інфраструктури може бути віднесено установу як державної, так і приватної форм власності. Разом з тим, для приватних структур наразі відсутній обов'язковий механізм моніторингу та інформування основних суб'єктів національної системи кібербезпеки про кіберінциденти. Також, в Україні є лише Урядова команда реагування на комп'ютерні надзвичайні події CERT-UA, галузеві команди чи ті, які функціонували б при якійсь бізнес структурі – відсутні. Крім того, CERT-UA опрацьовує лише певну частину кіберінцидентів у державному секторі і ті запити приватних установ, що були ними ініційовані. Тобто, повномасштабної статистики щодо кіберзагроз наразі немає.

Ще однією проблемою стає нестача профільних фахівців у сфері кіберзахисту. Це стосується і об'єктів критичної інфраструктури, яким необхідні такі фахівці для забезпечення підтримки кібербезпеки та швидкої реакції у разі кіберзагрози на об'єкті, так і основних суб'єктів національної системи кібербезпеки, оскільки на них теж збільшується відповідне навантаження.

Отже, для ефективного кіберзахисту об'єктів критичної інфраструктури: швидкого реагування та запобігання кіберзагрозам, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем об'єктів можна запропонувати такі шляхи вирішення проблем:

- удосконалення механізмів взаємодії та обміну інформацією про кіберзагрози між основними суб'єктами національної системи кібербезпеки;
- створювати навчальних програм та курсів для підготовки кадрів у сфері

кіберзахисту, а також, системне напрацювання та підвищення рівня знань, вмінь та практичних навичок фахівців з кіберзахисту;

- створення регіональних та галузевих центрів та команд реагування на кіберінциденти та кіберзагрози;

- залучення міжнародних партнерів для підготовки українських фахівців;

Література

1. У ніч повномасштабного вторгнення рф ворог хотів знищити весь кіберзахист України, – СБУ: веб-сайт. URL: https://ssu.gov.ua/novyny/u-nich-povnomasshtabnoho-vtorhnennia-rf-voroh-khotiv-znyshchyty-ves-kiberzakhyst-ukrainy-sbu-video (дата звернення: 18.03.2023).

2. 14 млн підозрілих подій інформаційної безпеки за три місяці: звіт оперативного центру реагування на кіберінциденти ДЦКЗ: Державна служба спеціального зв'язку та захисту інформації України: веб-сайт. URL: https://cip.gov.ua/ua/news/14-mln-pidozrilikh-podii-informaciinoyi-bezpeki-za-tri-misyaci-zvit-operativnogo-centru-reaguvannya-na-kiberincidenti-dckz (дата звернення: 18.03.2023).

3. Former Conti ransomware gang members helped target Ukraine, Google says: веб-сайт. URL: https://www.theverge.com/2022/9/7/23341045/former-conti-ransomware-gang-target-ukraine-google (дата звернення: 18.03.2023).

4. «Позбавити українців інформації». У Держспецзв'язку прокоментували кібератаку на Укрінформ: веб-сайт. URL: https://biz.nv.ua/ukr/tech/kiberataka-na-ukrinform-u-derzhspeczv-yazku-nazvali-naslidki-novini-ukrajini-50298355.html (дата звернення: 19.03.2023).

5. Держспецзв'язку: вороги атакують електронні пошти військових: веб-сайт. URL: https://ms.detector.media/manipulyatsii/post/29036/2022-02-25-derzhspetszvy azku-vorogy-atakuyut-elektronni-poshty-viyskovykh/ (дата звернення: 19.03.2023).

6. «Бійтесь і чекайте гіршого»: хакери атакували урядові сайти та «Дію» : веб-сайт. URL: https://www.pravda.com.ua/news/2022/01/14/7320353/(дата звернення: 18.03.2023).

7. Довідкова інформація з питань діяльності CERT-UA за фактами впливу на стан кібербезпеки у 2022 році: Computer Emergency Response Team of Ukraine: веб-сайт. URL: https://cert.gov.ua/article/37121 (дата звернення: 16.06.2022).

8. https://speka.media/rosiiski-xakeri-zdiisnili-bezprecedentnu-kiberataku-na-oficiinii-sait-energoatoma-p11k5p (дата звернення: 20.03.2023).

9. Статистика кібератак на українську критичну інформаційну інфраструктуру: 15–22 березня: Державна служба спеціального зв'язку та захисту інформації України: веб-сайт. URL: https://cip.gov.ua/ua/news/statistika-kiberatak-na-ukrayi nsku-kritichnu-informaciinu-infrastrukturu-15-22-bereznya (дата звернення: 20.03.2023).

10. Satellite outage caused 'huge loss in communications' at war's outset -Ukrainian

official URL: https://www.reuters.com/world/satellite-outage-caused-huge-loss-communications-wars-outset-ukrainian-official-2022-03-15/ (дата звернення: 19.03.2023).

Запорожець А.С.
студент Національної академії СБ України

ОСНОВНІ НАПРЯМИ ДЕРЖАВНОЇ ПОЛІТИКИ У ВОЄННІЙ СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Безпека є головною умовою суспільного життя, а її забезпечення це одна з основних функцій держави. Неспроможність втілити й гарантувати цю базову соціальну цінність призводить до неминучого занепаду суспільства та держави. Економічний добробут і панування законів є важливими умовами комфортного соціального співіснування людей, однак доцільним та виправданим це існування робить захищеність від фундаментальних загроз. Безпека спільно з такими поняттями як суспільство, нація, особистість, держава, влада, світовий розвиток і світопорядок, належить до числа базових цінностей і цілей життєдіяльності. Вона належить до числа найбільш актуальних і в той же час дискусійних тем різних галузей знань.

Актуальність теми дослідження обумовлюється повномасштабним вторгеннням Російської Федерації на територію України у лютому 2022 року та існуванням кризи існуючої системи міжнародної безпеки, поширенням практики погроз силою та безкарне застосування військової агресії окремими державами для реалізації власних інтересів у міжнародних відносинах коли під реальною загрозою знаходиться національна безпека нашої держави.

Об’єкт роботи - процеси реалізації державної політики у воєнній сфері національної безпеки України.

Предмет - вплив сучасних загроз на процеси реалізаії державної політики у воєнній сфері національної безпеки України.

Мета дослідження полягає у формуванні національної безпеки держави.

Виклад основного матеріалу дослідження. Проблеми безпеки та її забезпечення є одним з найважливіших явищ в умовах сучасного світу. Найважливішим досвідом підвищення ролі безпеки зіграло ХХ століття, що включило в себе дві найбільші світові війни, велику кількість локальних конфліктів. Досвід забезпечення безпеки виявляв особливу значимість не тільки міжнародної безпеки, а й державної в цілому. Поняття «держава» та «безпека» пов’язані нерозривно. Перспективи розвитку української державності багато в чому визначатимуться здатністю держави і суспільства сформувати систему заходів забезпечення безпеки, адекватну рівню загроз, що виникають.

Відповідно до пункту 3 Положення про Міністерство оборони України [1], головним органом у системі центральних органів виконавчої влади у формуванні та реалізації державної політики з питань національної безпеки у воєнній сфері, сфері оборони і військового будівництва, тобто у формуванні й реалізації воєнної політики, є Міністерство оборони України.

На мою думку, перед тим, як дослідити основні напрями державної політики у воєнній сфері національної безпеки України, необхідно виявити особливості воєнної політики загалом.

По-перше, воєнна політика є політикою головного політичного інституту держави. Інші політичні учасники, такі як громадські рухи, партії, групи інтересів та інші соціальні групи також можуть брати участь у розробці та реалізації воєнної політики, але переважно лише через своїх представників в органах державної влади. Таким чином, можна зробити висновок про неповну тотожність суб'єктів воєнної політики та суб'єктів політики. Оскільки держава має монополію на військову силу, вона виступає головним учасником воєнної політики. Втрата контролю над військовою силою з боку держави тягне або зміну політичного режиму або втрату суверенітету.

По-друге, основним завданням воєнної політики є недопущення великомасштабного військового зіткнення та забезпечення воєнної безпеки держави. Тут також головним суб'єктом виступає держава.

По-третє, воєнна політика перебуває у діалектичному зв'язку з військовою силою. Жодна інша складова державної політики (економічна, екологічна, духовна, соціальна, демографічна тощо) не має такого потенціалу.

По-четверте, зміст воєнної політики розкривається через її основи, механізми її реалізації, військово-політичний базис, суб'єктно-об'єктну складову, воєнно-політичні відносини, воєнно-політичну діяльність, цілі та засоби їх досягнення.

По-п'яте, така політика має власну матеріально-економічну базу у вигляді військово-промислового комплексу. Армія, будучи частиною суспільства, займає особливе місце у його соціально-політичній структурі.

Тож, воєнна політика взаємодіє практично з усіма сферами суспільного життя, які пов'язані зі створенням і використанням військової сили.

Президент України ввів у дію рішення Ради національної безпеки та оборони України від 30 грудня 2021 року «Про стратегію забезпечення державної безпеки» [2]. Відповідно до затвердженої Указом Стратегії вона визначає реальні та потенційні загрози державній безпеці України, напрями та завдання державної політики у сфері держбезпеки, є основою для планування та реалізації політики у цій сфері.

Пункт 23 Указу прямо визначає напрями державної політики у сфері забезпечення державної безпеки. Деякі положення, які стосуються воєнної сфери: розмежування повноважень та завдань між суб'єктами сектору безпеки й оборони, удосконалення взаємодії, у тому числі інформаційного обміну, та координації дій

між ними, а також з іншими державними органами; удосконалення національного законодавства у сфері забезпечення державної безпеки та гармонізація із законодавством Європейського Союзу і документами НАТО; приєднання до міжнародних програм співробітництва, урахування міжнародного досвіду щодо функціонування системидержавного управління, упровадження нових гнучких підходів до забезпечення державної безпеки стосовно охорони інформації з обмеженим доступом.

Пункт 24 Указу визначає основні завдання державної політики у сфері забезпечення державної безпеки, а саме: удосконалення контррозвідувального забезпечення державного суверенітету, конституційного ладу, територіальної цілісності, оборонного, економічного і науково-технічного потенціалу, економічної безпеки, об'єктів критичної інфраструктури від впливу суб'єктів розвідувально-підривної діяльності; попередження, виявлення та припинення злочинів проти основ національної безпеки, миру і безпеки людства, розповсюдження зброї масового ураження й інших злочинів, які становлять загрозу державній безпеці України; впровадження гармонізованих зі стандартами безпеки НАТО та ЄС механізмів функціонування системи забезпечення безпеки державної таємниці та службової інформації; забезпечення подальшого розвитку та поліпшення загальнодержавної системи захисту державного кордону; посилення міграційного контролю на державному кордоні та в державі та ін.

Як можна помітити, деякі положення стосуються узгодження національного законодавства з законодавством ЄС та документами НАТО. Вважаю ці положення одними з ключових, оскільки зараз наша держава перебуває на шляху вступу до ЄС і НАТО. Тому докладніше варто зупинитись на цьому. Основним і незмінним завданням НАТО є захист свободи і безпеки усіх членів Альянсу політичними і військовими засобами. В основу НАТО покладено принцип колективної оборони, який забезпечує дух солідарності і згуртованості між членами організації.

Сьогодні Україна є ключовим регіональним стратегічним партнером США, яка спрямовує колосальні зусилля на проведення реформ збройних сил та підвищення їхньої оперативно-бойової сумісності із збройними силами країн — учасниць НАТО. Сполучені Штати Америки продовжують підтримувати Україну у її прагненнях до євроатлантичної солідарності. В угоді України зі США про стратегічне партнерство основна увага приділяється важливості підтримки двосторонньої співпраці та подальшої прихильності до зобов'язань з боку США підтримувати націленість України на взаємодію з НАТО.

Перевагами вступу України в НАТО може стати одержання міцних гарантій її національній безпеці, незалежності, суверенітету та територіальної цілісності; відхід із сфери геополітичного домінування Росії і досягнення з нею рівноправних міждержавних відносин; зміцнення внутрішніх основ національної безпеки; покращення міжнародного іміджу тощо.

Україна вже зазначила в Основному Законі про намір вступу до НАТО.

З метою набуття членства в цій організації держава має відповідати певним стандартам і критеріям, яким відповідають країни Альянсу, але яким наразі не відповідає Україна. У разі проведення дієвих реформ і реального їх втілення в життя Україна повинна пройти довгий шлях перебудови основних інституцій системи державного управління. Це означає, що слід провести глобальну конституційну реформу, яка вплине на форму держави і систему державного апарату [3].

Підсумовуючи, варто зазначити, що загальна оцінка ситуації навколо України показує, що загрози її воєнній безпеці еволюціонують, стають багатофакторними, концентруються в масштабах всієї держави, взаємно впливають одна на одну, набувають комплексного характеру і тому вимагають усвідомленого, цілеспрямованого та системного підходу для їх нейтралізації. У шкалі пріоритетів воєнної безпеки України головним є збереження її державної цілісності. Тут, насамперед, слід розглядати виклики ззовні, що мають воєнно-політичну та економічну спрямованість.

Проблема вдосконалення державної політики та управління у сфері безпеки об’єктивно існує, і до її вирішення мають бути залучені професіонали силового блоку, кваліфіковані експерти від громадянського суспільства та наукового середовища, використання позитивного досвіду зарубіжних держав.

Література

1. Указ Президента України «Про Положення про Міністерство оборони України та Положення про Генеральний штаб Збройних Сил України» № 406/2011 від 6 квітня 2011 р. [Електронний ресурс]. – Режим доступу до ресурсу: https://www.president.gov.ua/documents/4062011-12968 .

2. Указ Президента України «Про рішення Ради національної безпеки і оборони України «Про Стратегію забезпечення державної безпеки» №56/2022 від 30 грудня 2021 р. [Електронний ресурс]. – Режим доступу до ресурсу: https://www.president.gov.ua/documents/562022-41377 .

3. Чукаєва В.О., Дивнич Д.І. Нова доктрина розвитку державності України: вступ до НАТО. Актуальні проблеми вітчизняної юриспруденції № 2. 2019. с.41-43.

Zviertsev H.
postgraduate student
Department of Cyber Security
National Technical University "Kharkiv Polytechnic Institute"
Tomashevsky B.
PhD, Associate Professor
Department of Cyber Security
Ternopil Ivan Puluj National Technical University

THE TECHNIQUE DESIGN TO GUARANTEE PRIVACY AND LEGITIMACY IN WIRELESS COMMUNICATION PATHWAYS

A method has been developed to ensure the authenticity and integrity of data in wireless channels based on post-quantum cryptographic systems. Smart technologies use wireless communication channel standards such as IEEE 802.11X, IEEE 802.15.4, and IEEE 802.16, where authenticity and confidentiality protocols are based on symmetric algorithms. However, in the post-quantum era, the stability of such algorithms is questionable. Post-quantum algorithms - McEliece/Niederreiter cryptosystems based on elliptic/modified elliptic/subspace/low-density parity-check code constructions are proposed to be used. Creating multi-loop information security systems allows for an objective assessment of the current state of the system and the formation of preventive measures against cyber threats. The proposed method of ensuring confidentiality, integrity, and authenticity based on cryptosystem constructions takes into account the level of confidentiality of transmitted information and provides the necessary level of stability, speed, and reliability of information.

Various approaches are proposed to ensure security and expand digital services based on smart technologies, including classical mechanisms, blockchain technologies, and threat analysis. Modeling information security systems (ISS) can be described based on business process modeling notation (BPMN) and a multi-domain language for component-oriented modeling of CPS Modelica. The internal and external loops of multi-loop information security systems provide an objective assessment of the current state of the system and the formation of the necessary tuples of ISS elements. An authentication protocol based on the use of authentication smart cards using random number generators on elliptic curves is proposed in [1]. However, this approach is susceptible to skimming attacks and does not provide confidentiality and integrity services in wireless communication channels.

This work provides an overview of various methods and protocols for ensuring the security of key data transmission in cyber-physical security (CPS) systems. Both classical methods, such as hash-based protocols and mechanisms for ensuring data authenticity and integrity, and modern methods, such as protocols based on crypto-code

constructions (CCC) of McEliece and Niederreiter on algebraic-geometric codes, were considered.

In works [2] and [4], protocols were presented that provide data authenticity and confidentiality based on the use of the A5 stream cipher and the two-factor authentication and key agreement (AKA) scheme for 5G mobile communication. However, in work [4], a vulnerability of the 5G-AKA protocol to Linkability of AKA Failure Messages (LFM) attacks was identified, which reduces the level of data confidentiality.

Methods based on crypto-code constructions of McEliece and Niederreiter on algebraic-geometric codes were proposed in works [5, 6] to ensure the security of key data transmission in the post-quantum period. Practical ways to reduce energy and computational costs when using these methods were also presented.

Thus, to ensure the security of key data transmission in CPS, both classical methods and the latest methods based on crypto-code constructions can be used. When choosing a specific method, it is necessary to take into account the multi-circuit architecture of CPS and the hybridity and synergy of APT attacks.

A protocol based on an enhanced multi-server key agreement scheme with hash-based authenticity verification and autonomous RS is proposed to ensure the security of key transmission in [2]. Threat analysis on CPS and the use of OTP passwords in various authentication schemes are presented in [3], however, this approach does not consider the multi-loop architecture of CPS and the synergy of APT attacks. Analysis of the 5G-AKA protocol and its modification for confidentiality is presented in [4], where it was found that 5G-AKA is vulnerable to LFM attacks. In [5, 6], the use of McEliece and Niederreiter cryptographic constructions on algebraic-geometric codes is proposed to provide security services in the post-quantum period, while in [6, 7], ways to reduce energy and computational costs for using cryptographic code-based (CCB) schemes in wireless channel security systems are presented.

The analysis shows that the growth of computing resources and mobile technologies has driven the development of wireless channels based on smart technologies. This enables the creation of CPS and SCPS and expands the range of digital services. However, the expansion of wireless technology capabilities also reduces the security of smart-city systems and Next Generation Networks. Mechanisms for ensuring confidentiality and integrity in 4G-6G technologies are necessary. An important direction in constructing security systems is the use of post-quantum algorithms and the formation of multi-loop security systems on algebraic-geometric codes.

The aim of the work is to develop a method for ensuring security in wireless channels based on post-quantum algorithms. To do this, it is necessary to develop the concept of a two-loop CPS security system, a mathematical model, and a practical implementation algorithm. Security in wireless channels is being investigated using post-quantum cryptographic code constructions of McEliece and Niederreiter based on

algebraic-geometric codes [5, 6, 8]. These constructions are based on the theory of error-correcting coding and the orthogonality of the G and H matrices of the linear code. They allow for confidentiality and data integrity services with practically the same energy costs for encryption, despite the trade-off between wireless channel speed and the use of cryptographic algorithms. However, in the post-quantum period, the demands for symmetric cryptography algorithms increase, which raises doubts about the possibility of compromising between the volume of key data and the memory capacity of switching devices, as well as the ability to encrypt various information streams based on symmetric cryptography in offline mode.

Both cryptographic code constructions use masking matrices: X, P, D, G, and H. X and P are randomly generated matrices, D is a diagonal matrix, and G and H are the generating and checking matrices, respectively. The Niederreiter cryptosystem uses balanced coding to ensure fast encoding. Table 1 shows the main characteristics of elliptic (EC) and modified elliptic (MEC) codes using the Galois field GF(q), the smooth projective algebraic curve X, the curve's genus g, the set of its points N=X(GF(q)), the divisor class C, and the mapping φ:XPk-1. The set yi=φ(xi) defines the code, and the number of points of intersection between φ(X) and a hyperplane is α, where n–dα. This construction allows for codes with parameters of k+dn–g+1, where the length n is less than or equal to the number of points on curve X.To create a two-circuit security system for CPS based on post-quantum algorithms, an approach from [8] was used, based on the concept of crypto-code constructions. It is recommended to use a gradation of the degree of information secrecy when choosing codes for crypto-code systems in socio-cyberphysical systems.

Table 1. Main (*n, k, d*) characteristics *EC*, *MEC*

(*n, k, d*) parameters of the code, which is built through a mapping of the form $\varphi: X \rightarrow P^{k-1}$	$n = 2\sqrt{q}+q+1$, $k \geq \alpha$, $d \geq n-\alpha$, $\alpha = 3 \times degF$, $k+d \geq n$	
(*n, k, d*) parameters of the code, which is built through a mapping of the form $\varphi: X \rightarrow P^{r-1}$	$n = 2\sqrt{q}+q+1$, $k \geq n-\alpha$, $d \geq \alpha$, $\alpha = 3 \times degF$, $k+d \geq n$	
Characteristics	Shortened *MEC*	Elongated *MEC*
(*n, k, d*) parameters of the code, which is built through a mapping of the form $\varphi: X \rightarrow P^{k-1}$	$n = 2\sqrt{q}+q+1-x$, $k \geq \alpha-x$, $d \geq n-\alpha$, $\alpha = 3 \times degF$, $k+d \geq n$	$n = 2\sqrt{q}+q+1-x+x_1$, $k \geq \alpha-x+x_1$, $d \geq n-\alpha$, $\alpha = 3 \times degF$
n, k, d) parameters of the code, which is built through a mapping of the form $\varphi: X \rightarrow P^{r-1}$	$n = 2\sqrt{q}+q+1-x$, $k \geq n-\alpha$, $d \geq \alpha$, $\alpha = 3 \times degF$, $k+d \geq n$	$n = 2\sqrt{q}+q+1-x+x_1$, $k \geq n-\alpha$, $d \geq \alpha$, $\alpha = 3 \times degF$

A dual-circuit security system based on various error-correcting codes is proposed to ensure confidentiality and authenticity of information in socio-cyber-physical systems (CPS). The internal circuit consists of physical control devices and a dispatch server,

while the external circuit includes a key generation server and mobile applications. Hardware encryptors are proposed to be installed on the elements of the internal circuit, and the Niederreiter Cryptosystem is used to connect the circuits. The use of two Niederreiter Cryptosystems enhances the level of security, and long-term keys are stored in an encrypted form. This approach ensures the closure of all information transmission channels and uses post-quantum cryptosystems.

The presented mathematical model uses the McEliece Cryptosystem and Niederreiter Cryptosystem to ensure security in cyber-physical systems based on wireless communication channels. It integrates crypto-code constructions on McEliece Cryptosystem and rank-metric codes, which allows creating hybrid cryptosystems for practical implementation on resource-limited chipsets. Experimental studies have shown that this approach requires a mobile Internet channel and takes into account the multicycle nature of CPS, which makes it possible to form a reliable information protection system in the post-quantum period with possible ART-attacks characterized by hybridity and synergy.

The proposed method for ensuring confidentiality and authenticity in wireless channels uses bidirectional communication channels, such as communication between a key fob and a car's onboard computer. The McEliece Cryptosystem is used to form "dialogue encoding," which requires a receiver and transmitter in the main module and key fob. Information packets are encrypted on the internal security circuit. A long-term secret key stored on the external circuit allows for the formation of personal keys and public keys of the cryptosystem at the user's request. To ensure the authenticity of the command sent from the key fob, a random number generated by the car's onboard computer is used at each "appearance." A generator based on a linear feedback shift register with feedback (LFSR) modulo an irreducible polynomial of degree 76 is used to generate pseudo-random numbers.

The key sequence Ki fills the shift register during the first k time steps, then the key is switched to the lower position and the values of the shift register are output from the device. The shift register moves the information one cell to the right at each time interval, receiving values from the feedback loop of the LFSR. Using the feedback function, a pseudo-random sequence of maximum period of length 76 bits is generated. Multiplexers are used to convert the number into an information sequence I1×19 with elements from the GF (24) field.

The developed method for ensuring authenticity and confidentiality of information in wireless channels is based on resilient protection against post-quantum threats from Grover and Shor, and allows for tunneling mode in open channels, confirmed by the results of research. The parameters of error-correcting codes and cryptosystems based on the McEliece and Niederreiter PKC provide practical applications. The software implementation of PKC on MES in the GF(26) field requires significantly fewer group operations than the implementation of McEliece PKC in the GF(210) field.

The HCCC algorithm increases the performance of systems by 20 times for cryptographic protection on resource-constrained devices. NIST tests showed that the statistical characteristics of cryptosystems based on HCCC and CCC McEliece on GF (210) are comparable. The use of CCC allows for secure communication in wireless channels without VPN channels, which simplifies practical usage in smart city architecture. The disadvantage is the use of tunneling mode or mobile internet channel without filters and provider limitations. The proposed approach can be improved by using CC McEliece and Niederreiter with the formation of the Systematic Unit based on a desktop server.

The use of socio-cyber-physical systems with the integration of wireless and mobile internet technologies and the Internet of Things requires multi-loop information protection. CC in wireless channels and post-quantum algorithms provide security for critical CPS elements. This approach allows for considering the synergy and hybridity of threats and evaluating the overall security of CPS.

The mathematical model based on CC McEliece and Niederreiter provides confidentiality, integrity, and authenticity services. Various error-correcting codes increase the speed of information transmission and reduce energy consumption.

Implementation of security services based on algebraic-geometric and subspace codes using post-quantum algorithms McEliece and Niederreiter allows for closing the wireless channel and expanding functionality.

Земляков Р.Ю.
студент групи Н-221м ННІ ІБ СК НА СБ України
Науковий керівник:
Жевелєва І.С.
к.ю.н., доцент
доцент кафедри ОЗІОД ННІ ІБ СК НА СБ України

СТРАТЕГІЯ СТВОРЕННЯ СУПУТНИКОВИХ СИСТЕМ ДЛЯ ДОСЯГНЕННЯ НАУКОВИХ ТА РОЗВІДУВАЛЬНИХ ЦІЛЕЙ В РАМКАХ РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ СТРАТЕГІЇ РОЗВИТКУ ОЗБРОЄННЯ

Механізм комплексного забезпечення інформацією в сегментах наукових досліджень, отримання розвідувальної інформації та проведення системного моніторингу за цілями наземного, атмосферного, стратосферного та підводного базування потребує застосування комплексних систем супутникових апаратів, що орієнтовані на проведення наукових досліджень, а також реалізацію космічних розвідувальних програм. Першочерговим завданням є створення стратегії будівництва комплексів космічних апаратів, що мають цільове призначення у

відповідності до сегменту застосування, специфіки оброблюваної інформації та наявного інструментарію апаратного забезпечення[4, с. 28].

Напрямнауковихдослідженьорієнтований на реалізацію програм Державного космічного агентства України та має диверсифіковане цільове призначення. Водночас, сегмент космічної розвідки має розвиватися на платформі забезпечення Державного космічного агентства, для реалізації запитів Головного управління розвідки України, Служби безпеки України, Міністерства оборони України, що потребує використання комплексної структури космічних апаратів, цільового призначення, систем операційної інформаційної діяльності та нормативного забезпечення для створення ефективного механізму. Окремим сегментом даної структури є розробка внутрішніх стандартів збирання, обробки, зберігання та циркулювання інформації всередині супутникових систем, а також при переміщенні інформації до наземних центрів забезпечення. Важливим етапом проєктування супутникових систем є інтеграція міжнародних стандартів захисту інформації, та їх реалізація у внутрішніх сегментах систем космічних апаратів[5, с. 114].

Дослідження процесу розробки та модернізації стратегії створення комплексних супутникових систем різного цільового призначення проводили А. Фарретті, Р. Карвальо, Х. Естела та М. Лангер.

Модернізація механізмів функціонування космічних апаратів та систем Державного космічного агентства України повинне включати формування та реалізацію трьох етапів даного процесу: визначення необхідних напрямів розширення систем національних супутникових технологій, визначення основних можливостей на напрямів диверсифікації даних технологій, а також, удосконалення існуючого забезпечення систем передачі, захисту та зберігання інформації всередині супутникових систем[4, с 42]. План розширення супутникових систем повинен складатися із сегментів структури космічних апаратів, нормативного забезпечення при інтеграції міжнародних стандартів захисту інформації, а також механізмів внутрішнього забезпеченняфункціонуваннясупутникових систем[4, с. 44].

Основою нормативного забезпечення механізму функціонування комплексу супутникових систем повинна стати Головна космічна політика, що необхідна як регулюючий документ при розробці та проведенні операційної діяльності у відкритому космосі та для узгодження політики між країнами учасницями «Договору про принципи діяльності держав з дослідження та використання космічного простору, включаючи Місяць та інші небесні тіла», що був прийнятий Резолюцією 2222 (XXI) Організації Об'єднаних Націй[6; 7].

Важливим елементом стратегії створення супутникових систем є чітка та визначена взаємодія із Європейським космічним агентством, а також Комісією Європейського Союзу та Відділом оборонної промисловості та космосу Комісії ЄС, в рамках координації технологічної стандартизації, нормативного

забезпечення та розробки механізму взаємодії у процесі виводу штучних об'єктів на орбіту Землі. Головним аспектом даної взаємодії, в рамках інтеграції України до Європейського Союзу та Організації Північноатлантичного договору, повинна стати розробка системи нормативного забезпечення в напрямках взаємодії з Європейським оборонним фондом, доєднання до Європейського ринку оборонного обладнання та забезпечення дотримання правил закупівель ЄС у сфері оборони, створення окремого Плану дій щодо військової мобільності космічних сил, сприяння політиці інтеграції інновацій та інвестицій у національну космічну галузь, розробка Національної космічної програми та юридичне закріплення прагнення України, як суверенної держави, реалізувати власний потенціал у космічному просторі[1; 2].

Інтеграція міжнародних стандартів захисту інформації, що необхідна на всіх етапах реалізації стратегії створення супутникових систем, має на меті забезпечення ефективного проходження всіх операційних процесів обробки інформації у кожному сегменті апаратного забезпечення та каналів циркулювання інформації в межах космічних апаратів, в їх комбінаціях та поза їх межами[3].

Застосування стандартів Міжнародної організації із стандартизації повинне базуватися на використанні кожного стандарту в окремому сегменті загальної системи та їх адаптація, відповідно до специфіки кожного елемента. Основою для функціонування механізму управління інформаційною безпекою супутникових систем є міжнародний стандарт інформаційної безпеки ISO/IEC 27001 2005[8].

Забезпечення управління ризиками інформаційною безпекою супутникових систем необхідно проводити на основі міжнародного стандарту захисту інформації ISO/IEC 27005 2022[9].

При розробці механізму функціонування технологій безпеки супутникових систем, необхідною складовою є також інтеграція положень міжнародного стандарту захисту інформації ISO/IEC 27002 2022[10].

Варто зробити висновок, що стратегія створення супутникових систем передбачає реалізацію цілей досягнення наукових завдань, а також, забезпечення розвідувальною інформацією та диверсифікацію військових можливостей державного оборонного сектору. Процесмодернізаціїкосмічних систем Державного космічного агентства повинен включати: визначення необхідних напрямів розширення систем національних супутникових технологій, визначення основних можливостей на напрямів диверсифікації даних технологій, а також, удосконалення існуючого забезпечення систем передачі, захисту та зберігання інформації всередині супутникових систем. Реалізація стратегії створення комплексних супутникових систем має проводитись в сегментах структури космічних апаратів, нормативного забезпечення при інтеграції міжнародних стандартів захисту інформації, а також механізмів внутрішнього забезпечення функціонування супутникових систем.

Література

1. NATO’s overarching Space Policy. URL: https://www.nato.int/cps/en/natohq/official_texts_190862.htm (дата звернення: 15.03.2023);

2. European Commission: Department of Defence Industry and Space. URL: https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/defence-industry-and-space_en (дата звернення: 15.03.2023);

3. Strategic plan: Explore NASA small spacecraft. URL: https://www.nasa.gov/sites/default/files/atoms/files/smallsatstrategicplan.pdf (дата звернення: 12.03.2023);

4. A. Farretti. Satellite InSAR Data: Reservoir Monitoring from Space (EET 9): EAGE, 2006. 160 с;

5. RogerioAtem de Carvalho, Jaime Estela, Martin Langer. Nanosatellites: Space and Ground Technologies, Operations and Economics: Wiley, 2020. 712 с;

6. Договір про принципи діяльності держав по дослідженню і використанню космічного простору, включаючи Місяць та інші небесні тіла: Міжнародний договір від 10 жовтня 1967 року Документ 995_480: станом на 15 берез. 2023 р. https://zakon.rada.gov.ua/laws/show/995_480#Text (дата звернення: 15.03.2023);

7. RESOLUTION ADOPTED BY THE GENERAL ASSEMBLY 2222 (XXI). Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies: Resolution 1967 2222 (XXI): станомна 15 берез. 2023 р.
https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/outerspacetreaty.html (дата звернення: 15.03.2023);

8. ISO/IEC 27001:2005 Information technology — Security techniques — Information security management systems — Requirements. Чиннийвід 2005-10. Вид. офіц. Geneva, Switzerland : The International Organization for Standardization, 2005. 34 с;

9. ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks. Чиннийвід 2022-10. Вид. офіц. Geneva, Switzerland : The International Organization for Standardization, 2022. 62 с;

10. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls. Чиннийвід 2022-02. Вид. офіц. Geneva, Switzerland : The International Organization for Standardization, 2022. 152 с.

Іванова Р.Д.
студентка 1 курсу магістратури спеціальності «Право»,
ННІ ІБ СК
Національної академії Служби безпеки України, (м. Київ, Україна)
Науковий керівник:
Столбовий В.М.
доктор юридичних наук, доцент,
Національна академія Служби безпеки України (м. Київ, Україна)

АКТУАЛЬНІ ПРОБЛЕМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ: ДОСВІД УКРАЇНИ ТА ІНШИХ КРАЇН

Актуальність дослідження. Одним з найбільш проблемних правових питань в еру інформаційних технологій є захист персональних даних. До того ж у світі, поглиненому глобалізацією, дані користувача однієї країни можуть використовувати треті особи з будь-якого куточка світу (в тому числі незаконно).

Ніхто з нас не уявляє кількості баз даних, де відображена інформація про нас, і місць, де такі бази зберігаються: банки, туристичні та інші агентства, інтернет - магазини, поштові служби, мобільні та інші оператори, сервіси бонусних програм і багато іншого. Практично будь-який адресний або іменний сервіс передбачає заповнення анкети з внесенням персональних даних, після чого ці дані складуються у різних базах. І далі ми не знаємо, що відбувається з ними, і часом не володіємо інформацією про вимоги законодавства до їх зберігання та свої права. Зрозуміло, що при заповненні таких анкет та укладанні договорів з сервіс - провайдерами ми надаємо згоду на обробку даних, а далі є визначені законодавством процедури їх захисту. Та на жаль, не всі вони дотримуються та виконуються, що і призводить до проблем.

Актуальність захисту персональних даних — питання, що турбує дуже багато розвинених держав, адже людина, яка знає ціну своєї особистості, в т. ч. своїх персональних даних, високо цінує своє право власності, що сприяє укріпленню прав і свобод громадян і, відповідно, економічному розвитку держави. У рамках такого захисту країни Заходу регулярно посилюють нормативні вимоги стосовно персональних даних, а також збільшують штрафи за порушення таких вимог.

Аналіз досліджень і публікацій. Забезпечення захисту персональних даних громадян посідає зараз одне з провідних місць серед актуальних викликів цифрової трансформації економіки країни. Це підтверджують численні роботи вітчизняних науковців, таких як В.М. Брижко, О.В. Гронь, О.Ю. Наливайко, А.К. Погореленко, І.М. Сопілко, А. Тунік та ін., які пропонують методологічні підходи до класифікації персональних даних, визначають актуальні проблеми захисту

персональних даних, розробляють відповідне нормативно-правове поле для використання персональної інформації в бізнес-процесах.

Мета дослідження. Визначення основних проблем захисту персональних даних на прикладі вітчизняного та міжнародного досвіду

Виклад основного матеріалу. В Україні існує законодавство, що регулює захист персональних даних, але воєнний стан може призвести до обмеження прав і свобод громадян, включаючи право на конфіденційність персональних даних.

Відповідальність за порушення правил захисту персональних даних під час воєного стану буде найбільш суворою, оскільки порушення цих прав може призвести до негайних загроз для безпеки держави та її громадян.

У разі введення воєнного стану необхідно розробити стратегію захисту персональних даних, що включає в себе плани дій щодо збору, зберігання та обробки цих даних, а також заходи щодо їх захисту від несанкціонованого доступу. Крім того, у період воєнного стану необхідно забезпечити дотримання принципів законності, обґрунтованості та пропорційності щодо обробки персональних даних, а також забезпечити доступ до цих даних відповідним органам та особам згідно з вимогами законодавства.

Одним з найбільш важливих завдань в цій області є забезпечення належного рівня свідомості громадян про їх права щодо захисту персональних даних, а також про можливі наслідки.

В Україні питання захисту персональних даних регулюється Законом України «Про захист персональних даних», який набрав чинності у 2011 році На виконання його завдань у 2012 році був створений спеціальний орган — Державна служба України з питань захисту персональних даних. Однак вже через два роки її ліквідували, а тягар захисту персональних даних поклали на Уповноваженого Верховної Ради України з прав людини та суди (далі – Уповноважений).

Велика Палата Верховного Суду сформувала принципи обробки персональних даних (відкритість і прозорість, відповідальність, адекватність, не надмірність їх складу та змісту стосовно визначеної мети обробки), а також підстави для обробки персональних даних (згода суб'єкта персональних даних).

Найпростішим прикладом, коли від особи беруть згоду обробку на персональних даних, є реєстрація на сайті. Під час такої процедури більшість осіб мало цікавить, хто і як надалі оброблятиме персональні дані. Для багатьох послуг, що надають державні органи, також отримується згода на обробку персональних даних. На жаль, запам'ятати, кому і які персональні дані надаються, а також спрогнозувати можливий витік наданих даних майже неможливо. В цьому питанні існує безліч проблем, тож пропоную зупинитися на найбільш поширених.

По-перше, текст згоди на обробку персональних даних завжди однотипний, не передбачає внесення змін та має лише одну опцію — погодитися. Непідписання такої згоди призводить до неможливості отримати необхідні послуги. Однак

потрібно зважати на те, до яких наслідків призведе надання згоди в тій чи іншій ситуації.

По-друге, особа не знає, куди та кому в майбутньому можуть бути передані її персональні дані. Зокрема, статтею 8 Закону України «Про захист персональних даних» визначено, що суб'єкт персональних даних може отримувати інформацію про умови надання доступу до персональних даних, інформацію про третіх осіб, яким передаються його персональні дані, мати доступ до своїх персональних даних і навіть відкликати згоду на обробку персональних даних.

Нещодавно стався масштабний витік персональних даних українських громадян, переважно з водійських посвідчень, тому підозра одразу впала на додаток «Дія». Через деякий час влада заперечила причетність цього додатку. Встановити дійсну причину витоку даних досі не вдалося. Однак були порушені права не тільки користувачів цього додатку, але й мільйонів інших осіб.

Як відомо, володільцем найбільшої кількості персональних даних є держава, тому саме до неї висуваються найсуворіші вимоги щодо їх збереження та уникнення поширення у випадках, коли це не передбачається згодою особи. Очевидно, що витік інформації з державних баз даних лише посилює недовіру до держави та створює відчуття незахищеності перед внутрішніми й зовнішніми загрозами. Таким чином, ми не можемо говорити про захист персональних даних приватними особами, якщо навіть державні бази даних перебувають під загрозою.

Що стосується питання захисту персональних даних в інших країнах, традиційно, найбільш розвиненою юрисдикцією вважається США. Однією з причин необхідності розвитку такого законодавства є значна кількість порушень у сфері персональних даних. У зв'язку з цим у 2020 році у штаті Каліфорнія був прийнятий новий закон про захист персональних даних. Насамперед, його важливість полягає в тому, що в Каліфорнії знаходяться такі компанії як Facebook, Google, Apple, що працюють з персональними даними користувачів по всьому світу. За невиконання вимог закону передбачені значні штрафи у кілька тисяч доларів, навіть якщо компанія порушує законодавство через необережність.

Також варто зазначити, що в Європейському Союзі у 2018 році був прийнятий Загальний регламент захисту даних (GDPR), яким встановлюються суворі вимоги до опрацювання персональних даних. Вони полягають в тому, що персональні дані мають збиратися законно, правомірно, прозоро та відповідно до цільового обмеження.

Висновки. Підсумовуючи, можна зробити висновок, що українська практика в питанні захисту персональних даних відрізняється від міжнародної набагато меншою кількістю справ, але не через відсутність порушень, а у зв'язку з низькою правовою культурою громадян щодо власних персональних даних та неефективною системою їх захисту. Варто зазначити, що сьогодні найбільш дієвим способом захисту своїх персональних даних є ретельна фільтрація, кому та з якою метою ці дані передаються. На жаль, забезпечити абсолютний захист

персональних даних наразі не може жодна держава у світі, проте особа може обмежити обсяг тих відомостей, на обробку яких вона надає згоду.

Література

1. Про захист персональних даних : Закон України від 01.06.2010 р. №2297-VI / Верховна Рада України. Офіційний вісник України від 09.07.2010 р. Офіц. вид. 2010.№ 49. С. 199.

2. Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних даних : З. Закон України №3454-VI від 2 червня 2011 р. / Верховна Рада України. Офіційний вісник України. Офіційне видання від 04.07.2011 р. 2011. № 48. С. 42.

4. Про затвердження документів у сфері захисту персональних даних. Наказ № 1/02-14 від 08.01.2014 р. Баланс. 2014, 06 бер. 2014. № 19. Ст. 5.

5. Бем М. В., Городиський І. М. Відповідальність за порушення законодавства про захист персональних даних: проблеми відповідності законодавства України вимогам регламенту Європейського Союзу щодо захисту персональних даних (GDPR). Право України. 2019. № 2. С. 237–255.

6. Посібник з європейського права у сфері захисту персональних даних. К.: К.І.С., 2020. 432 с.

Іщенко К.С.
курсант НА СБ України
Новосилецький Б.Л.
курсант НА СБ України

ОКРЕМІ АСПЕКТИ ПІДВИЩЕННЯ РІВНЯ СТІЙКОСТІ ВІЙСЬКОВОСЛУЖБОВЦІВ ДО ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ ВПЛИВІВ

Впродовж більше року повномасштабної російсько-української війни продовжуються активні заходи інформаційно-психологічного впливу рф на військовослужбовців ЗСУ та інших суб’єктів сектору безпеки та оборони. Такий стан спонукає до пошуку більш ефективних та дієвих контрзаходів, з метою захисту як власних сил оборони так і створення негативних ситуацій для ворога.

На думку директора Національного інституту стратегічних досліджень, Володимира Горбуліна: «Саме поява нових технологій надає особливу гостроту і витонченість сучасним конфліктам, у яких все частіше використовуються методи, засновані на комплексному застосуванні політичних, економічних, інформаційних та інших невоєнних заходів, реалізованих з опорою на військову силу» [1].

Інформаційно-психологічний вплив рф на особовий склад збройних формувань може мати різні форми: від пропаганди російської ідеології та геополітичних інтересів до дезінформації, психологічного тиску та дестабілізації ситуації.

Серед першочергових системних заходів слід виокремити заходи навчального характеру, зокрема доцільно проводити комплексні навчання зі збільшення обізнаності та підвищення культури інформаційної та кібербезпеки серед військовослужбовців.

Перш за все, необхідно забезпечити якісне навчання особового складу з питань інформаційної безпеки та виявлення шкідливих інформаційних впливів, дезінформацій, фейкових новин, пропагандистських вкидів тощо. Такі навчання повинні проводитись постійно, а також включати практичні заняття з реагування на інформаційні та кіберзагрози.

Друге, не менш важливе завдання - забезпечення доступу до об'єктивної та достовірної інформації. Особовий склад збройних формувань має бути ознайомлений з інформацією про те, як російські пропагандисти працюють з масовою аудиторією, та як вони можуть бути викриті. Також потрібно надавати доступ до незалежних джерел інформації, щоб уникнути спотворення фактів та забезпечити можливість аналізу інформації з різних джерел.

Це можна реалізувати наступним шляхом:

1. Джерела інформації: особовий склад збройних сил повинен бути навчений визначати джерела інформації та їх достовірність. Важливо, щоб військові мали доступ до інформації з різних джерел та могли порівнювати її для визначення правдивості.

2. Критичне мислення: критичне мислення є важливиою навичкою для аналізу інформації з різних джерел. Особовий склад збройних сил повинен бути навчений критично оцінювати інформацію на предмет достовірності.

3. Факти та докази: важливо навчити особовий склад збройних сил використовувати факти та докази для підтвердження інформації. Також важливо, щоб військові знали, як знаходити докази для оцінки достовірності інформації.

4. Огляд різних джерел: військові повинні мати доступ до різних джерел інформації для отримання більш повної картини. Важливо, щоб вони використовували різні джерела, які можуть мати різні точки зору, та уникати підходу до вибору лише тих джерел, які підтверджують їхні власні погляди.

Третє, важливо забезпечити посилення контролю за інформаційним простором та запобігання поширенню пропаганди та фейкових новин. З початком бойових дій на Сході країни військове керівництво повернулося до ідеї, яка реалізовувалася на початку 90-х: в кожному з’єднані має бути прес-служба (із 2020 року – служба зв’язків з громадськістю). Однак, досвід інформаційного протистояння, на думку дослідників, показав, що 1-2 особи штатні одиниці неспроможні адекватно реагувати на виклики і виконувати вкрай важливі

завдання нейтралізації інформаційних загроз і такі дії не показали свою ефективність [2].

Для цього необхідно використовувати сучасні технології моніторингу інформаційного простору, а також розробляти ефективні антидезінформаційні кампанії. Існує кілька способів забезпечення посилення контролю за інформаційним простором та запобігання поширенню пропаганди та фейкових новин, а також розробки ефективних антидезінформаційних кампаній серед особового складу збройних сил. Ось деякі з них:

Моніторинг інформаційного простору: Особовий склад збройних сил може бути навчений самостійно використовувати ці технології, щоб виявляти та запобігати поширенню дезінформації

Створення антидезінформаційних кампаній: Розроблення та реалізація ефективних антидезінформаційних кампаній можуть допомогти зменшити вплив пропагандистської інформації та фейкових новин на особовий склад збройних сил. У цих кампаніях можуть брати участь військові журналісти, психологи та інші фахівці [3].

Навчання особового складу: Особовий склад збройних сил може бути навчений розпізнавати та відрізняти дезінформацію від об'єктивної інформації, а також виявляти та запобігати поширенню шкідливої інформації. Навчання може проводитись як частини військової підготовки, так і у формі додаткових курсів або тренінгів.

Співпраця з медіа: Співпраця з медіа може допомогти забезпечити поширення об'єктивної та достовірної інформації, забезпечення ефективної взаємодії у сіспільстві [4].

Крім того, варто проводити регулярні психологічні тренінги для особового складу, щоб забезпечити підвищення стійкості до деструктивного інформаційного впливу. Можуть бути використані наступні підходи:

Розроблення спеціальних курсів: Спеціальні курси з інформаційної безпеки та виявлення шкідливих інформаційних впливів можуть бути розроблені для різних рівнів особового складу збройних сил. Ці курси повинні охоплювати різні аспекти інформаційної безпеки, включаючи виявлення шкідливих інформаційних впливів, критичне мислення та аналіз інформації, використання сучасних технологій для захисту від шкідливих впливів та інше.

Практичні заняття: Практичні заняття можуть допомогти особовому складу збройних сил здобути практичні навички з інформаційної безпеки та виявлення шкідливих інформаційних впливів. Наприклад, військові можуть бути навчені використовувати спеціальні програми для перевірки достовірності інформації та аналізувати її з різних точок зору.

Використання сучасних технологій: Сучасні технології, такі як відео-конференції, онлайн-курси, ігри-симулятори та інші, можуть бути використані для навчання особового складу збройних сил з питань інформаційної безпеки та

виявлення шкідливих інформаційних впливів. Ці технології можуть забезпечити доступ до навчальних матеріалів з будь-якого місця та в будь-який час.

Література

1. Бараннік В.В., Сідченко С.О., Белікова Т.В., Олійник Ю.О., (2019) Метод виявлення деструктивно інформаційно-психологічного впливу на підсвідомість особового складу та населення України DOI: 10.30748/soivt.2019.60.16

2. Інформаційно-психологічна боротьба у воєнній сфері: монографія / Г.В. Пєвцов, А.М. Гордієнко, С.В. Залкін, С.О. Сідченко, А.О. Феклістов, К.І. Хударковський. – Х.: Вид. Рожко С.Г., 2017. – 276 с.

3. Лікарчук, Н. В., & Лікарчук, Д. С. (2022). Інформаційно-психологічні війни: міжнародно-політичний аналіз. Міжнародні відносини: теоретико-практичні аспекти, (9), 157–171. doi: https://doi.org/10.31866/2616-745X.9.2022.265457.

4. Горбулін В.П. "Гібридна війна" як ключовий інструмент російської геостратегії реваншу / В.П. Горбулін // Стратегічні пріоритети. –2014. – № 4(33). – С. 5-12.

5. Хударковський К.І., Залкін С.В., Пєвцов Г.В., Пацек П., Сідченко С.О. Механізм протидії негативному інформаційно-психологічному впливу на особовий склад Збройних Сил України. *Наука і техніка Повітряних Сил Збройних Сил України*. 2020. № 1(38). С. 72-78. https://doi.org/10.30748/nitps.2020.38.08.

6. Лікарчук, Н. В., & Лікарчук, Д. С. (2022). Інформаційно-психологічні війни: міжнародно-політичний аналіз. Міжнародні відносини: теоретико-практичні аспекти, (9), 157–171. doi: https://doi.org/10.31866/2616-745X.9.2022.265457.

7. Основні особливості ознак проведення інформаційно-психологічної операції Російської Федерації в АР Крим / Г.В. Пєвцов, С.В. Залкін, С.О. Сідченко, К.І. Хударковський, А.О.Феклістов, А.В. Антонов // Наука і техніка Повітряних Сил Збройних Сил України. – 2014. – Вип. 1(14). – С. 37-39

8. Богданович В.Ю. Моделювання стратегії, орієнтованої на зміну режиму у вибраній країні-мішені через її занурення в хаос, на основі методу функціонально значимих проміжних станів / В.Ю. Богданович // Сучасний захист інформації. – 2015. – № 2. – С. 44-53.

Кисильова Є.С.
студентка ННІ ІБСК НА СБ України

ТЕЛЕГРАМ-КАНАЛИ ЯК ЗАГРОЗА НАЦІОНАЛЬНІЙ БЕЗПЕЦІ ТА ТЕРИТОРІАЛЬНІЙ ЦІЛІСНОСТІ УКРАЇНИ

Сучасна комунікативістика активно проявляє інтерес до вивчення нових інструментів медіа. Одним із сучасних форматів мас-медійної комунікації сьогодні активно виявляються публічні Telegram-канали. Як відомо, месенджер «Telegram» був створений у 2013 році Павлом Дуровим та його командою. Цей програмний продукт був задуманий як конкурент WhatsApp. У Telegram передбачено функції чатів, каналів та ботів. Спочатку користувачі використовували інструмент здебільшого для приватного спілкування, розваг, як альтернативу іншим месенджерам. Згодом політики, журналісти, фахівці інформаційних технологій почали застосовувати канали Telegram як інструмент ЗМІ – для поширення інформації, формування громадської думки.

Telegram-канали в умовах конвергентної журналістики стали одним з інструментів медіа, які дають змогу диверсифікувати донесення інформації до користувачів. Серед позитивів такої платформи – швидкість донесення інформації, лаконічність, можливість подавати мультимедійні матеріали, відносна простота, доступність та дешевизна поширення інформації через Telegram. В умовах авторитарного суспільства, як наприклад, у Білорусі, анонімність таких каналів і практична неможливість їхнього повного блокування також є перевагою інструмента. Серед негативів анонімних Telegram-каналів, на нашу думку, варто назвати суб'єктивність публікацій, наявність політичної джинси, маніпуляцій, фейкової інформації, можливість їх використання в арсеналах інформаційних воєн. Це черговий аргумент на користь підвищення медіаграмотності споживачів інформаційної продукції незалежно від каналів її передавання [1].

Месенджер Telegram – один із найпопулярніших серед українців. Основна цільова аудиторія месенджера – люди віком 18-35 роки. Їх приваблює не лише зручність, а й одна з конкурентних переваг: анонімний канал Telegram. Це внутрішні ЗМІ, які публікують різноманітний вміст від мемів до політичних і бізнес-інсайдів. Такі засоби масової інформації є дешевими у виробництві та легкими для трансляції. В ідеальному світі анонімні канали були б зайняті інсайдерами галузі, експертами та активістами, які не можуть публічно висловлювати свою думку. На практиці це створює умови для появи міні-медіа, які поширюють політичні повідомлення, які є вигідними іншим, просувають шкідливі для суспільства тенденції та атакують конкурентів.

Реалізація імперських амбіцій Російської Федерації та агресивних зовнішньо політичних цілей, спрямованих в Україну, має системний і комплексний характер, зокрема в інформаційній сфері. У нинішніх умовах не можна недооцінювати

масштаби та тенденції використання месенджерів. Особливо це стосується месенджера Telegram. На жаль, систематичне поширення останнім часом матеріалів розвідувально-підривного характеру, забороненого контенту та закликів до розпалювання міжнаціональної ворожнечі, закликів до вчинення терористичних актів, насильницької зміни чи повалення конституційного ладу, захоплення державної влади та порушення територіальної цілісності, а також прагнення політичного керівництва рф дестабілізувати суспільно-політичну ситуацію в Україні.

Негативний вплив використання Telegram-каналів на національні інтереси України може бути пов'язаний з поширенням неперевіреної або фейкової інформації, яка може спричинити соціальну напругу та порушення громадського порядку. Наприклад, в Україні було кілька випадків, коли Telegram-канали використовувалися для поширення фейкових новин, спрямованих на порушення стабільності та безпеки в країні. Крім того, Telegram-канали можуть використовуватися для організації незаконної діяльності, наприклад, протестів, що може загрожувати державній безпеці та порушувати громадський порядок. Це може включати організацію протестів, а також пропаганду антидержавних ідей і насильства.

Telegram може використовуватися для координації кібератак на національну інфраструктуру, що може завдати значної шкоди економіці та безпеці країни. Нарешті, відсутність контролю над каналом Telegram може сприяти діяльності терористичних та злочинних організацій, які можуть використовувати цю платформу для поширення пропаганди та вербування нових членів. Таким чином, негативний вплив використання Telegram-каналу на національні інтереси України є дуже значним і може включати різні загрози безпеці, стабільності та демократії країни.

У контексті поширення дезінформації, маніпуляцій та звинувачень формат анонімного каналу, ймовірно, є найбільш привабливим. Хоча Telegram має безліч функцій соціальних мереж, по суті це месенджер. В Україні анонімний канал Telegram вже є серйозним бізнесом. На ринку існують команди, які розробляють ці канали "підключ" і наповнюють їх відповідним контентом. Теми варіюються від оборонної промисловості та війни до інфраструктурних проблем столиці. Таким чином, за допомогою функціонування телеграм-каналів легко маніпулювати громадською думкою та залучати нову аудиторію користувачів. Читачам буде досить важко відстежити першоджерело та підтвердити дійсність прочитаної інформації.

Важливою складовою загальної політики забезпечення інформаційної безпеки України є підвищення участі громадськості у процесах удосконалення зв’язку “суспільство – держава”. Подальше зміцнення інформаційної безпеки країни вбачається у спільних, злагоджених діях усіх державних інституцій, громадськості, медіа-спільноти. В сучасних умовах необхідно вирішувати не лише

такі важливі завдання, як формування власного інформаційного простору та його захисту від загроз, а й переходити від захисних стратегій до наступальних [2].

Російська Федерація та її спецслужби давно проводять спеціальні розвідувальні операції, більшість з яких спрямовані на ліквідацію української нації та руйнування української ідентичності. Деструктивний контент Telegram-каналів провокує екстремістські прояви, нагнітає панічні настрої, погіршується дестабілізує суспільно-політичну та соціально-економічну ситуацію, розпалює етнічні та міжконфесійні конфлікти в Україні [3].

В Україні існує безліч анонімних Telegram-каналів, наповнених фейками маніпуляціями, іноді з явно "проросійським" слідом. Багато анонімних каналів пов'язані один з одним. Цей зв’язок можна легко простежити за репостами, згадками і рекомендаціями на каналах. Більшість анонімних телеграм-каналів у нинішніх умовах є інструментами гібридної війни проти нашої країни. Вітчизняні експерти довели, що більша частина інформації з таких телеграм-каналів є маніпульованою та фейковою. Кількість фейків і маніпуляцій в анонімних телеграм-каналах часто сягає понад 80%.

У сучасному світі цифрові технології набувають дедалі більшого значення на тлі низької медіаграмотності та цифрової обізнаності населення. Тому необхідно посилити роботу з українською громадськістю та навчати громадян медіаграмотності, щоб мінімізувати деструктивну пропаганду, яку поширюють з анонімних Telegram-каналів. Вся інформація в Telegram-каналах є не лише суб'єктивною думкою, а й часто є потенційно пропагандистською (як внутрішньою, так і зовнішньою). Тому середньо статистичному українцю необхідно фільтрувати, перевіряти та критично аналізувати всі повідомлення [3].

У ситуаціях, що склалися, видається необхідним законодавчо врегулювати діяльність мережі Telegram у національному сегменті Інтернету, зокрема, шляхом регулювання алгоритмів цієї мережі, щоб унеможливити розповсюдження особистої інформації та фейків, а також створення екстремістських груп і терористичних ідеологій. Вважається за необхідне унеможливити створення екстремістських груп терористичних ідеологій. З фейковим неналежним контентом у Telegram також слід боротися, насамперед викриваючи тих, хто публікує та розповсюджує фейки.

Література

1. Жугай В.Й., Кузнєцова Т.В. Особливості телеграм-каналів як новітніх інструментів медіа: Український контекст. URL:https://www.philol.vernadskyjournals.in.ua/journals/2021/6_2021/part_3/21.pdf

2. Солодка О.М. Пріоритети удосконалення інформаційної безпеки України *Інформація і право* с. 36-42., 2015. URL: http://www.ippi.org.ua/solodka-om-prioriteti-udoskonalennya-informatsiinoi-bezpeki-ukraini-st-36-42.

3. Гуржій С.В. Сучасні загрозливі тенденції використання Telegram-каналів на шкоду державним інтересам с. 162-169., 2021р. URL: http://ippi.org.ua/gurzhii-sv-suchasni-zagrozlivi-tendentsii-vikoristannya-telegram-kanaliv-na-shkodu-derzhavnim-intere.

Ківало А.В.
Національна академія СБ України

ВІЙСЬКОВА АНАЛІТИКА ЯК ЗАСІБ ВПЛИВУ НА ГРОМАДСЬКУ ДУМКУ

Розуміння військових аспектів забезпечення інтересів національної безпеки становить актуальне завдання в умовах російської агресії проти України. У цьому контексті важливим є дослідження впливу українських військових експертів на громадську думку. Військові експерти формують громадську думку через активну участь у телевізійних програмах або в інтернет-виданнях, де оприлюднюються їхні виступи, статті, інтерв'ю, блоги, авторські аналітичні матеріали.

Військові експерти прямо або опосередковано впливають на поведінку та настрої людей насамперед завдяки кваліфікованому роз'ясненню складних питань національної безпеки та оборони. Вони надають докладну інформацію з найбільш чутливих військово-політичних проблем, розв'язання яких потребує наша країна. Виважені міркування українських військових експертів часто поєднуються з грунтовними оцінками політичних експертів, що надає великої ваги такій інформаційно-аналітичній діяльності і нівелює спроби заангажованих російських політтехнологів і пропагандистів посіяти безлад серед військових і цивільного населення України.

Українські військові аналітики сформували свій досвід завдяки спеціальним знанням з різних галузей науки і техніки, які дають їм змогу професійно аналізувати та оцінювати ситуацію військово-політичного та безпекового характеру. Провідні українські військові експерти досконало орієнтуються в різних видах озброєнь, боєприпасів, технічних та інших військових пристроях, їхніх можливостях, кількісних і якісних характеристиках.

Слід виокремити й інші групи знань, притаманних для публічної діяльності військових експертів : геополітичні – знання про військові організації, політичну систему, економіку та культуру інших країн, здатність аналізувати і прогнозувати розвиток геополітичних процесів; регіональні – знання місцевості, на якій відбуваються бойові дії, реалізуються логістичні операції; розвідувальні – знання про методи збору та аналізу розвідувальної інформації, вміння оцінювати достовірність та актуальність отриманої інформації; спеціальні військові – знання про тактику та стратегію бойових дій, сильні та слабкі сторони противника, методи планування бойових дій; інформаційно-комунікаційні – знання важливості

інформації, уміння швидко її знаходити та аналізувати, використовуючи різні джерела. Загалом усі ці знання дають змогу українським військовим аналітикам професійно оцінювати військово-політичну та безпекову ситуацію в країні та світі, пропонувати власне бачення стратегії та тактики бойових дій.

Виділимо основні шляхи впливу військових експертів на громадську думку.

Роз'яснення складних військових питань. Аналітики допомагають громадськості зрозуміти такі питання, як рівень військових загроз для національної безпеки, особливості оборонної політики, воєнної тактики і стратегії, озброєння тощо. Це допомагає представникам громадськості бути більш інформованими щодо питань ведення війни та свідомими у прийнятті життєво важливих рішень.

Висвітлення ролі військових. Військові аналітики повідомляють про роль різних родів Збройних Сил України у забезпеченні національної безпеки та захисті країни. Це збільшує повагу до військових та їхню підтримку.

Виявлення проблем та запитів. Військові аналітики розкривають проблеми і артикулюють запити військових підрозділів на вдосконалення військової тактики і стратегії, постачання військової техніки, зброї і боєприпасів.

Поширення оптимістичних та мотиваційних повідомлень. Військові аналітики сприяють збереженню високого морально-бойового духу та конкретній підтримці українських воїнів у важкий період.

Вплив українських військових аналітиків на громадську думку може бути як позитивним, так і потенційно негативним.

Позитивним є те, що експерт своєчасно інформує громадську думку щодо різноманітних тем, пов’язаних із військом та обороною України. Аналітики надають цінну інформацію про оборонні стратегії, проблеми безпеки та інші військові теми, які корисні широкому загалу.

Водночас судження військових аналітиків, які хоч і грунтуються на різноманітних джерелах інформації, є неминуче суб’єктивними. У оцінках або висловлених твердженнях, припущеннях завжди переслідується мета, спрямована на консолідацію суспільства. З одного боку, це справді може призвести до інформаційного заспокоєння громадськості, а з іншого – до появи хибного відчуття безпеки громадян. Особливу загрозу становить використання деякими недобросовісними аналітиками своїх позицій для просування політичних завдань або корпоративних інтересів, що здатне спричинити деформації й політичне розшарування в громадянському суспільстві.

Таким чином, оскільки російсько-українська війна наразі є найважливішою темою для України і світу, вплив військової аналітики на громадську думку має значний інформаційний, політичний і соціальний ефект. Інформаційно-аналітична діяльність військових експертів заслуговує на посилену увагу майбутніх фахівців у сфері забезпечення державної безпеки в інформаційній сфері з точки зору освіти, набуття досвіду і навичок ефективних комунікацій.

Клунник М.С.
Національний університет оборони України імені Івана Черняховського

ОСОБЛИВОСТІ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В ІНТЕРЕСАХ МЕРЕЖЕЦЕНТРИЧНОЇ КІБЕРРОЗВІДКИ НАТО

Мережецентрична кіберрозвідка в кіберпросторі є проривом у сфері інформаційних технологій, що призвів до формування нових тенденцій в сфері управління Збройними Силами. Це є також перевірка в умовах реальних бойових дій нових видів зброї, розвідки, радіоелектронної боротьби, автоматизованих систем управління й зв'язку. Новітні технології вимагають від військово-політичного керівництва країн НАТО, і насамперед США, переосмислити й здійснити трансформацію теорії і практики застосування кіберрозвідки під час будівництва збройних сил, у тому числі оцінити нові тенденції в розвитку процесу управління й організації взаємодії між національними Збройними Силами при проведенні об'єднаних і коаліційних операцій.

У сучасних умовах мережецентрична кіберрозвідка в кіберпросторі виступає на передній план, оскільки саме кіберрозвідка дозволяє зв'язати між собою військово-політичні, економічні, науково-технічні, власне військові й надзвичайні фактори в умовах розширення НАТО й придання його діям глобального характеру. Прикладом тому є події широкомасштабної збройної агресії рф проти України.

На думку відомих американських експертів в області трансатлантичної безпеки й трансформації альянсу Джефрі П. Бьялоса й Стюарта Л. Коеля, "військова перевага в операціях XXI століття визначається вже не стільки кількістю танків і ракет, що перебувають на озброєнні, скільки достовірним знанням ситуації в кіберпросторі і його розумінням всіма учасниками операції (як військовими, так і невійськовими), можливостями по наданню послуг безпечного зв'язку, наявністю структур управління мережецентричною кіберрозвідкою, що функціонує на основі аналізу даних розвідувально-інформаційного забезпечення в реальному масштабі часу" [1].

Об'єктивні й суб'єктивні недоліки організації й ведення об'єднаних операцій, а також тенденції розвитку процесів управління мережецентричною кіберрозвідкою визначили необхідність реалізації ряду програм трансформації управління бойовими діями. Так, в ОЗС блоку завершується розробка концепції "Комплексні мережні можливості НАТО" (NATO Network Enabled Capability – NNEC). Ця концепція формується в рамках більш загальної концепції побудови єдиного кіберпростору (TBG) НАТО на період з 2025 по 2030 рік. Її поява безпосередньо пов'язана із процесом розробки "Нової стратегічної концепції НАТО" (Allied Joint Doctrine) і концепції альянсу "Організація й ведення об'єднаних спільних операцій майбутнього", зі створенням високоточної зброї, що

діє на нових фізичних принципах, а також з появою нових оперативно-стратегічних категорій, таких як “інформаційні операції”, “інформаційна перевага” [2].

На формування мережецентричної кіберрозвідки великий вплив зробили концепції “мережецентричної війни” (МЦВ) США й “комплексні мережні можливості” (КМВ) Великобританії. Автори концепції “мережецентричної війни” – колишній начальник управління по реформуванню ЗС США адмірал Артур Цебровськи, експерт КНШ Джон Гарстка й фахівець апарата помічника МО США Девід Альберті вважають її результатом революції, що відбувається, в управлінні бойовими діями. Концепція розроблена з метою досягнення загальної високої боєздатності, збільшення оперативності управління військами, забезпечення високих темпів проведення операції, найвищого ступеня поразки супротивника, збільшення живучості своїх ЗС і підвищення ступеня їхньої взаємодії. Внаслідок реалізації цих можливостей бойова ефективність об’єднаних оперативних формувань повинна значно зрости.

Функціональним елементом при веденні мережецентричної кіберрозвідки є високопродуктивна інформаційна інфраструктура, доступ до необхідних інформаційних ресурсів, високоточна вогнева поразка й маневр силами й засобами, ефективні процеси автоматизованого бойового управління, а також тісне інтегрування даних розвідувально-інформаційного забезпечення в процеси управління й вогневої поразки”.

Збройні сили США й провідних західноєвропейських країн використовують різну термінологію для визначення мережецентричної кіберрозвідки. Так, наприклад, командування ЗС США використовує термін “мережецентрична розвідка” (NCW – Network Centric Warfare); ЗС Великобританії – “комплексні мережеві можливості ЗС” (Network Enabled Capability – NEC); ЗС Франції – “інформаційно-центрична війна” (Info-Centric Warfare – ICW); ЗС Нідерландів використовує оперативну концепцію “мережецентричні операції” (Network Centric Operations – NCO), а командування ЗС Швеції – “оборона (захист), базована на використанні мереж зв’язку”, або “мережевий захист (оборона)” (Network Based Defense – NBD).

Таким чином, концепції мережецентрична кіберрозвідка передбачають об’єднання всіх компонентів бойового простору в інтерактивну мережу з використанням даних космічної розвідки, засобів розвідки повітряного й наземного базування, у тому числі безпілотних літальних апаратів і роботизованих бойових і допоміжних наземних платформ.

Література

1. Крутских А., Федоров А.Про міжнародну інформаційну безпеку, Міжнародне Життя, № 2, 2010.

2. Домарев В. Безопасность информационных технологий. Методология создания систем защиты: Киев, Украина: ООО “ТИД “ДС”, 2002.

Козак І.Р.
студент Національної академії СБ України

РОЗВІНЧУВАННЯ МІФУ, ЩО СЕВАСТОПОЛЬ – МІСТО РОСІЙСЬКОЇ СЛАВИ ТА МІСТО ПЕРЕМОГ РОСІЙСЬКОЇ АРМІЇ

Російська імперія постійно переписує історію, щоб показати тисячолітнє минуле «руського миру», славні перемоги російської армії. З кожної поразки росіяни намагаються вийти переможцями. Якщо ж неможливо приховати програш, то акцентують на тому, що хоч імперія програла, проте, був великий героїзм російського народу, який не можливо здолати. Яскравим прикладом є слова радянського історика Євгена Тарле, що «оборона Севастополя є дивовижним літописом про патріотизм, самовідданість військових якостей і доблесті російського народу. Тільки російський моряк і російський солдат могли створити таку разючу історичну драму, написану російською кров'ю» [1].

Міф про Севастополь, як місто «російської слави», місто «перемоги російської армії» є одним із найбільш відомим та поширених міфів російської пропаганди. Цей міф використовували усі три російські імперії для пропагандистських цілей проти власного населення, так і на міжнародній арені.

В найближчій перспективі перед ЗСУ стоятиме завдання звільнення Севастополя від російської окупації. Тому вже сьогодні потрібно порушувати питання про розвіювання вищевказаного міфу, щоб мінімізувати спротив деокупації та, у подальшому, опір проросійські налаштованих громадян Криму.

Насамперед, важливо донести до мешканців Севастополя, що «перемоги російської армії» в місті – це вигадки російської пропаганди для відвернення уваги населення від програшу в Кримській війні 1853-1856 рр., продажу Аляски американцям 1867 року, невдалої оборони Севастополя під час Другої світової війни. Після 2014 року, міф є найбільш важливим аргументом на підтримку окупації Криму, «правильного» виховання нового покоління, що повинно віддати своє життя за нову «російську імперію».

Крім того, з розпадом срср, міф використовувався для підривної роботи проти Української держави в АР Крим. Наприклад, для створення проросійських громадських та політичних рухів, для будівництва розгалуженої агентурної мережі, широкого фінансування робіт по відновленню «пам’ятників культури» та відкриття нових монументів, які показують «російську історію Севастополя». За інформацією ГУР МОУ у 2011-2012 рр., «…стається багато інцидентів, коли Росія

самовільно захоплює українське навігаційне обладнання. І це були перші ознаки, що Росія може силовим шляхом забрати об'єкти, які належать Україні. ….на території Криму йде підготовка воєнізованих груп. А 810-а бригада морської піхоти на своїх полігонах відпрацьовує питання підготовки, оснащення незаконних збройних формувань на території Криму» [2]. В кінцевому підсумку, це призвело до окупації Кримського півострова російськими військами.

На сьогодні, необхідно в інформаційному просторі зосередити увагу на зміні офіційних символів міста Севастополь - герба, прапора, гімну, які підіграють міфу та скасувати для Севастополя «спеціальний статус, який визначається законами України» [3], після завершення воєнного стану. Варто сказати, що існує необхідність створення коротких роликів про справжню історію Севастополя, який пережив не дві облоги, а п'ять: у 1854-55, 1918, 1919, 1941-42 та 1944 роках. Місто протягом п'яти облог, брали всі кому не лінь.

Важливо, провести після звільнення Севастополя деімперіалізацію та декомунізацію топонімів, розібратися з «культурними символами» російської та радянської імперій, що є місцями «поклоніння» адептів «руського миру» та лягають в основу міфу про Севастополь.

Підсумовуючи все вище сказане, можна зробити висновок, що міф про «Севастополь - місто «російської слави», місто «перемог російської армії» є відвертим перекрученням історії та інструментом пропаганди для зміцнення національної гордості суто російських громадян. Міф було побудовано на ідеях, що Севастополь завжди був під російським контролем, був «захищений» російською армією в Кримській війні, в обороні Севастополя у 1941-1942 рр., та так званої «Кримської весни» 2014 року. Оскільки, Севастополь разом з Кримом для російської імперії це «альфа та омега», майбутня деокупація Севастополя буде мати для рф катастрофічні наслідки.

Література

1. Громенко С. Севастополь – місто російської слави. Міф і викриття. *Крим.Реалії*. URL: https://ua.krymr.com/a/news/27658249.html (дата звернення: 08.03.2023).

2. Руденко А., Євчин Д., Дорогань А. Від Тузли до анексії. Чому Росії вдалося захопити Крим у 2014-му? Радіо Свобода. URL: https://www.radiosvoboda.org/a/chomu-rosiji-vdalosia-zaxopytykrym/31106434.html (дата звернення: 08.03.2023).

3. Конституція України : від 28.06.1996 р. № 254к/96-ВР : станом на 1 січ. 2020 р. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text (дата звернення: 08.03.2023).

Кристич В.А.
курсант НА СБ України

СТРАТЕГІЧНІ КОМУНІКАЦІЇ В МІЖНАРОДНИХ ВІДНОСИНАХ

Ефективні комунікації сьогодні визнаються центральними не лише для досягнення зовнішньої політики чи дипломатичного успіху, але й для реалізації будь-яких стратегічних цілей [1].

Стратегічна комунікація — це вирівнювання множинності напрямків діяльності (наприклад, реалізація політики, публічна справи, переміщення сил, інформаційні операції тощо), які разом створюють результати для підтримки національних цілей [2].

Комунікація має значний вплив на зовнішню політику як у процесі формування політики, так і на більш високому рівні, пов’язаному з взаємозв’язком зовнішньої політики та міжнародних відносин. Комунікація передбачає передачу або передачу інформації за допомогою системи символів, знаків або поведінки. Комунікація з'єднує групи; (ре)конструює контекст; і визначає, описує та окреслює варіанти зовнішньої політики.

У багатьох дослідженнях виділяють три складові стратегічних комунікацій:

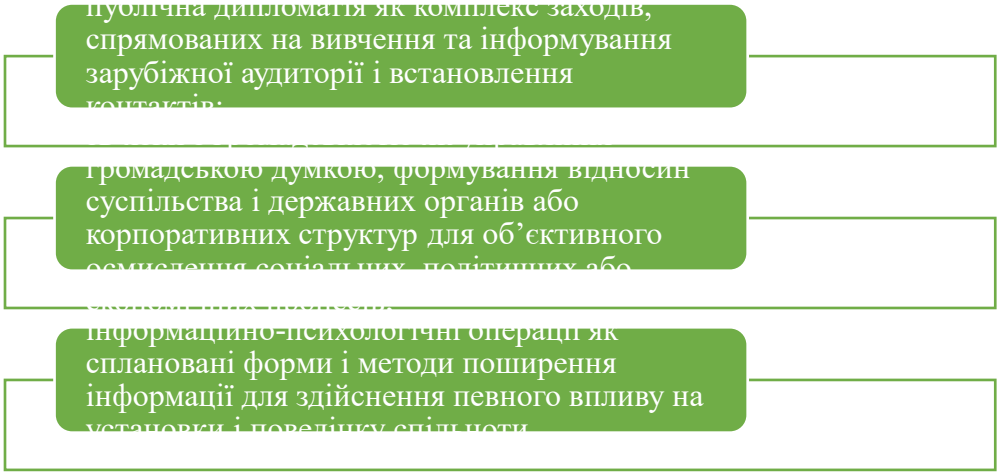


Рис.1. Три складові стратегічних комунікацій

Саме такі операції складаються з політичних, військових та ідеологічних заходів, що передбачають зміну поведінки та емоцій певних груп суспільства у потрібному напрямку. Вони можуть здійснюватися в рамках державної політики як стратегічні комунікації. В тому числі, військовий аспект координується з діяльністю відповідних підпорядкованим уряду установ.

Тобто, розуміння важливості стратегічних комунікацій для забезпечення національних інтересів, підкреслюють фахівці, сприятиме їх ефективному використанню у практиці міжнародній взаємодії [2].

Сучасні тенденції є синтезом у багатьох сферах, зосередженим на психологічних процесах, пов'язаних з тим, хто спілкується, як, з ким і з яким ефектом у сфері зовнішньої політики; і зі структурними характеристиками комунікації чи дискурсу [3].

Міжнародні політичні процеси обумовлюють також включення стратегічних комунікацій в національні програмні документи для представництва держави та активної участі у збалансованому міжнародному співробітництві.

За В.Ліпканом виділяється три основні завдання національної системи стратегічних комунікацій країни, а саме:

1. розширення сектору безпеки та оборони. Сектори маються активно розвиватися на стратегічному та операційному рівнях;
2. навчання стратегічним комунікаціям. Представники сектору безпеки та оборони країн повинні навчатися на базі двосторонніх та багатосторонніх форматів;
3. міжвідомча взаємодія. Повинна відбуватися активна взаємодія у запровадженні сучасних та прогресивних комунікативних механізмів стратегічних комунікацій.

Стратегічна комунікація завжди орієнтована на певну цільову аудиторію: її цінності, погляди, гордість та віру. Також вона невід'ємно пов'язана з управлінською ефективністю: плануванням, узгодженням та контролем. Її успіх залежить не тільки від самої комунікації, але й від ефективності діяльності організації. Виділяють основні компоненти реалізації стратегічних комунікацій (рис.2.)

Рис.2. Основні компоненти реалізації стратегічних комунікацій

У сукупності усіх даних, можна визначити, що ефективність та сучасність інструментарію стратегічних комунікацій змушує міжнародні організації до включення їх у зовнішню політику, адже комунікативні технології сприяють забезпеченню міжнародних і національних інтересів країн у цифровому світі.

Література
1. Nicholas Michelsen Mervyn Frost Strategic communications in international relations: practical traps and ethical puzzles [Електронний ресурс]. – Режим доступу: https://stratcomcoe.org/publications/strategic-communications-in-international-relations-practical-traps-and-ethical-puzzles/193
2. Paul Cornish, Julian Lindley-French and Claire Yorke Strategic Communications and National Strategy [Електронний ресурс]. – Режим доступу: https://www.chathamhouse.org/sites/default/files/r0911es%E2%80%93stratcomms.pdf
3. Foreign Policy and Communication [Електронний ресурс]. – Режим доступу: https://oxfordre.com/internationalstudies/view/10.1093/acrefore/9780190846626.001.0001/acrefore-9780190846626-e-184

Кучмєєва Ю.О.
студентка НА СБ України
Науковий керівник:
Жевелєва І.С.
к.ю.н., доцент
доцент кафедри ОЗІОД ННІ ІБ СК НА СБ України

ОСОБЛИВОСТІ ВЕДЕННЯ КОНКУРЕНТНОЇ РОЗВІДКИ У СОЦІАЛЬНИХ МЕРЕЖАХ

У сучасних умовах глобалізації та жорсткої конкуренції набуває популярності впровадження методів конкурентної розвідки в українських компаніях. Підприємства на сьогоднішній день мають можливість розвиватися та виходити на нові ринки. Але їм необхідно бути впевненими в правильності свої дій та навчитися передбачити ризикові ситуації та захищатися від конкурентів.

Під конкурентною розвідкою Т.Ю.Ткачук розуміє постійний процес збирання, нагромадження, структурування, аналізу даних про внутрішнє й зовнішнє середовище компанії та надання вищому менеджменту компанії інформації, що дає змогу йому передбачати зміни в обстановці й приймати своєчасні оптимальні рішення щодо управління ризиками, впровадження змін у компанії, а також відповідні заходи, спрямовані на задоволення майбутніх запитів споживачів та збільшення вартості компанії. [5]. Головною особливістю конкурентної розвідки є те, що вона використовує лише законні методи в своїй діяльності.

Методів конкурентної розвідки існує багато. Вони включають у себе як інформаційні (збору інформації), так і аналітичні (обробки та представлення інформації).

Метою конкурентної розвідки є: визначення дійсної стратегії конкурентів для коригування власної стратегії; визначення потенціалу конкурентів (їх сильні і слабкі сторони) для коригування власної стратегії; визначення організаційних, фінансових, технічних та інших способів забезпечення конкурентних переваг; оцінка ступеня вигідності умов співпраці з тими чи іншими постачальниками, партнерами і покупцями [2].

Функціями конкурентної розвідки є: інформаційна підтримка бізнесу на стратегічному, оперативному, тактичному рівнях; модернізація, бенчмаркінг бізнесів-процесів, технологій, товарів тощо; прогнозування в сферах розвитку ринку, технологій, товарів тощо [4].

Серед основних нормативно-правових актів якими в тій чи іншій мірі врегульовані питання щодо ведення конкурентної розвідки є: Конституція України (статті 32, 34, 50); Закон України "Про інформацію" – стаття 5; Закон України "Про національну програму інформатизації" – стаття 5; Цивільний кодекс України – статті 700, 868, 911 тощо, якими встановлюється обов'язок творців або власників інформації, яка призначена для передавання споживачам, забезпечити її об'єктивність, вірогідність, повноту і точність. Крім того, деякі питання конкурентної розвідки регулюються Законами України:. "Про державну таємницю", "Про захист інформації в автоматизованих системах" та указами Президента України і постановами Кабінету Міністрів України, присвячених регулюванню відносин у цій сфері.

У наукових працях Гарматія Н.М та Горяни О.Г.[2; 4] констатовано, що сучасні відкриті мережеві ресурси, веб-сайти, соціальні мережі перетворилися в основне джерело і ефективний інструмент для конкурентної розвідки. Вони дозволяють в режимі реального часу не тільки відслідковувати дії компаній-конкурентів, але і виявляти останні тенденції щодо необхідної тематики.

В перелік найбільших соціальних мереж, які можуть бути цікавими для ведення конкурентної розвідки в соціальних мережах, можна включити: Facebook, Google+, Linkedln, Badoo, Twitter тощо. Усі вищевказані соціальні мережі мають відношення до проведення конкурентної розвідки, оскільки мають узагальнену інформацію щодо продуктів, власників, а також можуть містити правову інформацію.

Ведення конкурентної розвідки в соціальних мережах можна розділити на 4 основні етапи: перший – визначення мети; другий – збір інформації; третій – обробка зібраної інформації; четвертий - представлення обробленої інформації [1].

Система ведення конкурентної розвідки у соціальних мережах включає такі компоненти [4] :

- комплекси контент-моніторингу інформації з відкритих мереж (веб-простору, соціальних, піринговых мереж тощо);
- засоби екстрагування понять (компаній, персон, подій тощо) з повнотекстових документів;

- засоби виявлення та візуалізації інформаційних зв'язків, виявлення аномалій, неочевидних закономірностей;

- засоби формування аналітичних документів, які надаються особам, які приймають рішення .

Змістовна частина, інформаційна база інформаційно-аналітичної системи конкурентної розвідки формується комплексом контент-моніторингу. За допомогою комплексів контент-моніторингу в рамках конкурентної розвідки, як правило, вирішуються такі завдання [1]:

- моніторинг діяльності партнерів, конкурентів, регулювальних органів;
- контроль медіаприсутності та медіаактивності учасників ринків;
- знаходження інформації про учасників ринків;
- виявлення нових продуктів на ринках;
- виявлення нових гравців на ринках;
- організація ретроспективного інформаційного фонду документів для їх подальшого використання в аналітичній діяльності.

Процес перетворення сирих даних на знання і доведення їх до кінцевих споживачів заведено називати розвідувальним циклом.

У своєму класичному розумінні розвідувальний цикл (розвідцикл) заведено розділяти на п'ять основних етапів[2] :

- цілевказування, планування, визначення джерел інформації;
- збір, добування даних;
- обробка розвідувальних даних (розвідданих) - перетворення їх на розвідувальну інформацію;
- аналіз і синтез розвідувальної інформації - перетворення її на знання - висновки, рекомендації, рішення;
- доведення інформації до кінцевих споживачів

Відмітитимо, що найважливішим елементом успішного проведення заходів конкурентної розвідки є моніторинг соціальних медіа За допомогою соціальних медіа можна дізнатися найбільш повну інформацію про аудиторію товару або послуги, її думку про роботу компанії.

Виділяють сім різновидів соціальних медіа, це: соціальні мережі; блоги; форуми; сайти відгуків; сервери фото- та відеохостингу; віртуальні служби знайомств і геосоціальні мережі. Слід зазначити, що чітких меж між цими різновидами немає.

Для удосконалення конкурентної розвідки у соціальних мережах пропонується застосувати технології проведення конкурентної розвідки на основі відкритих джерел (англ. Open source intelligence, OSINT), оскільки вони дозволяють отримати якнайбільше потрібної інформації у короткий термін та витрачаючи щонайменше ресурсів (існує достатня кількість безкоштовних інструментів OSINT), що є досить важливим в умовах воєнного стану. До їх переваг можна віднести доступність різноманітних джерел інформації, а також

обсяг її масивів, різносторонність інформації, велику кількість існуючих технік, методик і технологій. Кінцевим результатом OSINT завжди є певні знання, отримані у результаті висновків з отриманої інформації

Для наглядного представлення результатів конкурентної розвідки рекомендується застосовувати елементи інфрографії (креслення, малювання, відтворення, копіювання, фотознімки, малюнки, діаграми, гістограми, мапи, схеми, графіки та ін).

Підсумовуючи вищезазначене слід відмітити, що в умовах сьогодення, коли Україна відстоює свою незалежність борючись із доволі сильним та підступним ворогом, ведення конкурентної розвідки, у тому числі і соціальних мережах, набуло певних особливостей. Відмічається широке поширення державно-приватного партнерства, коли приватні компанії та окремі фахівці, які раніше спеціалізувались на проведенні конкурентної розвідки почали допомагати сектору безпеки та оборони України, спрямувавши свої знання уміння та навички на благо своєї держави. З огляду на зазначене можна спрогнозувати, що в повоєнні часи відбудуться певні трансформації в особливостях ведення конкурентної розвідки в нашій державі.

Література

1. Гарасим М.П., Сайко Л.Я., Необхідність інформаційних систем і технологій в управлінні підприємством URL: http://ena.lp.edu.ua:8080/bitstream/ntb/12500/1/62_327332_Vis_722_menegment.pdf (дата звернення: 19.03.2023).

2. Гарматій Н.М. конкурентна розвідка: чинник успіху підприємства. URL: http://intkonf.org/garmatiy-nm-konkurentna-rozvidkachinnik-uspihu-pidpriemstva/ (дата звернення: 19.03.2023).

3. Гончарук О.В. Стан і перспективи розвитку підприємств поліграфічної промисловості в Україні та світі. Молодий вчений, 2018р. № 1 (53). С 864-868. URL: http://molodyvcheny.in.ua/files/journal/2018/1/201.pdf (дата звернення: 19.03.2023).

4. Горяна О.Г. Система управління інформаційною безпекою на підприємстві. URL: http://ir.nmu.org.ua/bitstream/handle/123456789/1876/SUIB.pdf?Sequence=1&isallowed=y. (дата звернення: 19.03.2023).

5. Ткачук Т.Ю. Конкурентна розвідка. Навчальний посібник. Київ. 2013. 295 с. URL: https://studfile.net/preview/5065393/ (дата звернення: 19.03.2023).

Кудрявцева Н.О.
Юрист

ВЕРИФІКАЦІЯ КОНТЕНТУ ЯК ЕЛЕМЕНТ ЕФЕКТИВНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ

Відповідно до Стратегії інформаційної безпеки [1] інформаційна безпека України – це складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації**, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів** (виділ – авт.)**,** у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом (розділ «Загальні положення» Стратегії).

Незважаючи на те, що глобалізація в інформаційному просторі відбулася уже давно, проте як зазначається в розділі «Аналіз загроз та викликів інформаційній безпеці» Стратегії від грудня 2021 року, ефективна система реагування на дезінформаційні виклики в Україні досі не створена, не забезпечено функціонування розвиненої національної інформаційної інфраструктури, що обмежує можливість належним чином протидіяти інформаційній агресії з метою захисту національної безпеки та реалізації національних інтересів України.

З огляду на те, що обсяг інформації, якою володіє людство (як правдивої так і недостовірної) щодня збільшується в геометричній прогресії, то цілком логічно буде стверджувати, що кількість інформаційних загроз, що і можуть прямо чи опосередковано завдати шкоди інтересам держави, її національній безпеці та обороні, також пропорційно зростає. Зважаючи на те, що ресурси будь-якої діяльності, в тому числі й управлінської, є обмеженими, то в даному випадку, ефективність управління інформаційною безпекою більшою мірою залежить насамперед не від кількості здійснення державою дезінформаційних компаній, а від можливості встановлення контролю за змістом контенту, що поширюється в інформаційному полі.

Так, в умовах сьогодення, коли інформаційні мережі та віртуальна взаємодія по суті займають більшу частину часу пересічного громадянина, ефективне стримування та протидія загрозам інформаційної безпеки України, нейтралізація інформаційної агресії можливі виключно через запровадження відритого і прозорого механізму роботи інформаційного простору в цілому. У даному випадку йдеться про необхідність застосування таких понять як структурування,

категорування інформації, верифікація контенту інформаційного простору загалом.

Верифікація (пізньолат. *verificatia* – підтвердження; лат *verus* – істинний, *facio* – роблю) – це доказ того, що вірогідний факт або твердження є істинним [2]. Верифікація інформації може здійснюватися через перевірку джерел поширення інформації, перевірку викладених фактів, перевірку дат публікації інформації, перевірку контексту тощо. Загальноприйняті способи верифікації контенту є досить масивними, довготривалими і не завжди доступними. Переважна більшість користувачів інформаційного простору прагнуть отримати інформацію одразу без здійснення її критичного опрацювання чи перевірки. Якщо ж і трапляються такі, хто здійснюють верифікацію інформації, то вони ж є або працівниками фактчекінгових організацій або припиняють верифікацію контенту, знайшовши подібну за змістом в інших джерелах публікацій.

Оглядовий аналіз змісту інформації (включаючи коментарі під дописами публічних осіб, віртуальне обговорення представниками громадськості суспільно важливих тем), свідчить про те, що у більшості випадків авторство поширеної інформації, а отже її достовірність і відповідальність за таке поширення, в тому числі й якщо вона була розповсюджена шляхом репосту, встановити неможливо. Більше того, якщо автор публікації й відомий, для підняття своїх рейтингів прочитання, формально йому дозволяється застосовувати різні способи маніпулювання свідомістю громадян. Так, для прикладу, інформація, що є думкою автора, часто подається з високою долею ймовірності як загальновідомий факт. Зазначене, безумовно, має значний вплив на свідомість недосвідченого користувача інтернет-контентом і залежно від мети використання такої інформації в подальшому може становити додаткову загрозу національній безпеці України в інформаційній сфері.

Система управління інформаційною безпекою держави буде ефективною лише за умови встановлення контролю за змістом інформації, що створюється автором чи розповсюджується іншими особами. Мова не йде про запровадження цензури чи порушення свободи слова, права на самовираження громадян, а розглядається лише як варіант можливого застосування окремих шаблонів чи приміток до інформації, що поширюється в інформаційному просторі. Так, для прикладу, офіційна інформація державних органів чи їх публічних осіб повинна бути достовірною, чіткою, оперативною і не містити жодного емоційного забарвлення поданого тексту, гіперпосилання на таку інформацію у разі її поширення повинні бути обов’язковими, щодо поширення інформації не публічними особами, то доцільним було б обов’язкове запровадження до інформації, що подається, окремих авторських уточнень по тексту на кшталт «виключна думка автора», «загальновідомий факт», «офіційна інформація (з обов’язковим посиланням на текст публікації державного органу, публічної особи чи компанії)», «достовірність інформації та її джерело невідома» тощо. Безумовно,

запропонована модель умовного категорування інформації зробить контент викладеного менш цікавим і захоплюючим, проте більш відкритим, інформативним та достовірним. Крім того, такий алгоритм верифікації контенту дозволить перевірити джерело інформації та факти, що в ній викладені, а також сприятиме зменшенню рівня дезінформації в інформаційному просторі держави.

Вважаємо, що запропонований у публікації механізм верифікації інформаційного контенту належним чином дозволить створити систему раннього виявлення прогнозування та запобігання інформаційним загрозам, а також сприятиме посиленню спроможностей держави щодо забезпечення безпеки держави, її інформаційного простору, стабільності, оборони держави та загальному забезпеченню прав та свобод громадян.

Література

1. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки":Указ Президента України від 28.12.2021 № 685/2021 URL: http://zakon.rada.gov.ua/laws/show/685/2021 (дата звернення: 17.03.2023).

2. Верифікація. URL: http://uk.m.wikipedia.org (дата звернення: 17.03.2023).

Легкоконець В.О.
Національна академія Служби безпеки України

МЕДІАЛІНГВІСТИКА: СУТНІСНИЙ ВИМІР У ПАРАДИГМІ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

Від початку гібридної агресії рф проти України з 2014 року у вітчизняному безпековому середовищі актуалізувалося питання загроз інформаційного характеру. У зв’язку з цим гостро постала проблема розробки інноваційних інструментів протидії гібридним загрозам, у тому числі шляхом забепечення розвитку інформаційної грамотності та медіалінгвістичних компетенцій громадян.

За даними фахівців Центру стратегічних комунікацій та інформаційної безпеки при Міністерстві культури та інформації, на сьогодні модель російської пропаганди має 5 характерних рис:

- Наративізація
- Швидкість, безперервність та повторюваність
- Відірваність від об’єктивної реальності
- Відсутність послідовності
- Великий обсяг і мультиканальність [1].

Також, зазначені фахівці вважають, що медіаосвіта громадян є одним з етапів боротьби з ворожим інформаційним впливом на державному рівні.

Кожного дня російська пропагандистська машина запускає в інформаційний простір безліч меседжів деструктивного характеру, що мають на меті підрив довіри населення України до державних та безпекових інституцій, поширення паніки в середовищі та дестабілізацію внутрішніх настроїв і, як наслідок, національної стійкості.

У зв'язку з ситуацією, що склалася в українському безпековому середовищі, постає доцільним запровадження низки заходів, що будуть пов'язані з розвитком медіаграмотності, інформаційної грамотності з метою запобігання деструктивному впливу російських фейків, дезінформації та маніпуляції на суспільну свідомість українського народу.

Канадський науковець і президент Канадської асоціації медіаосвітніх організацій Джон Панджente (John J. Pungente) виділяє вісім ключових рівнів медіаграмотності:

- осягнення основних положень (розуміння, що це відбувається не з ним/нею);
- усвідомлення мови (розпізнавання мовного звучання та ототожнювання значень слів);
- усвідомлення викладеної інформації (відрізнення вигадки від того, що може бути в реальності, вирізнення реклами тощо);
- розвиток скептицизму (оцінювання можливої брехні в рекламі, чітке розуміння, що подобається, а що ні, здатність побачити смішне в некомічних героях);
- інтенсивний розвиток (потужна мотивація до пошуку конкретної інформації, вироблення чітких наборів інформації, якій надається перевага, високий рівень розуміння корисності здобутої інформації);
- емпіричне вивчення (пошук різних форм подання контенту та переказів, пошук сюрпризів і нових емоційних, моральних реакцій та почуттів);
- критичне оцінювання (сприймання повідомлень такими, якими вони є, й подальше оцінювання їх у відповідному середовищі, глибоке й детальне розуміння історичного, економічного та художнього контекстів систем, представлених у повідомленні, здатність помічати нюанси в поданні інформації та відмінність від форми подання інших повідомлень на цю ж тему, здатність зробити висновки про сильні та слабкі сторони повідомлення);
- соціальна відповідальність (розуміння, що певні повідомлення більш позитивно впливають, ніж інші; усвідомлення, що чиясь думка впливає на суспільство, й не важливо, як сильно; визнання, що існують певні способи, завдяки яким особистість може конструктивно вплинути на суспільство) [2].

Війна з рф, у тому числі в інформаційному просторі, дає підстави стверджувати, що базові знання з медіаграмотності необхідні у кожній сфері життєдіяльності українця, тож на сьогодні можна виділити такі ключові елементи медіаграмотності:

- Розвиток критичного мислення при сприйнятті інформації, вміння критично інтерпретувати повідомлення в медіа;
- відповідальне споживання, створення та розповсюдження контенту;
- вміння аналізувати контент у мережі на наявність дезінформаційного змісту;
- наявність базових навичок лінгвістичного аналізу, з метою розпізнавання лінгвістичних маркерів та наративів ворога, що можуть нести потенційну небезпеку для споживача інформації.

З огляду на викладене та з урахуванням загроз, що постійно виникають в інформаційному просторі, можна зробити висновок про необхідність використання системи медіаосвіти як фундаментальної складової інформаційної безпеки України, що сприятиме протидії інформаційній агресії, а також розвитку і консолідації громадянського суспільства.

Література

1. «Гібридна війна Росії проти України. Як перемогти на інформаційному фронті»: аналітичний посібник / команда центру стратегічних комунікацій та інформаційної безпеки; За редакцією команди Центру демократії та верховенства права. Київ: 2023. 56 с.

2.Медіаосвіта та медіаграмотність: підручник / Ред.-упор. В. Ф. Іванов, О. В. Волошенюк; За науковою редакцією В. В. Різуна. Київ: Центр вільної преси, 2012. 352 с.

Личик В.В.
аспірант, асистент кафедри Інформаційної безпеки НН ФТІ НТУУ
Київський політехнічний інститут імені Ігоря Сікорського
Гальчинський Л.Ю.
к.т.н., доцент кафедри Інформаційної безпеки НН ФТІ НТУУ
Київський політехнічний інститут імені Ігоря Сікорського

НЕОБХІДНІСТЬ ПОШУКУ РІШЕННЯ КОМПЛЕКСНОГО ПІДХОДУ ДО ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ ОБ’ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Останні події в Україні та світі викликали гостре питання здатності об'єктів та організацій критичної інфраструктури досягати запланованого рівня безпеки,

незважаючи на кібервпливи та недостатність ресурсів. Забезпечення кіберстійкості відіграє надзвичайно важливу роль для цілих секторів промисловості, IT-систем та, як показала сучасна гібридна війна – для життєдіяльності цілих держав. Зокрема, кібератаки в енергетичному секторі впливають не лише на сам сектор, але й на економіку в цілому та всю структуру держави, як на соціальну, так і на організаційну.

Для початку потрібно розглянути термін «кіберстійкість» (з англ. - Cyber Resilience). Кіберстійкість - це здатність організації забезпечити розвиток діяльності (стійкість підприємства) за рахунок готовності до кібер-загроз, можливості реагування на них, засобів відновлення після кібератак [1]. Кіберстійка організація (об’єкт) здатна адаптуватися до відомих та невідомих криз, загроз, несприятливих факторів, викликів та здатна забезпечити мінімізацію шкоди від потенційних атак/ризиків. У кінцевому підсумку кіберстійкість дозволяє підприємству підтримувати рівень розвитку за умов негативних чинників (кризи, пандемії, фінансових проблем, військових дій, тощо.)

Хоч і поняття кіберстійкості виникло відносно нещодавно, науковці та дослідники змогли створити не тільки певний термінологічний апарат для цієї предметної області, але і також конкретні підходи та парадигми, на основі яких можна оцінювати рівень забезпечення кіберстійкості. В ході досліджень та пошуків було зроблено висновок, що найбільш узагальнюючим прикладом до розробки цілісної моделі кіберстійкості для критичної інфраструктури можна вважати парадигму Prevention-Response (профілактика-реакція), запропоновану Річардом Баскервілем та Паоло Спаньолетті [2]. Також було визначено, що концепція стійкості серед експертів із безпеки тісно пов'язана з ризиками, а не загрозами. Тобто акцент змістився із запобігання, стримування та захисту від загроз на пом'якшення наслідків від інциденту.

Що стосується характеристик, що використовуються для описання природи стійкості є:

- Надійність – стійкість системи чи її окремого компонента;
- Надлишковість – рівень взаємодії системи чи її окремого компонента;
- Винахідливість – можливість направляти ресурси на підтримку системи;
- Швидкість – своєчасне відновлення після інциденту.

В свою чергу у результаті досліджень та аналізу матеріалів було виявлено п’ять основних систем для оцінки кіберстійкості:

- Метрика групи І. Лінкова (Resilience metrics for cyber systems) [3];
- Фреймворк для оцінки кіберстійкості, розроблений всесвітнім економічним форумом [4];
- Стандарти Агентства Європейського для мережевої та інформаційної безпеки (European Union Agency for Network and Information Security (ENISA) Standards);

- Платформа для підвищення рівня кібербезпеки критично-важливої інфраструктури (Національний інститут стандартів і технологій (NIST)).
- Методологія дослідників американської неприбуткової організації Корпорація Mitre (стилізована як The MITRE Corporation і MITRE)

Жодна з цих систем на даний час не стала домінуючою і необхідні додаткові дослідження, щоб оцінити переваги чи недоліки кожної з них. Проте виходячи з певних спільних рис цих систем оцінювання можна зробити деякі попередні висновки. Так, орієнтуючись на метрику І. Лінкова та його колег по Університету штату Арізона та Центру інженерних досліджень і розробок армії США орієнтиром у побудові моделі кіберстійкості є виділення чотирьох областей: фізична; інформаційна, когнітивна та соціальна.

Які в свою чергу мають підтримуватись циклом управління подій та інцидентів для забезпечення кіберстійкості. Цикл складається з:

- Планування та підготовка;
- Поглинання;
- Відновлення;
- Адаптація.

Що стосується українських реалій, то пропонується взяття за основу не певного стандарту чи метрики для оцінки рівня кіберстійкості об’єкту чи системи, а знаходження релевантного комплексного рішення з можливістю забезпечення проміжних етапів безпеки. Це потрібно для уникнення спотворення результуючої моделі на користь конкретної структури, щоб забезпечити створення гнучкої моделі, яку можна вдосконалити в майбутньому (так як певні стандарти з часом змінюються, що є громістким процесом для організацій державного сектору). Перші спроби адаптації зазначених підходів для українських об’єктів критичної інфраструктури показали принципову можливість практичного застосування[7].

Зокрема Фреймворк Шотландського державного сектору, представлений у 2021-му році включає в себе вже існуючі стандарти (наприклад, NIS та ISO27001) та має три рівні (етапи) розвитку, які собою являють прогресивні рівні забезпечення.

- «Базовий» рівень (Initial baseline): забезпечивши даний рівень, організації зможуть протистояти більшості кібер-загроз.
- “Цільовий” етап (Target): охоплює вимоги відразу певного набору стандартів, що дасть змогу організаціям пом’якшувати наслідки від кібервпливів.
- “Просунутий” етап (Advanced): підтримка NIS-CAF та ISO-27001 для охоплення комбінованих вимог. Досягнення даного етапу дасть змогу пом’якшити наслідки від складних постійних кібер-атак, які можуть нести безпосередню шкоду для життєво необхідних послуг, даних або ресурсів, які є на великих індустріальних об’єктах критичної інфраструктури.

Просування по рівнях забезпечується у досягенні прогресу у об'ємному переліку категорій, які представлені у 4-х окремих секціях (доменах):

- Керування (Manage);
- Захист (Protect)
- Виявлення (Detect);
- Реагування та відновлення (Respond and recover).

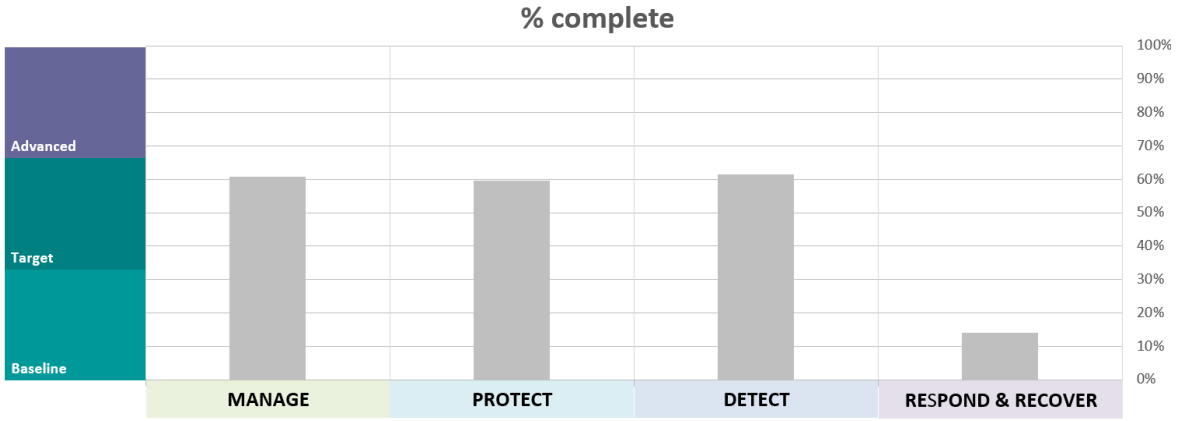


Рисунок 1 – Демонстраційна діаграма відношення виконання вимог кожного домену для забезпечення певного рівня кіберстійкості

Література

1. Björck, Fredrik; Henkel, Martin; Stirna, Janis; Zdravkovic, Jelena (2015). Cyber Resilience - Fundamentals for a Definition. Advances in Intelligent Systems and Computing. Vol. 353. Stockholm University. pp. 311–316.

2. R. Baskerville, P. Spagnoletti, and J. Kim, “Incident-centered information security: Managing a strategic balance between prevention and response,” Inf. Manag., vol. 51, no. 1, pp. 138–151, Jan. 2014.

3. Igor Linkov, Daniel A Eisenberg, Kenton Plourde, Thomas P Seager, Resilience metrics for cyber systems December 2013 Environment Systems and Decisions 33(4) DOI:10.1007/s10669-013-9485-y

4. World Economic Forum (2016a) A framework for assessing cyber resilience. URL – http://bloustein.rutgers.edu/wp-content/uploads/2016/05/2016_WEF.pdf

5. Brand, F. S., and K. Jax. 2007. Focusing the meaning(s) of resilience: Resilience as a descriptive concept and a boundary object. Ecology and Society 12(1): Article 23.

6. Bodeau D, Graubart R, McQuaid R, Woodill J (2018) Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring: Enabling Systems Engineers and Program Managers to Select the Most Useful Assessment Methods. (The MITRE Corporation, Bedford, MA), MITRE Technical Report

7. Харламова, К., & Гальчинський , Л. (2022). ОЦІНЮВАННЯ КІБЕРСТІЙКОСТІ ОБ’ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ. Collection of Scientific Papers «SCIENTIA», (November 11, 2022; Vilnius, Lithuania),

118–120. Retrieved from https://previous.scientia.report/index.php/archive/article/view/545TR-180314.

Макарук С.М.
курсант
Навчально-наукового гуманітарного інституту
Національної академії Служби безпеки України

ІНСТРУМЕНТИ ВЗАЄМОДІЇ ВЛАДИ І НАСЕЛЕННЯ В ДАВНЬОРУСЬКІ ЧАСИ (V – СЕРЕДИНА XI СТ.). СТАНОВЛЕННЯ КУЛЬТУРИ МАСОВИХ ЗІБРАНЬ І ПОВІДОМЛЕНЬ

Комунікація дає початок усім первинним устроям, справам, формуванням. Це процес двостороннього обміну інформацією, що веде до взаємного розуміння. Саме з неї розпочинається побудова відносин та вирішення проблем, що , безумовно, торкається проблеми становлення держави, взаємодії влади і населення. Комунікація - фундамент для створення суспільства.

Для кращого розуміння багатьох процесів сучасності, варто розглянути з чого все розпочиналося, як утворювалися народи та формувалися держави. На основі тих засобів комунікацій будується багато сучасних взаємовідносин, тільки удосконалені часом та підковані досвідом. Цю інформацію варто знати й для загального розвитку, щоб бути всебічно обізнаним і орієнтуватися в часі і просторі, знати, звідки з'явилися певні явища у суспільстві. Оскільки на комунікації побудовано все наше життя, то варто знати, що таке комунікація, які є комунікативні засоби та яку роль вони відіграли у створенні народу, перших держав та взаємодії влади з народом. Ми вже з'ясували, що Комунікація - процес двостороннього обміну інформацією, що веде до взаємного розуміння, а засіб спілкування - спосіб передачі інформації.

V ст. - період, коли на території сучасної України, почала формуватися держава, перші взаємовідносини з іншими державами, перший устрій та влада. Звичайно, що засоби комунікацій лише формувалися та створювали підгрунття для подальшого удосконалення.

В давні часи люди використовували різні засоби комунікації, які допомагали їм обмінюватись інформацією та ідеями, будувати відносини та вирішувати різні проблеми. Ці засоби були дуже різноманітними, і використовувалися в залежності від того, яка була потреба. Зокрема, це можуть бути:

1. Усна мова: Основним засобом комунікації в давньоруських часах була усна мова. За допомогою неї передавалися інформація, історії, легенди та традиції, які спершу існували між родами, плем'ями, а потім поширювалися по території.

2. Писемна мова. Існували різні форми писемності, такі як глаголиця, кирилиця та рунічна абетка. Ці засоби використовувалися для написання літописів, байок, легенд, листів, договорів, та інших текстів. Наприклад:

“На підтвердження ж і непорушність [миру, що має] бути межи вами, християнами, і [нами], руссю, цей мирний договір учинили ми, [руси], і ви, оба [цесарі], новим написанням на двох хартіях...” [1]

3. Жестова мова була важливим засобом комунікації для людей з обмеженими можливостями або для тих, хто не міг використовувати усну мову. Жести та міміка використовувалися для передачі різних ідей та інформації. Зрозуміло, що жести широко використовувалися в повсякденному житті.

4. Посланці. У давньоруські часи відправлялися посланці, які передавали важливі повідомлення та документи від одного місця до іншого. Цей засіб комунікації був дуже важливим для державних та політичних відносин.

“У рік 6420 [912]. Послав Олег мужів своїх налагодити мир і укласти договір межи Греками і Руссю” [1]

“Великий княз русьский и бояре его, да посилают в Греки к великим царем греческим корабли, елико хотят, с посли своими и с гостьми” [2]

5. Символіка була дуже важливою для передачі різної інформації. Наприклад, герби, прапори та інші символічні знаки використовувалися для визначення належності до певної держави або роду, що давало змогу розпізнати князя чи військо.

6. Художній мовлення. У давньоруській культурі були поширені різні жанри художньої літератури, такі як лірика, епіка, драма, фольклорні та міфологічні тексти. Ці жанри використовувалися для передачі різних ідей та інформації, а також для розваги. Особливими є билини новгородського та київського циклів (Добриня Никитич, Ілля Муромець, Альоша Попович, Садко та інш.).

7. Ритуали та церемонії були дуже важливими для спілкування та передачі інформації. Наприклад, церковні обряди передавали релігійні ідеї та традиції, а воєнні церемонії могли вказувати на важливі події та рішення.

8. “...и сказал Олег Аскольду и Диру: «Не князья вьі и не княжеского рода, но я княжеского рода», а когда винесли Игоря, добавил: «Вот он смн Рюрика». И убили Аскольда и Дира...”[3]

9. Мистецтво використовувалося не лише з творчої сторони, а й для комунікації та передачі ідеї. Наприклад, ікони та фрески могли вказувати на релігійні традиції та вірування, а різноманітні ремесла та вироби могли передавати інформацію про культурні традиції та спосіб життя. Це донесло до сьогодення інформацію про спосіб життя людей того часу.

10. Мова тіла була дуже важливим засобом комунікації. Наприклад, рухи та жести можуть передавати різні емоції та інформацію про ставлення до іншої людини. Зрештою, для сьогодення рухи теж є важливим чинником.

11. Книгодрукування. У давньоруських часах книгодрукування не було, але рукописні книги та пергаменти були дуже важливими засобами передачі інформації та збереження знань. До сьогодні відомі різні літописи, наприклад; “Повість минулих літ” , ”Слово о Полку Ігоревім”, “Слово про Закон та Благодать", "Житіє Феодосія Печерського" та інш.

12. Торгівля була важливим засобом комунікації у давньоруських часах. Вона дозволяла людям з різних регіонів спілкуватися, обмінюватися товарами та ідеями, а також встановлювати соціальні та економічні зв'язки.

Із спогадів Ібн-Фадлана про асортимент товарів руських купців (20-ті рр. X ст.): “Я видел Русов, когда они пришли со своими товарами... Каждьій из них имеет при себе неразлучно меч, нож и сокиру [...], ... каждьій из них выходит, имея с собою хлеб, мясо, молоко, лук и горячий напиток”[2].

13. Інформаційні вісники передавали важливу інформацію та новини. Наприклад, боярські листи передавали важливі повідомлення від князів та бояр, а купецькі книги містили інформацію про торгівлю та економіку.

14. Музика передавала історії та традиції різних регіонів, а церковна музика допомагала передати релігійні ідеї.

15. Технічні засоби: У давні часи були створені різні технічні засоби, які допомагали людям обмінюватись інформацією та комунікувати. Наприклад, це можуть бути дзвони, дзвіниці, гончарні вироби, які мали символічні значення та використовувалися для передачі повідомлень або сигналізації про небезпеку. Також в давні часи використовувалися торгові шляхи, які допомагали зв'язувати різні регіони та країни і встановлювати контакти з іншими культурами та народами.

Одним з прикладів удосконалення комунікації між владою та народом є Культура масових зібрань та повідомлень. Вона почала формуватися в давньоруські часи з появою різноманітних великих заходів, таких як релігійні свята, ярмарки, збори і наради.

Наради та збори також були важливими подіями для розповсюдження інформації та прийняття важливих рішень. Ці збори можна було проводити на різних рівнях, від найменших сільських нарад до зборів у великих поселеннях чи містах та на рівні державних зборів.

"Новгородци бо изначала, и смоляне, и кыяне и полочане и вся власте яко-же на думу на вече сходятся..." (Лавр, 1176 р.).

987 р. "созва Володимер бояры своя и старцы градские"(для ознайомлення з різними релігіями).

"Й бысть люба речь (их) князю и всем людям" (Лавр, 987 р.).

Загалом, становлення культури масових зібрань та повідомлень в давньоруські часи було досить складним та тривалим процесом. Це пов'язано з тим, що відсутність сучасних технологій та засобів комунікації зумовлювала потребу у створенні спеціальних форм зборів та повідомлень, які були

ефективними для взаємодії між людьми.

У цілому, дієвість комунікативних технологій в давньоруські часи залежала від рівня розвитку суспільства, доступності інформації та технологій для її передачі та сприйняття. Це дало хороший початок для наступних поколінь. В той час, було розроблено декілька дієвих комунікативних технологій, які були використані для вирішення соціальних, політичних, релігійних та економічних проблем. Однак, в порівнянні з сучасними технологіями комунікації, вони були обмеженими і менш дієвими. Але варто пам'ятати, що це були давні часи і перші спроби створення держав та взаємодій народу з владою.

Література

1. Літопис руський. Київ, 1989. С. 20-22.

2. Відома і чута в усіх кінцях землі. Друга половина IX — перша половина XII ст. Київ, 1993. С. 287.

3. Історія України: Хрестоматія / Упоряд. В. М. Литвин; Відп. ред. В. А. Смолій. НАН України. Інститут історії України, Київ: Наукова думка, 2013.

Миколаєнко Ю.О.
студентка ННІ ІБСК НА СБ України
Козюра В.Д.
кандидат технічних наук, доцент
Національна академія Служби безпеки України

ШЛЯХИ ВПРОВАДЖЕННЯ ПРОГРАМНИХ ЗАКЛАДОК В КОМП'ЮТЕРНІ СИСТЕМИ

Програмні закладки – це потайливі (недокументовані) можливості програмного та апаратного забезпечення комп'ютерів та периферійного обладнання, що дозволяють здійснювати прихований несанкціонований доступ до ресурсів системи (зазвичай за допомогою локальної чи глобальної мережі), тобто їх основне призначення – забезпечити несанкціонований доступ до конфіденційної інформації.

У більшості випадків після встановлення факту перехоплення управління системою з боку порушника він встановлює спеціальну програмну закладку в системі жертви для отримання необмеженого доступу в майбутньому.

Один з найбільш широко використовуваних способів інсталяції закладки полягає у використанні програмного забезпечення ActiveX (невеликі програми, за допомогою яких веб-сайти надають контент). Як тільки користувач відвідує сайт, вбудований ActiveX може автоматично запускатись у системі. З ActiveX порушник має повне керування системою, яка виконує ActiveX.

Компанія Microsoft багато разів офіційно повідомляла про реалізацію заходів політики безпеки для захисту системи від цього шахрайства. Наприклад, повинна дотримуватися умова, що розробники ActiveX підписують свої опубліковані файли ActiveX, при цьому підпис має бути чинним. Якщо будь-який користувач хоче запустити ActiveX без підпису, браузер показує попередження щодо проблем з безпекою, які можуть статися після запуску ActiveX.

Механізми організації невиявленого управління. Порушники зазвичай використовують різні механізми для того, щоб зробити свої закладки невиявленими та невідстежуваними. Якщо системний адміністратор бачить незвичайну поведінку системи, він може зрозуміти, що вона може бути викликана вірусом або закладкою, тому він буде змушений шукати закладку і порушник більше не зможе отримати доступ до системи. Якщо адміністратор зможе відстежити призначення таких пакетів, він також зможе виявити порушника. З цієї причини досвідчені порушники завжди намагаються сховати свої зв'язки та завдання закладки. При цьому вони використовують кілька способів подібного приховування.

Використання криптографії. У багатьох ситуаціях порушники використовують криптографію для кодування даних між атакованою системою і порушником. Вони використовують різні методи шифрування для подачі команд та передачі даних між машиною жертви та системою порушника, прозорі для системного адміністратора під час моніторингу мережного трафіку та поведінки.

Найчастіше немає необхідності використовувати якийсь оригінальний метод шифрування, оскільки порушник зазвичай використовує лише стандартні алгоритми шифрування приховування даних під час передачі. Якщо порушник використовує дуже потужний метод (типу RSA), він може викликати збільшення завантаження центрального процесора машини жертви і час передачі подовжиться.

У цих випадках порушники зазвичай використовують симетричні методи шифрування AES.

Інші алгоритми — SSH або VPN є стандартними методами, які порушники використовують для шифрування трафіку. Надсилання пакетів з використанням VPN або SSH не можна знайти за допомогою брандмауера та адміністратора, і порушник може використовувати стандартні сервіси, які вже інстальовані в мережі для шифрування пакетів під керуванням закладки.

Використання кореневих комплектів. Хоча програмні закладки можуть бути дуже небезпечними, але, оскільки вони працюють як звичайне застосування, вони можуть легко виявлятися. Поглянувши на список завдань системи, за допомогою сервісів або реєстру можна побачити закладку. Досвідчений порушник використовує більш потужні закладки, які називаються «кореневі комплекти». Кореневі комплекти працюють як частина операційної системи та не дозволяють користувачеві побачити реальні завдання чи сервіси. Операційна система буде під

повним керуванням порушника і може заховати будь-що в системі. Кореневі комплекти, у свою чергу, поділяються на дві основні групи з різною архітектурою: «класичні кореневі комплекти» та «кореневі комплекти Кернеля».

Класичні кореневі комплекти зосереджуються на операційних системах на основі UNIX (наприклад, Linux та SunOS). Зазвичай у цих кореневих комплектах порушники замінюють файл /bin/login іншою версією, яка дозволяє порушнику використовувати власне ім'я та пароль для входу в систему. Якщо системний адміністратор змінює кореневий пароль або обмежує доступ кореневого користувача для дистанційної реєстрації в системі, порушник може реєструватися за допомогою свого власного пароля. Він також може використовувати його для збереження паролів інших користувачів у базі даних порушника.

Іноді класичні кореневі комплекси змінюють команду ifconfig, щоб приховати прапори карти мережі від очей адміністратора. Якщо вони не змінюють класичний файл ifconfig під час пасивного прослуховування мережі порушником, адміністратор може побачити прапор PROMISC та може зрозуміти, що працює програма пасивного прослуховування мережі.

Можна вказати інші команди UNIX, які зазвичай змінюють під вплив класичних кореневих комплектів для приховування du, find, is, netstat і ps.

Кореневі комплекти kernel (ядро) замінюють самі себе на kernel операційної системи. У цьому випадку після запуску програми операційна система повідомляє результати, які бажає порушник. З кореневими комплектами kernel усі процеси, завдання, конфігурації мережі, номери портів, вміст файлів тощо можуть представитися самим собі іншим чином, і порушник може примусити операційну систему «брехати» щодо всього, що б не захотів знати користувач або адміністратор.

У разі застосування кореневих комплектів kernel виявлення та відстеження закладок дуже складно, оскільки вони навіть можуть зупиняти антивірус або монітори системи. Це найпотужніший спосіб застосування закладок.

Використання різних протоколів та номерів портів. Порушник може використовувати випадковий номер порту замість стандартних портів для роботи сервісних програм та атакованої системи. Несподівана робота сервісу SSH порту 22, який завжди контролюється адміністратором, може викликати відстеження атаки системним адміністратором. Тому більшість порушників використовує інші номери портів для ускладнення виявлення сервісів порушника, що працюють.

Деякі закладки працюють професійніше. Вони змінюють номери портів, використовуючи протокол під час атаки. Наприклад, розумна закладка може змінити протокол зв'язку від TCP на UDP і навіть ICMP. Якщо системний адміністратор блокує порт або протокол на шлюзі, закладка може автоматично переключитися на інший протокол або номер порту та дозволити порушнику підключитися до системи.

Реверсне управління. Більшість міжмережевих екранів (фаєрволів) або адміністраторів блокують деякі з'єднання із зовнішнім світом. Вони можуть дозволити локальному користувачеві лише переглядати сайти і не більше. Закладки можуть використовувати іншу стратегію у цих ситуаціях. Наприклад, порушник запускає свій власний сервер за конкретною IP-адресою і закладка намагається з'єднатися з сервером усередині фаєрвола та запитати з сервера порушника команди, які слід виконувати на машині жертви. Закладка може використовувати стандартний протокол HTTP для підключення до сервера порушника, і сервер подаватиме команду у форматі HTTP. Це виглядає як перегляд через мережу для фаєрвола або адміністратора. Подібна стратегія справді складна для виявлення.

Єдиний спосіб виявлення цих з'єднань полягає у моніторингу числа запитів, які надсилаються системою атакованого об'єкта на особливу IP-адресу. Іноді порушники використовують об'єднання в ланцюжок безлічі серверів за різними IP-адресами для випадкового підключення до системи жертви. Цей метод навіть складніше для захисту.

Тимчасова послідовність реалізації закладки. Існує безліч сервісів, які використовуються для оновлення систем під час простою. Команда Cron на машинах UNIX або завдання Schedule на машинах Windows це приклади таких сервісів.

Порушники можуть застосувати їх до використання закладок у заданий час. Наприклад, використовуючи таблицю Cron машини UNIX, закладка може почати працювати о 5-ої годині ранку і дозволити порушнику підключитися до системи під час, коли в офісі відсутній адміністратор.

Висновки:

1. Основні групи деструктивних дій, що здійснюються програмними закладками: копіювання інформації користувача комп'ютерної системи, зміна алгоритмів функціонування системних, прикладних та службових програм, нав'язування певних режимів роботи.

2. До основних методів приховування факту присутності програмної закладки у комп'ютерній системі відносяться використання криптографії, кореневих комплектів, різних протоколів та номерів портів, реверсне управління.

Муц Д.С.
курсант НА СБ України
Четверіков І.О.
к.т.н, доцент НА СБ України

БЛОКЧЕЙН В КРИТИЧНІЙ ІНФРАСТРУКТУРІ

Актуальність теми. Сьогодні технологія блокчейн стала революційною інновацією, і має в собі потенціал застосування в різних галузях, таких як фінанси, логістика, енергетика, охорона здоров'я, громадська безпека та інші. Це децентралізована система, яка дозволяє здійснювати безпечні та прозорі транзакції без посередників. Блокчейн працює шляхом створення мережі комп'ютерів або вузлів, які перевіряють і зберігають кожну транзакцію в блоці. Коли блок заповнюється транзакціями, він додається до ланцюжка попередніх блоків, створюючи незмінний запис усіх транзакцій у мережі. Кожен блок містить унікальний код або «хеш», який пов'язує його з попереднім блоком у ланцюжку, тим самим створюючи захищений від підробки запис. Така технологія дозволяє проектувати системи критичної інфраструктури, де людський фактор зведено до мінімуму.

У цій роботі ми розглянемо як саме використовується блокчейн в критичній інфраструктурі, а також застосування блокчейну в різних галузях.

Технологія блокчейн змінює наше суспільство, вона пропонує численні можливості та потенційні переваги в різних галузях.

Поняття блокчейну та його сутність. Взагалі надати визначення блокчейну в кількох словах досить складно, адже кожна людина спирається на свій унікальний образ мислення, досвід та знання, і тому може по-різному сприймати конкретні формулювання.

Л. Лелу [4] дає такі визначення:

Спрощене: Це велика бухгалтерська книга, або журнал (гросбух), куди кожен може вносити записи і який кожен може прочитати на величезній кількості комп'ютерів у всьому світі.

Буквальне: Блокчейн описує ланцюжок блоків (числових контейнерів), в яких зберігається інформація різного виду: транзакції, контракти, документи про власність, витвори мистецтва тощо.

Технічне: Блокчейн - це технологія організації бази даних, що спирається на Інтернет і повністю використовує всі його переваги, що включає відкритий протокол та здатність до розрахунків та шифрування. Сутність блокчейну полягає у тому, що він дозволяє створювати децентралізовані системи, в яких не потрібні довірені треті сторони для підтвердження транзакцій. У блокчейні кожен блок, що містить транзакції, підписується криптографічною функцією, що забезпечує його цілісність та незмінність. Крім того, блокчейн використовує принцип розподіленої

бази даних, що означає, що кожен валідатор мережі має копію бази даних, що робить систему більш стійкою до атак та втручань.

Поняття блокчейну в критичній інфраструктурі. Блокчейн - це технологія, яка може знайти своє застосування в критичній інфраструктурі, такій як енергетика, зв'язок, електронне голосування та інформаційна безпека. Вона може забезпечити безпеку, надійність та ефективність в обміні даними та інформацією. Блокчейн може бути використаний для покращення інфраструктури в різних галузях, таких як фінанси, логістика, енергетика, охорона здоров'я, громадська безпека, інформаційна сфера та інші.

Застосування блокчейну в критичній інфраструктурі. Найбільшу актуальність для реалізації функцій системи "Держава у смартфоні" має можливість застосування технології блокчейну в електронному голосуванні. Гарантовано кожен голос виборця буде врахований. Неможливо буде голосувати двічі, неможливо вкрасти голос виборця. При цьому особа голосуючого залишається конфіденційною. А можливість перевірити коректність транзакцій із голосами є у кожного бажаючого. Кожен голосуючий повинен мати зареєстрований в центрі сертифікації свій особистий відкритий ключ. Напрацьовано декілька алгоритмів консенсусу (PoS, FBA, BFT та ін.)[1].

Другим прикладом використання блокчейну в інфраструктурі є створення системи "розумного міста" (smart city), в якому блокчейн може забезпечити безпечну та ефективну комунікацію між різними системами та управляти різними процесами, такими як управління транспортом, розподіл енергії та водопостачання, системи обліку ланцюгів постачань, збір сміття та багато іншого. В критичній інфраструктурі, такій як енергетика, транспорт та комунікації, блокчейн може використовуватися для забезпечення надійності та безпеки даних, зменшення ризику кібератак та підвищення ефективності. Наприклад, блокчейн може бути використаний для створення розумної електромережі, яка може відслідковувати та управляти енергоспоживанням, або для побудови безпечної мережі автомобільних доріг, яка може автоматично регулювати рух транспорту. Застосування блокчейну в критичній інфраструктурі може допомогти забезпечити стійкість та надійність системи, зменшити ризик помилок та зловживань, а також забезпечити збереження даних, що не можуть бути змінені. Для того, щоб змінити інформацію в блокчейні, потрібно зламати одразу більше ніж 51% вузлів-валідаторів. Що не вбачається можливим.

Застосування блокчейну в інформаційній сфері. Блокчейн в інформаційній сфері - це технологія розподіленого реєстру, яка дозволяє зберігати дані в безпечному та недоступному для зламування форматі. Це робить її корисною в багатьох галузях, включаючи інформаційну сферу.

У інформаційній сфері блокчейн може бути використаний для зберігання, обробки та передачі інформації. Основні переваги використання блокчейну в інформаційній сфері включають:

1) Безпека. Блокчейн забезпечує безпечний спосіб зберігання та передачі даних, що дозволяє уникнути зламів та крадіжок.

2) Надійність. Блокчейн забезпечує надійний та незмінний реєстр даних, що дозволяє забезпечити достовірність та цілісність даних.

3) Швидкість. Блокчейн може обробляти великі обсяги даних швидко та ефективно, що дозволяє забезпечити високу продуктивність та ефективність.

4) Відкритість. Блокчейн забезпечує можливість перегляду даних всіма учасниками мережі, що дозволяє забезпечити прозорість та відкритість процесу.

У інформаційній сфері блокчейн може бути використаний для зберігання та передачі різних типів даних, включаючи фінансові, статистичні, медичні, транспортні та інші дані. Він також може бути використаний для розвитку нових технологій та рішень в галузі інформаційної безпеки та кібербезпеки.

Висновки. Під час дослідження було виявлено, що технологія блокчейн розвивається з кожним роком все швидше. Кожна нова ідея реалізується в стартапах та різноманітних додатках. Всі інновації залучаються до нових і нових галузей. Експерти переконані, що блокчейн вже сьогодні увійшов в наше життя та відіграватиме ключову роль у майбутньому. Очікують, що ця технологія все стрімкіше буде застосовуватись в критичній інфраструктурі. Застосування блокчейну в критичній інфраструктурі може допомогти забезпечити стійкість та надійність системи, зменшити ризик помилок та зловживань, а також забезпечити збереження даних, що не мають бути змінені. Для того, щоб зламати блокчейн і змінити дані, необхідна згода сторін, які досягають консенсусу. Якщо буде така змова і вони перепишуть ланцюг блоків і замінять його, це беззаперечно доводиться як факт атаки через історію транзакцій.

В ході дослідження ми виконали поставлені перед нами завдання, що дало нам змогу зробити такі висновки:

1. Коли йдеться про надійність і достовірність роботи з даними, забезпечення їх історичної послідовності і цілісності, в нагоді буде блокчейн.

2. Блокчейн гарантує прозорість та надійність даних, можливість їх перевірки спостерігачами та аудиторами.

3. В результаті аналізу та планування вимог щодо функціональності, масштабованості та безпеки системи що впроваджується, вибирають конкретний алгоритм досягнення консенсусу.

4. Для широкого застосування технології блокчейн в державі необхідно впроваджувати цифрову ідентифікацію та оцифрування всіх процесів в критичній інфраструктурі і пов'язаних сферах.

5. Використання технології блокчейн ще не набуло широкої популярності. Але в останні роки під керівництвом Комітету з питань цифрової трансформації з’являються все більше блокчейн-стартапів, які допомагають розвинутись цій технології і зробити наше життя безпечнішим.

Література
1. Кравченко П. Блокчейн і децентралізовані системи : навч. посібник у 3 ч. Ч. 1 Харків : ПРОМАРТ, 2019. 452 с.
2. Попереду планети всієї: які компанії займаються блокчейном в Україні. *Економічна правда Спец проєкт «Фінтекс»*. URL: https://www.epravda.com.ua/projects/fintech/2019/10/9/652378/ (дата звернення: 12.03.2023).
3. Комітет з питань цифрової трансформації. *Офіційне Інтернет представництво* URL: https://komit.rada.gov.ua/news/pro_komitet/72756.html (дата звернення: 12.03.2023).
4. Лелу Л. Блокчейн від А до Я. Все про технології десятиліття. ЭКСМО, 2018. 256 с.

Ольховик Д.А.
студент Національної академії СБ України

ВИКОРИСТАННЯ НАРАТИВУ: «КУЛЬТУРА НЕ ВИННА», ЯК МЕТОДУ ПРОПАГАНДИ рф

Перш ніж у країну в’їдуть ворожі танки, країни-агресорки «проїжджаються» культурною зброєю — насаджують власну і утискають ту, що панує на території іншої країни. Вклинюючи бажані наративи у культурне поле, вони формують сприятливі умови для ведення гібридної війни. Загарбники розраховують на те, що завдяки лояльності до їхньої культури, вони матимуть карт-бланш на території інших країн. За таким сценарієм роками працює і рф — експропріюючи українських культурних діячів, встановлюючи пам’ятники своїм вождям і всіляко проштовхуючи свій низькосортний контент в інфопростір. Фрази на кшталт «культура не на часі» чи «а при чому тут Пушкін?» за таких обставин стають шкідливими наративами, що загрожують національній безпеці України.

Різниця між тим, що Росія транслювала назовні і тим, як мистецтво впливало на внутрішню авдиторію, є величезною. Наприклад, якщо західне суспільство сприймало російські твори як загадковий східноєвропейський фаталізм, то для росіян вони лише посилювали впевненість в тому, що «малєнькій чєлавєк» у великому світі нічого не вирішує. І краще підкоритися сильнішому, ніж боротися і загинути. Російське мистецтво стало прикриттям для російської пропаганди, а пропаганда, в свою чергу, стала підґрунтям загарбницької війни.

Росія, яка століттями утискала українську культуру, насаджуючи думку про її меншовартісність і світу, і самим українцям, почасти досягла мети. Винищення представників української інтелігенції та їхніх здобутків, системні спроби зросійщення всіх рівнів життя українців, на жаль, зробили своє. Ще до 2014 року в

українському суспільстві зберігався міф про велич російської культури. І хоч Україна чи не найбільше постраждала від агресивної колоніальної політики рф, це не означає, що культура інших країн — у безпеці. Почавши повномасштабну війну, рф нарешті показала світу свої справжні наміри і методи, якими вона скроїла свою країну.

Отже, в інформаційному просторі усе частіше з'являються дискурси про непричетність російської культури до війни. І саме на це розраховує країна-агресорка. Кенселінг (скасування) російської культури наразі — це елемент самозахисту кожної країни, на чию самобутність зазіхає Росія, це потужний фронт робіт, який теж потребує чимало зусиль і згуртованості. Якщо хвороба імперіалізму намагається поширитися на суверенітет нашої держави, то в наших силах ліквідувати цю загрозу.

Література

1. Чому російська культура заслуговує бути скенсельованою • Ukraïner. Ukraïner. URL: https://ukrainer.net/vidmina-ros-kultury/ (дата звернення: 04.03.2023).

2. Українська правда. Російська культура – це і "потьомкінські дєрєвні", і вістря ракет. Українська правда - новини онлайн про Україну. URL: https://www.pravda.com.ua/columns/2022/11/8/7375497/index.amp (дата звернення: 04.03.2023).

3. Асєєв С. Достоєвський і Буча: російська культура вбиває?. Радіо Свобода. URL: https://www.radiosvoboda.org/a/rosiyskyy-fashyzm-putin-duhin-zahroza-svitu/31856995.html (дата звернення: 05.03.2023).

4. російська культура винна, бо допустила створення тоталітарної держави. Високий Замок. URL: https://wz.lviv.ua/blogs/464950-rosiiska-kultura-vynna-bo-dopustyla-stvorennia-totalitarnoi-derzhavy (дата звернення: 05.03.2023).

5. ім. Т.Г. Шевченка. ЧОМУ РОСІЙСЬКА КУЛЬТУРА - ФЕЙК? | Історія України від імені Т.Г. Шевченка, 2022. YouTube. URL: https://www.youtube.com/watch?v=NNvePYbQ9MI (дата звернення: 05.03.2023).

6. Ukraïner. Чому російська культура – це зброя? • Ukraïner, 2022. YouTube. URL: https://www.youtube.com/watch?v=GUm0OhRbeg0 (дата звернення: 05.03.2023).

Ольховська Є. О.
студентка групи Н-221м ННІ ІБ СК НА СБ України

Жевелєва І.С.
к.ю.н., доцент
доцент кафедри ОЗІОД ННІ ІБ СК НА СБ України

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ПРОТИДІЇ ТЕРОРИСТИЧНИМ ЗАГРОЗАМ ЯК ВАЖЛИВИЙ ЧИННИК ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Тероризм стає невід'ємною частиною політичних і економічних процесів у світі та являє собою все більшу загрозу громадській і національній безпеці, із поодиноких проявів перетворюючись в масове явище. В сучасних умовах повномасштабного вторгнення росії питання протидії тероризму в Україні стоїть як ніколи гостро. На це вказують дослідження напрацювань авторів, що безпосередньо вивчали історичний досвід України в аспекті формування та впровадження системи протидії тероризму в державну сферу. Багато робіт вітчизняних науковців присвячено іноземному досвіду боротьби з цим явищем, що є корисним для опрацювання майбутнього вдосконалення антитерористичної політики України.

Тероризм, за своїми ознаковими характеристиками, існував завжди. Вся історія світу пронизана біографіями осіб, що для досягнення успіхів в політичній чи суспільній, інколи релігійній діяльності вдавались до загроз та насильницьких дій. Як свідчить світовий досвід, розвинуті державні утворення завжди боролись та протистояли цьому явищу. Поняття «тероризм» не стосується диктатури або тоталітаризму, бо притаманна тероризму характеристика – дії під прикриттям суспільного запиту, «руху знизу». А диктатура або тоталітарний режим – централізовані дії згори [6].

Терор, за своїм латинським походженням, означає страх або жах. Багато років після першого застосування цього терміну, його значення не змінило змісту. Терором, загалом, називається загроза фізичної розправи з політичних чи будь-яких інших мотивів або залякування з загрозою розправи або вбивства.

Законодавство України, зараз, в період становлення як європейської держави має досліджувати та брати приклад законодавства інших держав. Особливо примітними є Європейська конвенція про боротьбу з тероризмом від 27 січня 1977 року, Міжнародна конвенція про боротьбу із захопленням заручників від 17 грудня 1979 року, Міжнародна конвенція про боротьбу з фінансуванням тероризму від 9 грудня 1999 року, Конвенція Ради Європи про запобігання тероризму від 16 травня 2005 року, Додатковий протокол до Конвенції Ради Європи про запобігання тероризму, підписаний Україною 28 жовтня 2015 року.

Дослідження Україною іноземного законодавства та велике бажання досягти високого рівня розвитку суспільства стали чинниками змін. Так, у Кримінальному кодексі України, прийнятому 5 квітня 2001 року, у ст. 258 встановлена відповідальність за вчинення терористичного акту, а Законом України від 20 березня 2003 року №638‑IV «Про боротьбу з тероризмом» передбачені основні організаційно-правові засоби протидії терористичним проявам [1; 26].

Визначення тероризму закріплено у Законі України «Про боротьбу з тероризмом». Тероризмом законодавець вважає суспільно небезпечну діяльність, яка полягає у свідомому, цілеспрямованому застосуванні насильства шляхом захоплення заручників, підпалів, убивств, тортур, залякування населення та органів влади або вчинення інших посягань на життя чи здоров'я ні в чому не винних людей або погрози вчинення злочинних дій з метою досягнення злочинних цілей [2].

Починаючи з 2014 року на території Донецької та Луганської області, а зараз і повноцінно по всій території України, держава-терорист – росія, використовуючи сили збройних незаконних формувань широко використовує терористичну тактику ведення бойових дій. Численні обстріли житлових масивів, критичної інфраструктури, масові розстріли людей в окупованих містах та територіях свідчать про терористичні дії зі сторони рф, які можна порівняти з діяльністю міжнародних терористичних організацій «Аль-Каїда» або «Ісламська держава». російська федерація з 2014 року напряму постачала бойовикам незаконних формувань ЛНР та ДНР озброєння, військову техніку, боєприпаси, надавала значні матеріальні та фінансові ресурси.

У нинішніх умовах терористичні дії ворога не лише негативно позначаються на безпековому середовищі, а й становить безпосередню загрозу для національної безпеки України. Необхідність мати план підвищення стійкості та протидії терористичним загрозам є важливим чинником забезпечення національної безпеки в цілому.

Факторами, що характеризують антитерористичну систему як стійкий та ефективний механізм, є насамперед спроможність передбачати й оцінювати ризики та загрози, прогнозувати їх характер і можливі масштаби; формування резервів і альтернативної стратегії дій на випадок надзвичайних ситуацій; здатність швидко й адекватно реагувати на загрозу, адаптуватися до умов, що швидко змінюються, забезпечувати безперервність процесу управління і відновлюватися після руйнівних наслідків кризи.

Підвищити ефективність протидії терористичним загрозам можна шляхом удосконалення українського законодавства в цій сфері у частині кримінально-правової складової з метою досягнення відповідності між ознаками складів злочинів та притаманними терористичним злочинам властивостями, бо ознаки складів злочинів мають більш чітко і повно відбивати сутнісні риси терористичних діянь як явищ реальної дійсності [1; 67]; налагодження системи

взаємодії спеціальних служб і правоохоронних органів з населенням з питань запобігання і протидії тероризму, а також мінімізації наслідків вчинення терактів.

У цих процесах має бути врахований досвід проведення АТО на території окремих районів Донецької й Луганської областей, річний досвід протистояння повномасштабному вторгненню, та, обов'язково – передовий іноземний досвід.

Складна ситуація, у якій опинилась Україна, спонукає до пошуків нових рішень та напрацювання більш дієвих антитерористичних заходів на національному, регіональному та глобальному рівнях. Цей процес є складним і вимагає відмови від усталених стереотипних підходів в оцінці суспільної небезпеки тероризму, актуалізує наукові дослідження з цієї проблематики, що мають велике значення на перспективу.

Тема боротьби з тероризмом є однією з максимально розвинутих та досліджених аспектів світової діяльності, в той самий час, аналіз динаміки здійснення терористичних актів як в Україні, так і у світі свідчить про застосування терористами нових форм, засобів, висування нових вимог, обґрунтувань та виконавців, що свідчить про доцільність подальшого вивчення науковцями та практиками цих явищ з метою їх уникнення. Україна, розпочавши свій шлях до Європейського суспільства, зіткнулась з жахливими випробуваннями війною, яка ведеться з активним використанням терористичних дій. Саме це спонукає впроваджувати нові, більш жорсткі норми, що регулюють антитерористичну діяльність. Імплементація європейського законодавства стане запорукою майбутнього нашої держави як для вступу в ЄС, так і для подальшої боротьби заради незалежності в цій підступній агресії.

Література

1. Ємельянов В. П. Антитерористичне законодавство: поняття, система, шляхи вдосконалення : монографія. Право, 2016. 88 с.

2. Про боротьбу з тероризмом: Закон України від 20 березня 2003 р. №638‑IV. URL: http://zakon.rada.gov.ua

3. Про ратифікацію Європейської конвенції про боротьбу з тероризмом: Закон України від 17 січ. 2002 р. №2990‑III. – URL: http://zakon.rada.gov.ua

4. Про ратифікацію Конвенції Ради Європи про запобігання тероризму: Закон України від 31 лип. 2006 р. № 54‑V. – URL: http://zakon.rada.gov.ua

5. Резнікова О. О., Місюра А. О., Дрьомов С. В., Войтовський К. Є. Актуальні питання протидії тероризму у світі та в Україні: аналіт. доповідь / за заг. ред. О. О. Резнікової. Київ : НІСД, 2017. 60 с.

6. Тероризм і Російська Федерація. Як далі бути? URL: https://www.ukrinform.ua/rubric-world/3314675-terorizm-i-rosijska-federacia-ak-buti-dali.html

Пітулько Є.О.
студент ННІ ІБ СК НА СБ України

БЕЗПЕКА ДЕРЖАВИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Агресія Росії проти України почала процес руйнування системи європейсько та трансатлантичної безпеки. Гібридні дії Кремля проти України та інших регіональних держав підривають стабільність на території від Балтійського до Чорного моря, створюючи серйозний виклик миру та безпеці в регіоні.

Гібридна війна — це не тільки силове протистояння ворогуючих сторін, проведення інформаційних операцій та пропаганда, а і використання можливостей організованих злочинних організацій, шляхом системного вчинення останніми протиправних дій, які розповсюджуються на органи влади управління та мають корупційний характер.

Особливістю війни гібридного типу є:

- активне використання сил спеціальних операцій, сил розвідки, військового нетрадиційного підрозділу;
- залучення або використання в цілях держави-агресора окремих осіб, груп, організацій і партій, їх можливостей шляхом явного та/або прихованого маніпулювання їхніми поглядами та переконаннями;
- розгортання широкої інформаційної війни для психолого-ідеологічної підготовки власного населення, населення та особового складу збройних сил країни, проти якої готується і ведеться гібридна війна, світове співтовариство з метою введення в оману щодо справжніх намірів агресор;
- створення сепаратистських рухів у державі, яка є об’єктом гібридної війни за політичними, етнічними чи релігійними ознаками;
- торгові війни ведуть шляхом припинення транзиту, введення підвищених мит або заборони ввезення товарів і недопущення їх надходження на свої ринки з держави, з якою планується гібридна війна;
- централізоване управління діями Збройних Сил, Сил спеціальних операцій, незаконних збройних формувань, сепаратистів, терористів, бойовиків, диверсійно-розвідувальних груп;
- організація плебісциту чи референдуму на запланованих для захоплення територіях для виправдання етнічної агресії з псевдометою захисту інтересів окремих груп населення (іншої національності чи релігії);
- створення на окупованій території органів державного управління, підконтрольних державі-агресору [1].

На думку військового аналітика, теоретика Ф. Гофмана [4], тенденція до конвергенції в сучасних конфліктах, що виявляється у зближенні та взаємному проникненні (поєднанні) вищезгаданих аспектів війни, є принципово новою характеристикою сучасної війни. Конвергенція, яка охоплює регулярні військові

та проксі-групи, стирає кордони між урядовими та неурядовими учасниками збройних дій, а також їхніми нерівними військовими можливостями. Ця тенденція змінює форми (модальності) ведення війни, і традиційні категоричні відмінності між тероризмом, звичайними військовими діями, злочинністю та нерегулярними війнами втрачають своє практичне значення.

Необхідно створити систему управління для протидії гібридній війні, яка здатна керувати різнорідними (багатовідомчими) силами і засобами на всіх вищезгаданих напрямках.

Забезпечення глобальної та регіональної стабільності стає неможливим без підвищення військової безпеки держави, підтримання стану обороноздатності країни, що забезпечує запобігання збройним конфліктам та припинення можливої військової агресії. Таким чином, існує нагальна потреба багатьох держав у реформуванні та розвитку всього сектору безпеки та оборони з метою підвищення його готовності протистояти сучасним небезпекам і загрозам.

Операція з окупації та анексії Криму стала зразковою за відповідністю досягнутих цілей раніше розробленому плану та послідовності його виконання. Це стало своєрідним неповторним стандартом гібридної агресії.

Оцінивши поточну ситуацію, можна збагнути, що військова складова гібридної війни зовсім не зменшується. Гібридна війна використовує всі виміри державної влади, щоб нав’язати свою волю іншій державі, розсуваючи найслабші місця розвитку та досягаючи результатів. Фактично цей тип війни передбачає, що саме суспільство стає першою лінією оборони. Для захисту держави необхідне поєднання цивільних і військових можливостей.

Для ефективної протидії гібридним загрозам потрібна міжнародна координація. Тому мета Росії — максимально послабити міжнародне співробітництво, створити опір багатосторонньому інституційному співробітництву. Міжнародна координація має вирішувати питання відповідної підготовки журналістів, лідерів думок та державних службовців таким чином, щоб вони навчилися розрізняти правду і брехню, професійно розуміти ситуацію, щоб кордони та мовне середовище не викликали упереджень[3].

Аналіз сучасної ситуації на світовій геополітичній арені свідчить про подальше зростання активності Москви в напрямку руйнування системи безпеки, що вибудовувалася десятиліттями, шляхом проведення спецоперацій як військового, так і гібридного (інформаційного, політичного, безпекового) характеру. Ефективно протидіяти цим ефектам можливо лише у разі переходу від реактивних до проактивних підходів до протидії гібридним загрозам.

Міжнародна координація у відповідь на гібридні загрози має також охоплювати такі сфери, як економіка, фінанси, суспільство, ЗМІ, кіберпростір, дипломатія тощо. Гібридна війна в широкому європейському контексті створює передумови для повномасштабної звичайної війни. Ризики для євроатлантичної безпеки продовжують зростати після 2014 року. Тому точна оцінка гібридних

загроз стає життєво важливою для мирного майбутнього.

За останнє десятиліття відбулися значні зміни в безпечному середовищі Східної Європи, насамперед через активну дестабілізуючу політику Російської Федерації щодо сусідніх держав, збройну агресію та порушення територіальної цілісності України (тимчасова окупація Російською Федерацією) Автономної Республіки Крим, м. Севастополь та військова агресія в окремих районах Донецької та Луганської областей). Агресія Російської Федерації проти України показала, що, незважаючи на інтенсивне використання різноманітних ненасильницьких засобів (політико-дипломатичних, економічних, інформаційних тощо), основна роль належить силовим, особливо військовим і спеціальним силам.

Завдання протидії широкому спектру цих військових і спеціальних засобів, притаманних російській гібридній агресії, зумовило необхідність створення якісно нової форми системи управління Збройними силами України, об'єднаної зусиллями її Збройних Сил, правоохоронних органів і спецслужб.

На даний момент Російська Федерація продовжує вести гібридну війну проти України, яка є поєднанням різноманітних динамічних дій підконтрольних незаконних збройних формувань та регулярних сил Російської Федерації, які взаємодіють із злочинними збройними формуваннями та злочинними елементами, активно використовують пропаганду, диверсії, умисне заподіяння шкоди, вчинення терористичних актів, цілеспрямований інформаційний (інформаційно-психологічний) та кібернетичний вплив (атаки) [2].

Ця діяльність повністю відповідає поглядам провідних експертів щодо методів ведення гібридної війни, а саме: використання нерегулярних груп, вчинення терористичних актів, у тому числі насильства та примусу, а також створення злочинного безладу. Ці мультимодальні дії можуть виконуватися окремими або одиничними формуваннями, які оперативно та тактично керуються та координуються в межах основного бойового простору для досягнення синергетичного ефекту.

Література

1. Антоненко С. (2017) Особливості функціонування системи управління Збройними Силами України в умовах гібридної війни. Інформаційний вимір гібридної війни: досвід України, матеріали міжнародної науково-практичної конференції . К.: Національний університет оборони України , 2017. С. 10-16

2. Галеотті Марк (2016) Гібрид, неоднозначний і нелінійний? Наскільки новим є російський «новий спосіб війни»?, Small Wars & Insurgions, 27:2, 282-301, DOI: 10.1080/09592318.2015.1129170

3. Гейтс, Р. (2009) Збалансована стратегія: перепрограмування Пентагону для нової доби. *Закордонні справи* , січень/лютий 2009 р., вип. 88, No 1, С. 28-40.

4. Гофман, Ф. Г. (2007) Конфлікт у 21 столітті: зростання гібридних

воєн, Інститут політичних досліджень Потомака. Грудень 2007 р. Доступно за адресою: http://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf

Попович М.
студент Національна академія Служби безпеки України

ПРОБЛЕМИ ПРОТИДІЇ ІНФОРМАЦІЙНИМ, ПСИХОЛОГІЧНИМ ВПЛИВАМ рф НА ОСОБОВИЙ СКЛАД ЗБРОЙНИХ ФОРМУВАНЬ СТРУКТУР СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

Протидія інформаційним та психологічним впливам російської федерації на особовий склад збройних формувань структур сектору безпеки та оборони України є одним з ключових пріоритетів української держави. Інформаційні та психологічні впливи рф на особовий склад збройних формувань структур сектору безпеки та оборони України мають на меті дискредитувати українські військові формування та дезорганізувати їхню діяльність. Зокрема, рф використовує такі методи як дезінформація, провокації, шантаж, дестабілізація тощо. Російська пропаганда намагається створити образ ворога, що може призвести до збільшення напруження та конфліктів в зоні бойових дій.

Також проблемою є використання соціальних мереж та інтернет-ресурсів для поширення пропагандистської інформації. Російські спецслужби можуть створювати фейкові акаунти, що може призвести до витоку конфіденційної інформації та порушення безпеки військових об'єктів.

Для протидії цим проблемам необхідно проводити постійну роботу з особовим складом, забезпечувати їх інформаційною безпекою та навчати розпізнавати фейкову інформацію. Також необхідно вдосконалювати систему контролю за використанням інтернет-ресурсів та соціальних мереж в зонах бойових дій, щоб запобігти витоку конфіденційної інформації та зберегти безпеку військових об'єктів. Для того, щоб ефективно протистояти цим впливам, необхідно вирішити декілька проблем: Відсутність комплексної стратегії протидії інформаційним операціям: Україні потрібно розробити та впровадити національну стратегію протидії інформаційним операціям та психологічному впливу, спрямовану на зміцнення інформаційної безпеки, розвиток протидії дезінформації та підвищення обізнаності особового складу сектору безпеки та оборони.

Недостатня освіта та підготовка: Забезпечення якісної освіти та підготовки військових та співробітників сектору безпеки з питань інформаційної безпеки, роботи з джерелами відкритої інформації та протидії дезінформації є важливим аспектом протидії інформаційному впливу рф.

Відсутність ефективних механізмів координації: Україні необхідно

забезпечити кращу координацію між різними структурами сектору безпеки та оборони, міністерствами, службами та організаціями, які займаються протидією інформаційним операціям. Необхідно проводити постійну професійну підготовку й відзначення відповідальності серед особового складу. Також важливо забезпечувати його достатньо високим рівнем матеріально-технічної бази, а також забезпечувати його правом на інформацію, в тому числі відповідно до принципів свободи слова та преси. Забезпечити належну соціальну підтримку військовослужбовців та їх сімей.

Отже, протидія інформаційним та психологічним впливам рф на особовий склад збройних формувань структур сектору безпеки і оборони України є важливою складовою національної безпеки. Це потребує комплексного підходу та спільних зусиль військових та цивільних структур, а також підтримки населення. Тільки таким шляхом можна забезпечити ефективну захист України від інформаційно-психологічних загроз. Крім того, важливо пам'ятати про необхідність розвитку кібербезпеки та забезпечення безпеки військових об'єктів від кібератак. Такі заходи допоможуть зменшити ризики для національної безпеки та зберегти життя військових.

Література

1. "Гібридна війна Росії проти України: протидія психологічним впливам", Ю. Смірнов, 2017 р.
2. "Інформаційна війна та пропаганда Росії в Україні", О. Іванова, 2015 р.
3. "Протидія інформаційній агресії Росії: проблеми та шляхи розв'язання", А. Васильєва, 2018 р.
4. "Психологічна війна рф: проблеми протидії", І. Шевчук, 2016 р.
5. "Інформаційна безпека України в умовах гібридної війни", В. Петренко, 2019 р.
6. "Психологічні аспекти забезпечення національної безпеки України", В. Лисенко, 2015 р.
7. "Інформаційна безпека в Україні: реалії та виклики", О. Шумилов, 2017 р.

Потапчук О.А.
курсантка НА СБ України

МЕТОДИ ВПЛИВУ ПРОПАГАНДИ ТА ПРОТИДІЯ ЇМ

Сучасний світ переповнений усіма видами конкуруючої пропаганди та контрпропаганди. Особливо активно працює «пропагандистська машина» російської федерації, яка всіма силами намагається виправдати всі звірства, котрі

загарбники принесли на нашу землю. Тому, проблема виявлення методів впливу пропаганди та протидії їй є складною та особливо актуальною в наш час.

Методів пропаганди існує дуже багато. Найбільш поширеними, зокрема, які використовує російська федерація для впливу на населення є :

1. Запрошення добре відомих або надійних осіб для впливу на цільову аудиторію.

2. Стереотипізація. Цей метод пропаганди висвітлює стереотипи, а потім або підсилює, або руйнує їх за допомогою засобів масової інформації.

3. Демонізація ворога. Ціль цих типів пропагандистської реклами та повідомлень полягає в тому, щоб налякати людей, щоб вони вжили бажаних дій. Наприклад, «Бандери їдять дітей» і інші подібні нісенітниці.

4. Феномен перемоги створює відчуття ізоляції та викликає (страх втратити) у людей, які прагнуть бути частиною якоїсь бажаної групи. Частина населення розуміє, що насправді відбувається, але просто боїться висловити свою думку.

5. Підміна понять. Як приклад можна навести підміну таких термінів «війна» - «спецоперація», «вибухи» - «хлопки». Також в ефірі почали вирізати слова «мир» та «війна».

6. Блискучі узагальнення використовують завантажені слова та яскраві гасла, щоб справити враження на аудиторію, яка сприймає повідомлення. Наприклад, «Де ви були вісім років?» і тому подібні [1].

Методів контрпропаганди також є багато. Але на мою думку, одним із особливих типів контрпропаганди є «викриття джерел» — інформування аудиторії про те, що пропагандисти погано поінформовані, є злочинцями або належать до якоїсь групи, яку аудиторія напевно вважатиме підривною, тим самим підриваючи довіру до них і, можливо, їх економічну діяльність [2].

Також важливим методом контрпропаганди є отримання інформації із різних джерел та її аналіз через призму критичного мислення.

Можна зробити висновок, пропаганда під час війни є особливим видом зброї. Існує безліч методів пропаганди, як і контрпропаганди. Тому важливо отримувати інформацію із різних джерел, критично мислити, ставити питання та перевіряти інформацію.

Література

1. Types of Propaganda Techniques in Advertising (With Examples). [Електронний ресурс]: Офіційний сайт. – URL: https://motioncue.com/types-of-propaganda-techniques-in-advertising/ (дата звернення 21.11.2022).

2. Measurement of the effects of propaganda. [Електронний ресурс]: Офіційний сайт. – URL: https://www.britannica.com/topic/propaganda/Measurement-of-the-effects-of-propaganda (дата звернення 21.11.2022).

Прокопчук М.С.

Національний університет оборони України імені Івана Черняховського

СУТНІСТЬ МОНІТОРИНГУ ІНФОРМАЦІЙНОГО ПРОСТОРУ В ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СИЛ ОБОРОНИ

Шляхом постійного моніторингу та аналізу інформаційних ефектів здійснюється формування вирішальних умов у досягненні цілей забезпечується мети моніторингу інформаційного простору в забезпеченні інформаційної безпеки Сил оборони України. Під час моніторингу інформаційного простору проводяться заходи спрямовані на оцінювання інформації про оперативну обстановка. Оперативна обстановка має декілька рівнів [1].

Так, на оперативному рівні процес оцінювання інформації основується на загальному аналізі показників вимірювання прогресу запланованих дій, створення потрібних ефектів, формування вирішальних умов та досягнення запланованих цілей. Оцінювання операцій на оперативному рівні зосереджується на двох аспектах:

перший, значно ширший за природою, спрямований відповісти на запитання: “Чи ми проводимо військову місію оперативного рівня?” Це також включає постійний моніторинг та оцінювання всіх ефектів, вирішальних умов та цілей, визначених у оперативному плані (OPLAN). Крім того, розглядається оцінка потрібних і небажаних ефектів в доменах PMESII – як вони можуть суттєво вплинути на кампанію або операцію або якщо вони чітко визначені в плані операції. Цей тип оцінки операції веде до розробки рекомендацій штабу для підготовки вказівок командира щодо уточнення / модифікації кампанії або операції.

другий, більш зосереджений, підтримує триваючу синхронізацію та виконання кампанії або операції. Це є коротко- або середньо-терміновим оглядом ефектів, що ведуть до вирішальних умов впродовж відповідних ліній операцій, та оцінюванням будь-яких спеціальних подій або ситуацій, що можуть з’явитися поза оперативним планом. Він підтверджує поточні операції та надає командиру рекомендації для прийняття рішень щодо модифікації / зміни через видання розпоряджень (FRAGO) або розробку нових координаційних наказів (директив) [2].

На тактичному рівні головна увага приділяється на вимірюванні завершеності запланованих дій, завдань та іншої діяльності з використанням узагальнених показників оцінювання ефективності. У деяких окремих випадках на тактичному рівні може вимірюватись формування вирішальних умов та створення оперативних ефектів, використовуючи індикатори оцінювання оперативної обстановки [3, 4].

До індикаторів оцінювання оперативної обстановки належать:

визначення та включення т. зв. “базових ліній (пунктів)” відліку для обраних показників (критеріїв), за якими буде в подальшому вимірюватись ступінь змін в інформаційному просторі;

оцінку існуючої інформації та розвідувальних даних;

визначення інформації (розвідувальних даних);

відслідковування (здійснення моніторингу) розвитку кризи і звітування встановленим порядком.

Таким чином, сутність моніторингу інформаційного простору в забезпеченні інформаційної безпеки Сил оборони України полягаю у визначенні ключових показників, які дозволяють здійснити поетапне дослідження оперативної обстановки.

Література

1. JP 5-0 JointPlanning, 01 December 2020. Доктрина ЗС США зоб’єднаного планування.

2. NATO Operations Assessment Handbook”, Version 3.0, посібник НАТО. 01 July 2015.

3. AJP-5 Allied Joint Doctrine for the Planning of Operations, Edition A Version 2, 24 May 2019,доктрина НАТО з оперативного планування.

4. ATP 3-13.1 The Conduct of Information Operations, публікація СВ США щодо ведення інформаційних операцій. October 2018.

Резнік А.О.
студентка групи К-191
ННІ ІБ СК НА СБ України

ПРОБЛЕМАТИКА ТЕЛЕБІОМЕТРІЇ: СТАН ТЕХНОЛОГІЙ, ВИКЛИКИ ТА ПЕРСПЕКТИВИ

Вступ

Протягом останніх кількох років, слово "телебіометрія" стало часто вживаним терміном при обговоренні питань, пов'язаних з визначенням кібербезпеки, аналітики сигналів та розпізнавання осіб. У своєму широкому контексті телебіометрія відноситься до вимірювання та розпізнавання біометричних характеристик людини на відстані. Вона може охоплювати відео, аудіо та інші формати імітації, а також може включати різні домени знань з багатьох сфер досліджень, таких як комп'ютерний, медицинський та інтелектуальний аналіз. Останнім часом технології телебіометрії все частіше стають предметом обговорення у контексті їх використання та можливих наслідків.

Проблеми та виклики в розробці та впровадженні телебіометрії:

Розвиток телебіометрії може бути поділений на ряд ключових проблем та викликів. Науковці та практики вдосконалюють алгоритми розпізнавання, працюють над стандартизацією та забезпечують дотримання принципів конфіденційності.

Одним з найважливіших проблем в телебіометрії є точність алгоритмів розпізнавання. Ефективність телебіометричних систем залежить від точності розпізнавання біометричних сигналів. Відповідні алгоритми використовують автоматичні розпізнавальні різні домени знань, для найефективнішого аналізу даних.

Стандартизація – це ще одна важлива проблема телебіометрії. Кожна телебіометрична система використовує власний набір характеристик, формат даних та алгоритми, що можуть створювати труднощі у їх взаємодії або порівнянні. Разом з координаторами стандартів, інженери та вчені працюють над прискоренням розвитку стандартів телебіометрії, що сприятиме взаємодії і налагодженню систем.

Конфіденційність також є важливою проблемою, що стосується телебіометрії. Використання біометричних даних не повинно порушувати права людини на особисту таємницю. Вони повинні проходити через технічні, організаційні та законодавчі заходи та відповідати принципам субсидіарності, відповідності та найменших можливих документів.

Попри ті проблеми та виклики, обговорені вище, перспективи розвитку телебіометричних технологій виглядають досить обнадійливо. Усім важливим у статті розділам притаманні тенденції до прискорення темпів росту, запровадження значних технічних вдосконалень та активного поширення.

Однак, у верхоліть, суспільство повинно точно зрозуміти впровадження телебіометрії до того, як ці технології будуть радикально впливати на різні сфери життя, як особистісні, так і професійні, в цілому.

Продумана політика в області стандартизації, захисту даних та відповідальності повинна бути основою для формування чіткої та послідовної системи розвитку телебіометрії на усіх рівнях: національному та міжнародному.

Висновок.

Враховуючи обговорення проблематики телебіометрії у даному викладенні, можна зробити декілька ключових висновків. По-перше, телебіометрія на сучасному етапі розвитку є актуальною та перспективною технологією, яка може відкрити нові можливості для безлічі сфер застосування, таких як кібербезпека, аналітика сигналів, розпізнавання осіб та моніторинг.

По-друге, розвиток телебіометрії стикається з рядом проблем та викликів, зокрема підвищення точності алгоритмів розпізнавання, стандартизація методів та даних, а також забезпечення конфіденційності використання біометричних даних.

По-третє, подолання перешкод у розвитку телебіометрії має відбуватися в рамках чіткої та послідовної політики, яка балансує між розвитком інноваційних технологій, стандартизацією процесів, захистом особистих даних користувачів та приватності.

Отже, розвиток телебіометричних технологій відкриває нові можливості в ряді галузей при одночасному врахуванні викликів та обмежень. Успіх у перетворенні цих технологій на корисні та безпечні інструменти сильно залежить від співпраці різних груп, включаючи науковців, практиків, розробників стандартів, законодавців та звичайних громадян. Тільки шляхом цілеспрямованого напрацювання та гармонійної співпраці можна розвивати технології телебіометрії, які допомагатимуть в дотриманні конфіденційності, підвищенні безпеки та вирішенні різноманітних викликів, що ставлять перед людством сучасні технології.

Рябов Н.С.
студент ННІ ІБ СК НА СБУ НА СБ України

ПРОТИДІЯ БОТОФЕРМАМ, ЯК ІНСТРУМЕНТУ ВПЛИВУ НА НАСЕЛЕННЯ УКРАЇНИ ТА КРАЇН ЗАХОДУ

Починаючи з 2014 року Україна веде війну з росією у інформаційному просторі, у якій росія активно використовує різні інструменти. Одним із таких стали “ботоферми”. Вони активно використовуються для просування російського норративу та деморалізації населення у соціальних мережах, де деструктивно впливають на думки населення як України, так і країн заходу.

Після початку повномасштабного вторгнення вплив від просування проросійського норративу різко впав, але “ботоферми” переключились на деморалізацію. Деморалізація відбувається шляхом розповсюдження відео з пораненими українськими військовими, все більше розповсюджується фейкових новин та відео. Паралельно з цим просувається думка про те, що треба домовлятися про мир. Також, вони доволі ефективно впливають на думки населення країн заходу. Доволі багато іноземців досі не розуміючи, хто насправді такі росіяни, продовжують підтримувати їх, або залишатися лояльними до агресора. І це відбувається у соціальних мережах, у коментарях під постами політиків, блогерів або навіть під постами на військову тематику. Акаунти “ботів” імітують акаунти реальних людей. Такі “боти” - це не лише машини, які пишуть схожі коментарі у великій кількості, але й люди, які проплачені російською владою або діють за власною ініціативою, із патріотичних помірковувань, та навіть можуть вести розмову, про що в одному із своїх відео більш детально розповів ізраїльський журналіст Сергій Ауслендер.

Активність “ботів” значно вище, ніж тих, хто намагається просувати іншу думку, через що і досягається така ефективність впливу. Як результат, кількість українців, що прагнуть миру ціною втрачених територій – зростає, що зменшує як фінансову допомогу збройним так і просування антиросійського настрою. Також, зростає кількість громадян країн заходу, які лояльні до російської агресії, що може вплинути на думку політиків, щодо необхідності надання допомоги Україні та українським біженцям. Вони, також, можуть провокувати окремих людей на активну розмову, виводити їх на емоції, через що користувачі можуть випадково порушити правила платформи та доступ яких може бути обмежений, через велику кількість скарг від ботів. Таке можливо через те, що технічна підтримка платформ реагує саме на заборонені слова та коментарі з негативним контекстом, а не на причину дискусії та її сутність.

У рамках вирішення цієї проблеми СБУ вже ліквідовувала ботоферми на території України, але значна їх кількість знаходиться закордоном. Припинити їх діяльність у соціальних мережах майже не можливо. Тому, я вважаю, що для протидії цим ботофермам треба створювати власні, які будуть формувати значну кількість коментарів та постів, в яких вже буде просуватися український норратив, розповсюджуватися інформація про військові злочини росії, пояснювати громадянам європейських країн, чому допомога Україні – це важливо і треба допомагати все більше. Зараз велика кількість громадян України виконує ці завдання, але цього замало. До населення країн заходу проукраїнська інформація доходить у значно меншій кількості, ніж проросійська. Також, можна спробувати домовитися із представниками компанії “Meta platforms” та “Google”, щодо впровадження системи обмеження доступу до платформ, власниками яких вони є, користувачам, які просувають норратив країни, що є державою-спонсором-тероризму. Також є важливим доносити більше інформації населенню України щодо ботоферм, як їм протидіяти, чому не можна вестись на провокації та який у цього може бути результат.

Література

1. Що таке ботоферма і як це працює: стаття. URL: ***https://qwaramedia.com/shho-take-botoferma-i-yak-cze-praczyuie/*** (дата звернення: 15.03.2023).

2. Намагаються розхитати державний лад України – як працюють кремлівські ботоферми та скільки їх: стаття. URL: ***https://vikna.tv/video/svit/shho-take-botofermy-kremlya-ta-yak-vony-praczyuyut/*** (дата звернення: 15.03.2023).

3. В Украине разоблачили две большие ботофермы – 7 тысяч ботов врали о ВСУ и восхваляли оккупантов: відео. URL: https://www.youtube.com/watch?v=E3RLpLcp3Jc (дата звернення: 15.03.2023).

Самчук А.О.
курсант НА СБ України

СТРАТЕГІЧНІ КОМУНІКАЦІЇ НАТО

Стратегічні комунікації впродовж останніх років займають важливе місце у діяльності Міністерства оборони України та й загалом у державних органів нашої держави, але зараз, в умовах війни, нам досить важливо отримувати досвід інших країн у цій сфері, бо російська федерація й надалі продовжує вводити у мережу ‘фейки”, які потрібно оперативно спростовувати, щоб населення не піддавалося впливу ворога.

Зараз на території України йде повномасштабна війна, а для застосування нашою державою інструменту стратегічних комунікацій проти мирного населення, вважаємо за доцільне звернутися до досвіду НАТО. Посол Німеччини в Україні Анка Фільдгаузен наголосила на тому, що: «Протидія дезінформації має посилювати верховенство права, щоб ми могли потім захистити свою позицію». Це вкрай важлива теза, тому що під час боротьби з пропагандою не варто забувати, що все це має відбуватися у правовому полі [1]. Різні стилі пропаганди мають на меті висвітлити свою правду як правильну. Наприклад, ми бачимо очевидні порушення з боку рф Женевської Конвенції, а загарбники методом абсолютної очевидності намагаються довести нам протележну інфомацію.

Терористичні організації та теракти у Європі у 2000-х роках все більше і більше змушували НАТО оновити свої стратегічні комунікації. Стратегічні комунікації спрямовані на підрив і делегітимізацію противника у спосіб набуття підтримки й визнання з боку місцевого населення, електорату своєї країни, міжнародного суспільств та інших груп. Активний розвиток теоретичних ідей та практики стратегічних комунікацій був зумовлений перебігом місії НАТО в Афганістані, точніше, допущеними там помилками. Ця ситуація зумовила, зокрема, рішення тодішнього Верховного головнокомандувача ОЗС НАТО в Європі генерала Джеймса Джонса про те, що діяльність у сфері стратегічних комунікацій має бути включеною до переліку завдань Штабу Верховного головнокомандувача ОЗС НАТО в Європі

Як свідчить практика військових місій НАТО, підтримка місцевого населення, населення країни в цілому та міжнародної спільноти є в край важливою. Населення країни дуже різко сприймає різну інформацію, тому потрібно вчасно спростовувати факти.

США у 2002 році створили Координаційний комітет з політики стратегічних комунікацій для «координації міжвідомчої активності та для того, щоб усі агентства працювали разом та з Білим домом для розвитку та поширення президентських меседжів по всьому світу» [2, 3]. Україна теж перейняла схожу систему. Щодо покращення рівня взаємодії керівництва держави з громадськістю

та побудови злагодженої системи комунікацій йдеться в затвердженій Концепції стратегічних комунікацій Міністерства оборони та Збройних Сил України (2017 р.)

Отже, система стратегічних комунікацій України перебуває на етапі становлення та удосконалення. Український уряд активно співпрацює з країнами-партнерами та міжнародними організаціями, зокрема з НАТО, про що свідчить підписання Дорожньої карти Партнерства, спрямованої на вдосконалення та використання зарубіжного досвіду у сфері стратегічних комунікацій. Налагодження чітких міжсекторальних комунікацій, розробка національної інформаційної стратегії та вдосконалення законодавчої бази є складовими ефективних державних комунікацій, які допоможуть протистояти інформаційним викликам і загрозам. Уряд України приділяє належну увагу технічному оснащенню і професійній підготовці фахівців у сфері стратегічних комунікацій, що дозволить координувати роботу як на стратегічному, так і тактичному рівнях.

Література

1. Як стратегічні комунікації допомагають Україні налагодити міжнародну співпрацю з протидії ворожій дезінформації . -2021 [Електронний ресурс]. – Режим доступу: https://armyinform.com.ua/2021/12/09/yak-strategichni-komunikacziyi-dopomagayut-ukrayini-nalagodyty-mizhnarodnu-spivpraczyu-z-protydiyi-vorozhij-dezinformacziyi/

2. Report of the Defense Science Board Task Force on Strategic Communication 2004 [Електронний ресурс]. – Режим доступу : http://www.acq.osd.mil/dsb/reports/ADA428770.pdf

3. Баровська А. Стратегічні комунікації: досвід НАТО Стратегічні пріоритети. – 2015. – No1. – С.147–152.

4. Сивак Т. Міжнародний досвід формування стратегічних комунікацій. - 2019, С. 82-85 [Електронний ресурс]. – Режим доступу: file:///C:/Users/Admin/Downloads/179084.pdf

5. NATO Communications and Information Agency. (2012). Strategic Communications for NATO: A Framework for Managing and Adapting Public Information. [Електронний ресурс]. Режим доступу : https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_06/20160601_160601-StratCom-Framework_en.pdf

6. Про затвердження Концепції стратегічних комунікацій Міністерства оборони України та Збройних Сил України [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/rada/show/v0612322-17#Text

Сенишак Ю.М.
Курсант НА СБ України
Добришин Ю.Є.
к.т.н., доцент НА СБ України

OSINT В НАЦІОНАЛЬНОЇ ОБОРОНІ ТА БЕЗПЕЦІ

Актуальність теми. Поняття OSINT (Open Source Intelligence) включає в себе збір та аналіз інформації, яка є загальнодоступною і також може надходити з різних джерел, таких як газети, соціальні медіа, телебачення та радіомовлення тощо. Саме можливості технології OSINT дозволяють використовувати інформацію для подальшого прийняття ефективних та зважених рішень та надає нові можливості для його використання, як перспективного інструменту розвідки у сфері національної оборони та безпеки. Важливими ознаками OSINT є:

- можливість завчасно попередити потенційні загрози національної безпеки та оборони, що дозволяє створювати умови вживання первинних заходів та прийняти обґрунтованих рішень щодо усунення загроз;
- надання інформації, яка має вирішальне значення для оцінки ризиків, пов'язаних із певним подіями та соціальними процесами, що відбуваються в країнах, регіонах на тій чи іншій території серед населення;
- оцінку інформації щодо намірів та діяльності іноземних урядів, організацій та окремих осіб з метою зрозуміння, яким чином інша країна буде себе поводити на міжнародній арені.
- суттєво зменшувати витрати щодо отримання необхідної інформації порівняно з іншими методами збору розвідданих, які зазвичай є дорогими і вимагають ретельної підготовки та планування.

Застосування OSINT для захисту національної оборони та безпеки неможливо залишити поза увагою, тому що аналіз джерел інформації на теперішній час є високоефективним засобом вивчення дій різних груп та осіб, які можуть становити загрозу безпеці нації. Така інформація може допомогти у визначенні потенційних цілей та моніторингу діяльності терористичних угруповань і злочинних організацій, які становлять загрозу безпеці країни.

Труднощі та особливості використання OSINT в Україні в умовах війни. Незважаючи на те, що технологія OSINT є цінним джерелом інформації, існують певні проблеми щодо його використання. Основними з них є:

- складності, які виникають під час обробки великої кількості інформації, доступної в Інтернеті;
- тривалий час, що відводиться на аналіз інформації, а також визначення її автентичності та відповідності джерелам, які були доступні;
- аналіз іноземних джерел, які потребують досконального знання різних мов, що ускладнює доступ до інформації та перешкоджає швидкому її аналізу;

- процес збору та аналіз інформації вимагає застосування спеціальних технічних навичок та інструментів, які можуть бути також платними, або доступними для обмеженого кола осіб;

- застосування технології OSINT повинно здійснюватися відповідно до нормативних документів, включаючи правові та етнічні стандарти, щоб уникнути порушення приватного життя та прав людини.

- відсутність методичних підходів та стандартних алгоритмів щодо збору та аналізу інформації за допомогою компонентів OSINT;

- неспроможність під час аналізу інформації здійснити оцінку фейкових новин і дезінформації в Інтернеті, що може призвести до неузгодженості та труднощів в кінцевій оцінці даних;

- можливість застосування технологій OSINT зловмисниками, які можуть отримати доступ до різної інформації, використовувати для цього різного роду кібератакі, здійснювати доступ до сайтів з метою отримання облікових даних та іншої інформації, яка могла стати доступною у разі витоку.

З початком повномасштабної російсько-української війни, застосування технологій OSINT стає більш актуальним та набуває нового рівня його використання. Збройні сили України здійснюють виявлення ворожих позицій, знаходять докази російських воєнних злочинів, розвінчують тези ворожої пропаганди й ще роблять чимало справді дивовижних речей.

Наприклад, після початку російської збройної агресії проти України та захоплення Криму, на початку 2014 року за допомогою OSINT активістами створений ресурс «ІнформНапалм». За час існування зазначеного проекту проведено два ґрунтовні розслідування щодо катастрофи «Боїнга-777», збитого у небі над Донеччиною, впорядковано бази даних російських підрозділів, які воюють в Україні, і навіть таблиці з шевронами військовослужбовців рф.

OSINT допомагає встановити пряму відповідальність за військові злочини, скоєні в різних містах України. Документування військових злочинів, скоєних російськими окупаційними військами в Україні (яке пізніше може бути використаним для Гааги), передбачає використання відкритих джерел, таких як фотографії, відео, публікації в соціальних мережах, супутникові зображення та карти для розслідування та збору доказів для судових справ. Журналісти регулярно збирають дані про підтверджені жертви серед цивільного населення, пошкодження цивільних будинків та інфраструктури з 24 лютого 2022 року.

Одним із яскравих прикладів ефективного використання OSINT є запобігання спробам Росії приховати вбивства в Бучі. Так за допомого OSINT американська компанія супутникового знімання «Maxar Technologies», надала зображення тіл, знайдених у Бучі до того, як російські війська залишили місто, які допомогли довести, що росіяни брешуть про свою невинуватість.

Завдяки аналізу кількості російських військових невдач і українських успіхів, експерти змогли підняти моральний дух громадян України на початку війни, що

на теперішній час продовжує відіграти ключову роль у перемоги України з агресором.

Висновки. Отже, OSINT – це важливий інструмент національної безпеки та оборони, оскільки він допомагає збирати, аналізувати та поширювати інформацію, доступну у відкритих джерелах, таких як соціальні мережі, онлайн-новини. Крім того, OSINT є критично важливим інструментом у процесах прийняття рішень, пов'язаних з національною безпекою та обороною. Інформація, зібрана через OSINT, може допомогти політикам, військовим та навіть поліцейським у їхній діяльності.

OSINT зазвичай виконується за допомогою автоматизованих інструментів, таких як спеціалізоване програмне забезпечення, призначене для пошуку за певними ключовими словами, фразами або темами. Методи, які використовуються в OSINT, залежать від типу шуканої інформації, доступних ресурсів і бажаних результатів.

Література

1. Мартинюк С.О. Характеристика принципів функціонування osint у сфері національної безпеки. *Юридичний науковий електронний журнал*. 2021., №9. С 332-333.

2. Ржевська Н.Ф., Кожушко О.О. Розвідка відкритих джерел.(OPEN SOURCE INTELLIGENCE). Україна в системі глобального інформаційного обміну: теоретико-методологічні аспекти дослідження і підготовки фахівців: всеукраїнська наукова конференція, Львів, 27 травня 2011. Національний університет "Львівська політехніка". Львів: 2011. С. 257–261. веб-сайт. URL: https://ena.lpnu.ua:8443/server/api/core/bitstreams/a964dfbb-a16d-4e8a-b621-9aa6cb277197/content (дата звернення: 13.03.2023).

3. Технології OSINT: як відкриті джерела допомагають медівникам. Київ: Press Association UA, 2019. веб-сайт. URL: https://pressassociation.org.ua/ua/tehnologii-osint-yak-vidkriti-dzherela-dopomagayut-medijnikam/ (дата звернення: 14.03.2023).

Супрун А.О.
студентка НА СБ України
Науковий керівник:
Гоц О.В.
старший викладач кафедри ОЗІОД ННІ ІБ СК НА СБ України

АКТУАЛЬНІСТЬ ВЕДЕННЯ КОНКУРЕНТНОЇ РОЗВІДКИ В УМОВАХ СЬОГОДЕННЯ

В умовах глобалізації економіки інформаційна боротьба набирає значних обертів. Вона ведеться явно і приховано між державами, підприємствами і фірмами на захист власних інтересів, поділу зон впливу, ринків збуту, власності тощо. Щоб ефективно протидіяти конкурентам, необхідно знати, як діяти в конкретних умовах і якими засобами забезпечувати цю протидію [1].

Розвиток суспільства на даному етапі можна охарактеризувати зростаючою роллю інформаційного середовища, яке представляє собою сукупність інформації, інформаційної інфраструктури, суб'єктів, які здійснюють збір, формування, розповсюдження і використання інформації, а також системи регулювання виникаючих при цьому суспільних відносин. Інформаційна сфера активно впливає на стан політичної, економічної, соціальної та інші складові безпеки будь-якого підприємства.

В умовах жорсткої конкуренції сфера безпечного функціонування настільки звузилася, що постійне й масове незадоволення конкретної потреби негативно впливає на функціонування і розвиток окремих громадян, сімей, організацій, держави і суспільства в цілому, поглиблюючи кризовий стан їх життєдіяльності. Саме тому забезпечення економічної безпеки належить до числа національних пріоритетів і є гарантією незалежності країни, умовою стабільності й ефективності життєдіяльності та розвитку суспільства. Це пояснюється тим, що економіка є однією з найважливіших сторін діяльності особи, організації, держави. Без ефективної економіки неможливо забезпечити національну безпеку [2, с.4].

Проблеми оцінки конкурентного середовища звертали на себе увагу багатьох поколінь практиків і науковців. Створювалися і застосовувалися моделі аналізу і оцінки конкурентного середовища з різними припущеннями. Однак і в даний час питання застосування економічного інструментарію, що дає найбільш повне уявлення про взаємозв'язок господарюючого суб'єкта з зовнішнім середовищем, не втратив своєї значимості. Особливо актуальна в умовах глобалізації проблема підвищення ефективності реалізації відносин власності за рахунок розробки та впровадження нових методик оцінки діяльності конкурентів, що дозволяють найбільш адекватно оцінювати конкурентне середовище і визначати заходи реагування на зміни в ньому [3, с.7].

З моменту ведення російською федерацією спочатку гібридної, а тепер і повномасштабної війни проти України, ми можемо побачити значний інформаційний вплив на населення нашої держави, що в свою чергу значно ускладнює боротьбу проти країни-агресора.

Необхідність створення методичного забезпечення для більш повного економічного аналізу, що відповідає сучасному стану розвитку нашого суспільства, аналізуючи виклики і загрози, що постали перед країною, підтверджує актуальність обраної теми.

Концепція конкурентної розвідки представляє собою обґрунтовану систему поглядів на визначення основних напрямків, умов і порядку практичного вирішення завдань з організації легальної розвідувальної діяльності в умовах гострої конкурентної боротьби. Сучасний вітчизняний і зарубіжний досвід показує, що жодна особа, жодна організація не можуть ефективно діяти в умовах гострої конкурентної боротьби без глибокого і всебічного аналізу зовнішнього середовища або не маючи новітньої, повноцінної і достовірної інформації про те, що в ньому відбувається [5, с.5].

Конкурентна розвідка – це постійний процес збору та обробки інформації для підвищення конкурентоспроможності підприємства серед інших компаній певної галузі, а також дослідження зовнішнього середовища компанії [5, с.19].

Дослідження сутності конкурентної розвідки показало, що її головним завданням є отримання стратегічно важливої інформації про наміри конкурентів і партнерів, про їхню цінову політику, про стратегію розвитку, про їхні сильні та слабкі сторони, про вироблену ними продукцію, про стан ринку на якому працює компанія, основні ризики, тощо [4, с. 28]. Конкурентна розвідка також повинна бути націлена на швидке та ефективне вирішення проблем, які стоять перед будь-яким підприємством, незалежно від того, яка його сфера діяльності. Тобто основним завданням є забезпечення захисту інформаційної системи підприємства від прямих посягань конкурентів. Важливим є те, що діяльність конкурентної розвідки повинна бути безперервна та циклічна.

Правильно підібрані методи, технології та інструменти формують універсальну систему для оперативного реагування на будь-які зміни, що в подальшому нададуть можливість приймати правильні управлінські рішення.

Отже, використання конкурентної розвідки має під собою наступну мету: бажання визначити реальну стратегію конкурентів для корегування власної, визначити потенціал головних конкурентів (їх сильні й слабкі сторони), визначити організаційні, фінансові, технічні й інші способи забезпечення конкурентних переваг, оцінка ступеня вигідності умов співпраці з тими або іншими постачальниками, партнерами та покупцями.

Незважаючи на існування великої кількості методів розвідувальної діяльності підприємства, конкурентна розвідка посідає провідне місце у зборі та аналізі відкритої інформації про ринки, технології та провідних гравців. Вона

функціонує на високому професійному (аналітичному) рівні, з дотриманням усіх найсуворіших норм ділової етики [4].

Забезпечення доступу та сам процес отримання актуальної та достовірної інформації, вимагає наявності поновлюваних інформаційних ресурсів. Важливу роль в цьому відіграють сучасні технічні засоби та наявність індивідуального програмного забезпечення. Це дозволяє збирати, аналізувати та зберігати інформацію, отриману з різних джерел, для подальшої результативної обробки отриманих інформаційних даних, формування на цій основі обґрунтованих висновків та прогнозів необхідних висококваліфікованим фахівцям-аналітикам для прийняття рішень [4].

Використання аналітичних методів конкурентної розвідки (SWOT-аналіз, SPACE-аналіз, PEST-аналіз, методика аналізу конкурентів за Портером) дозволяє компанії успішно здійснювати прогноз кризових явищ в бізнесі. Тим самим своєчасно визначити можливість їх розвитку, провести локалізацію та вжити заходи попереджувального та профілактичного характеру. Володіння інформацією про можливу або майбутню кризу використовується в інтересах зміцнення свого становища та для ослаблення можливостей і ролі конкурента на ринку, перешкоджає їх діяльності.

Для прийняття якісного управлінського рішення необхідно розглядати усі сторони конкурента та використовувати декілька методів аналізу для більш достовірного і точного результату, в кожному випадку підходити до збору інформації творчо, ґрунтовно та використовувати тільки перевірені джерела інформації.

Повномасштабна війна російської федерації проти України вплинула і на діяльність компаній, які займаються конкурентною розвідкою. Посилилось державно-приватне партнерство. Багато українських спеціалістів з конкурентної розвідки спрямували свою діяльність на допомогу Збройним силам України у сфері OSINT. Зокрема, у здобутті інформації з відкритих джерел стосовно дислокації та переміщення ворога, наявності та складу ворожої техніки тощо. Яскравим прикладом є діяльність компанії Molfar [6], яка сконцентрувала свою діяльність на військових розслідуваннях, фактчекінгу, пошуку інформації та аналітиці.

Література

1. Горбаль Н. І., Смерека Л. В., Микитин О. З. Конкурентна розвідка: сутність, значення, перспективи розвитку. *Менеджмент та підприємництво в Україні: етапи становлення та проблеми розвитку.* 2019. Вип. 2. С.53-60

2. Керницький І.С., Живко З.Б., Копитко М.І. Конкурентна розвідка підприємств: курс лекцій. Львів: Ліга-Прес, 2015. 388 с.

3. Кирій В.В., Солодкий В.С., Тімофєєв В.О. Конкурентна розвідка та контррозвідка: навч. посіб. Харків: ХНУРЕ, 2015. 380 с.

4. Когут Ю.І. Конкурентна розвідка та безпека бізнесу: практ. посіб. Київ: Консалтингова компанія «СІДКОН» ВД Дакор, 2021. 318 с.

5. Ткачук Т. Ю. Конкурентна розвідка: навч. посіб. Київ: НАСБ України, 2013. 295 с.

6. OSINT-спільнота Molfar. URL: https://www.molfar.global/ (дата звернення 19.03.2023).

Софієнко К.С.
старший консультант 1 відділу
3 служби УРОС СБ України

ДО ПИТАННЯ НАСТАВНИЦТВА В УКРАЇНІ

Зростання конкуренції на світовому ринку, впровадження нових технологій і технічних засобів зумовлюють потребу в удосконаленні навичок працівників і необхідність у безперервному професійному навчанні та постійному підвищенні рівня кваліфікації персоналу. А тому під час дії правового режиму воєнного стану в Україні важливе значення мають окремі питання наставництва в Україні.

Наставництво передбачає навчання безпосередньо на робочому місці шляхом передання досвідченими працівниками набутого досвіду і знань особі, що потребує професійного навчання та формування необхідних навичок [1].

До переваг наставницької діяльності підприємств варто віднести: по-перше, забезпечення якості та ефективності професійного навчання молодих працівників з урахуванням реальних потреб й інтересів підприємств; по-друге, зменшення часу на освоєння нової техніки і виробничих технологій, витрат на навчання та підвищення кваліфікації працівників; по-третє, створення єдиного освітнього простору підприємств; по-четверте, прискорення адаптації молодих працівників до умов їхньої роботи на підприємствах, оволодіння ними виробничими функціями, галузевими та корпоративними стандартами [3]. Наставництво використовується для різних категорій населення: осіб, які вперше прийняті на посади; молодих працівників, які закінчили вищі та професійно-технічні навчальні заклади, та осіб, які переведені на інші посади, якщо виконання ними функціональних обов'язків потребує більше ґрунтовних професійних знань, нових практичних навичок та вмінь. Також наставництво може поєднуватися зі стажуванням або керівництвом виробничою практикою студентів та учнів професійно-технічних навчальних закладів.

Сучасна система наставництва з'явилася ще у XX ст., має тривалий шлях розвитку та на протязі свого існування довела свою ефективність та важливість, особливо для молодого покоління, яке тільки починає свій трудовий шлях та потребує професійної та моральної підтримки.

У вітчизняній практиці наставництво розвинулось у масовий рух у системі професійно-технічної освіти та професійного навчання на виробництві з кінця XX ст. як форма професійної адаптації та професійного розвитку на виробництві. Наставник забезпечує підопічному супровід, ділиться досвідом, знаннями та підтримує його протягом періоду адаптації. Основним завданням діяльності наставників є якісне виконання новопризначеними працівниками усіх вимог виробництва, сприяння їхній професій та соціальній адаптації, закріплення на виробництві та професійне зростання.

Якщо мову вести про УРСР, то позитивним було те, що дієвою школою наставництва були свого часу трудові династії, які брали активну участь в роботі з молодими робітниками. У 1980-х роках в Україні нараховувалось 2,6 млн. наставників, було запроваджено почесне звання «Заслужений наставник молоді», присвоювалось звання «Кращий наставник молоді» [3, с. 33]. На думку автора, трудові династії позитивно впливали на наступність поколінь та економіку країни в цілому.

Якщо мову вести про сучасний період, то для прикладу варто зазначити, що у Положенні про наставництво у Державному бюро розслідувань зазначено, що «наставництво може бути над новопризначеним працівником ДБР, у якого досвід роботи за відповідним напрямом становить менше трьох років та який потребує набуття нових практичних навичок і вмінь для виконання службових обов'язків за посадою. Наставництво здійснюється безпосередньо під час виконання службових обов'язків новопризначеним працівником ДБР та встановлюється на строк до шести місяців (у разі потреби строк наставництва може бути продовжено до одного року».

Таким чином, зробивши окремий екскурс в історію варто констатувати, що наставництво позитивно впливає на управління та формування трудового потенціалу і службової діяльності будь-якої організації в цілому, підвищує престиж робітничих професій, забезпечує стабільність виробництв, впливає на кар'єрне зростання, зменшує плинність кадрів тощо, а в умовах правового режиму воєнного стану в Україні це невід'ємне питання для підвищення економічного потенціалу країни.

Література

1. Наказ Мінсоцполітики України «Про затвердження Методичних рекомендацій щодо запровадження наставництва» № 1611 від 11.10.2017 р.

2. Терюханова І.М, Дрозач М.І., Стульпінас Н.К. Проблеми та перспективи розвитку наставництва в Україні / «SOCIOПРО СТІР: міждисциплінарний електронний збірник наукових праць з соціології та соціальної роботи». № 6. 2017. с. 31-38.

3. Наказ «Державного бюро розслідування» від 22.02.2022 р. № 112 (у редакції наказу Державного бюро розслідувань від 11.08.2022 р. № 402).

Требенко Т.С.
Національна академія СБ України

ЗАХИСТ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ В УМОВАХ ПОВНОМАСШТАБНОЇ ЗБРОЙНОЇ АГРЕСІЇ рф

Захист інформації з обмеженим доступом в умовах повномасштабної збройної агресії рф вимагає спеціальних заходів, що повинні бути здійснені згідно з вимогами законодавства та міжнародних стандартів, з метою забезпечення безпеки критичної інформаційної інфраструктури України.

У зв'язку з проведенням повномасштабної збройної агресії рф на території України, захист інформації з обмеженим доступом стає надзвичайно важливим завданням для забезпечення національної безпеки. Для цього необхідно вжити спеціальних заходів, які будуть відповідати вимогам законодавства та міжнародних стандартів. [3]

Один зі способів захисту інформації з обмеженим доступом - це забезпечення безпеки критичної інформаційної інфраструктури України. Згідно зі статтею «Сучасні загрози інформаційній безпеці країни та шляхи їх подолання» , це означає захист інформації, яка стосується критичної інфраструктури (електроенергетика, транспорт, зв'язок, інформаційні технології тощо) від несанкціонованого доступу, використання, розголошення або знищення в умовах загрози безпеці держави.[2]

Згідно з дослідженнями, для забезпечення захисту інформації в умовах війни в Україні використовуються спеціальні технічні та організаційні заходи, такі як шифрування даних, використання захищених засобів зв'язку та забезпечення кібербезпеки. [2]

Проте, окрім технічних та організаційних заходів, важливо також враховувати правові аспекти забезпечення захисту інформації з обмеженим доступом. Зокрема, за вимогами законодавства України (зокрема, Закону України "Про захист інформації в інформаційно-телекомунікаційних системах"), інформація з обмеженим доступом повинна бути об'єктом захисту від несанкціонованого доступу, використання, розголошення або знищення.[1]

Крім того, важливо дотримуватися міжнародних стандартів забезпечення захисту інформації, зокрема, конвенції Ради Європи про захист осіб щодо автоматизованої обробки персональних даних та конвенції ООН про права дитини, які встановлюють права та обов'язки у забезпеченні захисту персональних даних.

З метою ефективного захисту інформації з обмеженим доступом в умовах повномасштабної збройної агресії рф, необхідно також забезпечити моніторинг та аналіз потенційних загроз безпеці інформації, виявлення та реагування на випадки

порушення інформаційної безпеки, а також підготовку та навчання персоналу з питань захисту інформації. [4]

Отже, захист інформації з обмеженим доступом в умовах повномасштабної збройної агресії рф є надзвичайно важливим завданням для забезпечення національної безпеки України. Це вимагає вжиття спеціальних заходів, які повинні відповідати поточній ситуації та міжнародним стандартам забезпечення захисту інформації. Такі заходи повинні включати технічні, організаційні та правові аспекти, зокрема, використання захищених засобів зв'язку, забезпечення кібербезпеки, дотримання вимог законодавства та міжнародних стандартів забезпечення захисту інформації, моніторинг та аналіз потенційних загроз, виявлення та реагування на випадки порушення інформаційної безпеки, а також підготовку та навчання персоналу з питань захисту інформації. [3]

Для ефективного захисту інформації з обмеженим доступом необхідно також забезпечити співпрацю між різними державними органами та відповідальними за захист інформації установами, зокрема, Міністерством оборони, Службою безпеки України, Національною поліцією, Державною службою спеціального зв'язку та захисту інформації України, а також співпрацю з міжнародними партнерами з питань кібербезпеки та захисту інформації. [1]

Важливо також зазначити, що захист інформації з обмеженим доступом є постійним процесом, який повинен адаптуватися до змін у загрозах та технологіях. Тому, важливо забезпечувати постійну підготовку та навчання персоналу, вдосконалення технічних та організаційних заходів, а також співпрацю з міжнародними експертами та партнерами з питань захисту інформації.

Література

1. Верховна Рада. Закон України “Про захист інформації в інформаційно-комунікаційних системах”./ Верховна Рада України, Київ: Парлам. вид-во, 2007. 192-198с. Режим доступу: [https://zakon.rada.gov.ua/laws/show/85-16]

2. Слінько Т. Сучасні загрози інформаційній безпеці країни та шляхи їх подолання. Інформаційне суспільство: науковий журнал, 17-23с. Режим доступу: [https://www.constjournal.com/pub/4-2021/suchasni-zahrozy-informatsiyniy-bezpetsi-krainy-shliakhy-ikh-podolannia/]

3. Постанова НКРЕКП «Щодо захисту інформації, яка в умовах воєнного стану може бути віднесена до інформації з обмеженим доступом, у тому числі щодо об’єктів критичної інфраструктури»: за станом 26.03.2022, Офіц. вісник України, (100), 36-37с. – Режим доступу: [https://zakon.rada.gov.ua/laws/show/v0100500-18]

4. Ковальчук, І. В., Степаненко, О. В. Вимоги до захисту інформації у воєнний час [Requirements for information protection in wartime]: науковий вісник НЛТУ України, 111-114с.Режим доступу: [https://doi.org/10.36930/40291019]

Філон А.С.,
курсант,
Національної академії СБ України
Самойленко О.О.,
д.пед.н, доцент
ННІІБСК НА СБ України
Макаренко В.В.
к.ю.н., с.н.с.

ПРАВИЛА ЗАХИСТУ ІНФОРМАЦІЇ

Протягом століть інформація завжди набуває статусу важеля впливу. «Знай ворога, і знай себе – і можеш боротися в сотнях битв, не боячись поразки» - підкреслює цінність даних Сунь Цзи у трактаті «Мистецтво війни». Гостра необхідність захисту інформації у сучасних умовах спричинена масовим розповсюдженням і ускладненням інформаційних технологій, зростанням можливості несанкціонованого впливу на інформацію в процесі її зберігання, передачі та обробки. Найрізноманітніші технічні, а особливо електронні засоби трудової діяльності, засоби зв’язку і допоміжні засоби становлять небезпеку виникнення каналів витоку інформації. Захист інформації передбачає визначення можливих каналів її витоку, оцінювання важливості інформації та розроблення заходів для попередження її витоку й викрадення. [1]

Захист інформації з обмеженим доступом в умовах збройної агресії РФ може стати дуже складною задачею. В умовах збройної агресії може бути дуже важко контролювати доступ до інформації з обмеженим доступом. Наприклад, якщо комп'ютерні системи, що зберігають цю інформацію, розташовані на території, яку контролюють нападники, то можуть виникнути складнощі з їх захистом. Важливим аспектом є захист інформації від перехоплення. Умови збройної агресії можуть спричинити збільшення кількості спроб перехопити інформацію з обмеженим доступом. Наприклад, нападники можуть використовувати технічні засоби для злому систем безпеки або перехоплення мережевого трафіку. Захист інформації з обмеженим доступом також може ускладнити комунікацію між військовими підрозділами та владними структурами. Наприклад, у разі, якщо зв'язок між підрозділами переривається, може виникнути проблема з передачею інформації та зв'язку з командним центром. Водночас зберігання резервних копій інформації з обмеженим доступом також має певні ризики. Наприклад, можуть бути проблеми з забезпеченням захисту копій від знищення під час війни. Надійний захист інформації з обмеженим доступом також залежить від професіоналізму та знань кадрів, з їх цілеспрямованих дій в умовах збройної агресії. Це означає, що необхідно мати належно підготовлений та організований персонал, який здатний ефективно захищати інформацію з обмеженим доступом в

умовах конфлікту. Наприклад, кадри повинні бути підготовлені до виявлення та запобігання спробам підриву безпеки, а також знати про процедури захисту інформації та вміти застосовувати їх у практичних ситуаціях. Додатково, можуть бути встановлені додаткові вимоги до перевірки здібності персоналу зберігати конфіденційну інформацію, в тому числі створення умов для забезпечення дотримання режиму обмеженого доступу, відповідальності за проголошення та виконання заходів безпеки [2].

Отже захист інформації з обмеженим доступом в умовах збройної агресії вимагає комплексного підходу та ретельного планування. Належно організовані команди, дисципліновані процедури та відповідальне керівництво є ключовими чинниками успішного захисту цінної інформації в умовах війни. Правила захисту інформації - це набір правил та процедур, що регулюють доступ до інформації, її зберігання, передачу та використання з метою забезпечення її конфіденційності, цілісності та доступності [3].

Основні принципи захисту інформації:

1. Конфіденційність: інформація повинна бути захищена від несанкціонованого доступу та використання.
2. Цілісність: інформація повинна бути захищена від випадкових або навмисних змін.
3. Доступність: інформація повинна бути доступною для користувачів, які мають право на доступ.
4. Аутентифікація: ідентифікація користувачів та перевірка їхніх прав на доступ до інформації.
5. Авторизація: контроль доступу до інформації та обмеження прав користувачів на її використання.
6. Аудит: моніторинг доступу до інформації та збір інформації про дії користувачів.
7. Забезпечення безпеки: застосування технічних та організаційних заходів для забезпечення захисту інформації від несанкціонованого доступу, втрат, витоків, пошкодження чи розголошення.
8. Оцінка: періодична оцінка ризиків та оновлення правил та процедур захисту інформації для забезпечення її ефективного захисту.

Правила захисту інформації можуть варіюватися в залежності від конкретних вимог і потреб кожної організації або компанії. Однак, існують загальні правила, які можуть бути застосовані для захисту будь-якої інформації:

- Паролі. Використовуйте складні паролі, які складаються з букв, цифр та спецсимволів. Надзвичайно важливо не використовувати один і той же пароль для декількох облікових записів.
- Шифрування. Шифрування даних є ефективним методом захисту інформації.
- Оновлення програмного забезпечення. Потрібно регулярно

оновлювати програмне забезпечення на комп'ютері та мобільному пристрої для запобігання вразливості інформації, використовувати програмне забезпечення для захисту інформації, таке як антивірусні програми, брандмауери та програми шифрування.

- Безпека мережі. Варто переконатись у безпеці мережі та встановити захисні програми для захисту від зловмисного програмного забезпечення та інших загроз.
- Двофакторна аутентифікація. Доцільним є використання двофакторної аутентифікації для доступу до важливої інформації.
- Видалення конфіденційної інформації. Не варто зберігати конфіденційну інформацію після використання.
- Аудит. Аудити допомагають перевіряти те, як інформація зберігається, обробляється та передається в організації, та виявляти можливі загрози та вразливості.

Таким чином, захист інформації є пріоритетним напрямом розвитку інформаційних технологій. Варто пам’ятати та слідувати правилам захисту інформації, адже, безсумнівно, набагато легшим завданням є передбачити та попередити можливі деформацію чи пошкодження даних, а ніж приймати заходи після безпосереднього впливу на інформацію.

Література

1. В. О. Хорошко, М. В. Капустян. Захист інформації. Енциклопедія Сучасної України: онлайн-версія / редкол.: І. М. Дзюба та ін.; НАН України, НТШ. Київ: Інститут енциклопедичних досліджень НАН України, 2010. URL: https://esu.com.ua/article-15872

2. Про захист інформації в інформаційно-комунікаційних системах: Закон України. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80 (дата звернення: 18.03.2023).

3. Комісаров В. Ю., Курило Н. Захист інформації з обмеженим доступом. Military science, national security and sports. 2019. № 4. URL: https://www.ukrlogos.in.ua/10.11232-2663-4139.04.05.html (дата звернення: 18.03.2023).

Федірко Д.А.
курсант НА СБ України
Дацюк М.В.
курсант НА СБ України

ТЕХНІКА І РОЛЬ В УПРАВЛІННІ ЛЮДСЬКОЮ СВІДОМІСТЮ

Вступ. Сьогодні у демократичних країнах обличчя політика і, відповідно, його шанси на перемогу у виборах визначають не ідеології, а переважно політичні технології, зокрема конкретна сфера їх застосування – політична реклама. Одним із популярних нині методів політичної реклами, який чи не найкраще характеризує такий стан, стало нейролінгвістичне програмування (Neurolinguistic Programming (NLP) – управління людською свідомістю за допомогою лінгвістичних конструкцій, архетипів, візуальних зображень тощо.

Україна тільки сьогодні вступає у фазу застосування цих «високих» технологій – усі попередні вибори здебільшого проходили з використанням стандартних методик політичної реклами, без застосування психологічних факторів впливу на електорат.

Поняття NLP та управління. NLP – це сфера штучного інтелекту, яка займається розумінням і обробкою людської мови. NLP включає низку методів, таких як машинне навчання, статистичний аналіз, семантичний аналіз, обробка даних та інші, які дозволяють комп'ютерам розуміти та створювати людську мову.

Управління – це процес планування, організації, контролю та спрямування ресурсів для досягнення конкретних цілей. NLP може відігравати важливу роль в управлінні, особливо в управлінні даними та відносинах з клієнтами.

Одними із найпоширеніших методів NLP є:

-токенізація передбачає поділ фрагмента тексту на менші одиниці, які називаються токенами. Це полегшує обробку тексту та вилучення з нього інформації;

- додавання тегів до частин мови: передбачає визначення частини мови (іменника, дієслова, прикметника тощо) кожного слова у фрагменті тексту. Це може бути корисно для розуміння сенсу тексту та вилучення з нього інформації;

-аналіз настроїв: аналіз настроїв або емоцій, виражених у фрагменті тексту. Це може бути корисно для таких завдань, як обслуговування клієнтів і моніторинг соціальних мереж;

-машинний переклад: це передбачає автоматичний переклад тексту з однієї мови на іншу. Це може бути корисним для таких завдань, як міжнародне спілкування та локалізація;

-пошук інформації: це передбачає пошук відповідної інформації з великого масиву тексту. Це може бути корисним для таких завдань, як пошукові системи та системи відповідей на запитання;

- генерація тексту, яка дозволяє автоматично створювати текстові повідомлення, електронні листи, звіти тощо. Це може допомогти менеджерам ефективніше спілкуватися зі своїми колегами та клієнтами. Існує багато інших методів і технік NLP, і постійно розробляються нові. Вибір методу залежить від конкретного завдання і характеру аналізованого тексту.

Застосування технік NLP. NLP можна використовувати для розуміння емоцій і настрою клієнтів на основі їхньої мови, що допомагає краще зрозуміти їхні потреби та запити, а також для автоматичного перекладу, який може допомогти менеджерам спілкуватися зі своїми колегами та партнерами з інших країн.

Техніки NLP (обробка природної мови) можуть бути застосовані різними способами для покращення управління організацією. Ось кілька прикладів/

Чат-боти та віртуальні помічники: методи NLP можна використовувати для створення чат-ботів і віртуальних помічників, які можуть відповідати на запитання клієнтів, надавати підтримку та виконувати інші завдання. Це може допомогти організаціям скоротити час очікування клієнтів і підвищити якість обслуговування клієнтів.

Вилучення інформації. Техніки NLP можуть бути використані для вилучення відповідної інформації з документів, електронних листів та інших джерел неструктурованих даних. Це може допомогти організаціям автоматизувати такі завдання, як перегляд контрактів, обробка рахунків-фактур та інші адміністративні завдання.

Класифікація тексту. Методи NLP можна використовувати для класифікації документів та інших фрагментів тексту за категоріями, такими як відгуки клієнтів, маркетингові матеріали та юридичні документи. Це може допомогти організаціям ефективніше керувати своїми документами та автоматизувати такі завдання, як маршрутизація та архівування документів.

Персоналізація: методи NLP можна використовувати для аналізу даних про клієнтів і надання персоналізованих рекомендацій і маркетингових повідомлень. Це може допомогти організаціям покращити залучення клієнтів і збільшити продажі.

Методики NLP можуть допомогти організаціям підвищити свою ефективність, задоволеність клієнтів і загальну продуктивність шляхом автоматизації завдань, покращення комунікації та надання інформації про потреби та вподобання клієнтів.

NLP (обробка природної мови) може відігравати важливу роль в управлінні, зокрема в управлінні даними та відносинах з клієнтами. Ось кілька прикладів того, як NLP можна використовувати в менеджменті:

Управління даними: NLP можна використовувати для отримання корисної інформації з великої кількості неструктурованих даних, таких як відгуки клієнтів, публікації в соціальних мережах і новинні статті. Це може допомогти менеджерам

визначати тенденції та проблеми, важливі для їхнього бізнесу, і приймати більш обґрунтовані рішення.

Відносини з клієнтами: NLP можна використовувати для аналізу відгуків і настроїв клієнтів, а також для виявлення проблем і областей для покращення. Це може допомогти менеджерам підвищити рівень задоволеності та утримання клієнтів, а також розробити кращі продукти та послуги.

Комунікація: NLP можна використовувати для покращення комунікації між менеджерами та співробітниками, а також між менеджерами та клієнтами. Наприклад, чат-боти та віртуальні помічники можна використовувати, щоб відповідати на запитання клієнтів і надавати підтримку, а текстове підсумовування можна використовувати для швидкого підсумовування важливої інформації для зайнятих менеджерів.

Автоматизація: NLP можна використовувати для автоматизації таких завдань, як перегляд контрактів, обробка рахунків-фактур та інші адміністративні завдання. Це може допомогти менеджерам заощадити час і зменшити кількість помилок, а також зосередитися на більш важливих завданнях.

Прийняття рішень: NLP можна використовувати, щоб надати менеджерам уявлення про потреби та вподобання клієнтів, а також про ринкові тенденції та конкурентів. Це може допомогти менеджерам приймати більш обґрунтовані рішення та розробляти більш ефективні стратегії для свого бізнесу.

Загалом NLP може бути цінним інструментом для менеджерів у аналізі й обробці великих обсягів даних, розумінні потреб і переваг клієнтів, покращенні комунікації, автоматизації завдань і прийнятті більш обґрунтованих рішень.

Висновок. Під час дослідження було виявлено ,що NLP може бути цінним інструментом для менеджерів у аналізі та обробці великих обсягів даних, створенні звітів і повідомлень, розумінні потреб клієнтів і ефективній комунікації з колегами та партнерами.

Отже, NLP являє собою процес прискореного навчання і перенавчання, позбавлення від небажаних стереотипів поведінки, створення їх нових програм. Нейролінгвістичне програмування є поєднанням психотерапії образу та теорії слова. Його особливістю є відсутність будь-якого роду навіювань чи впливів, а пропонування вибору необхідної для людини програми. Набір технологічного інструментарію цієї новітньої науково-прикладної галузі - нейролінгвістичного програмування, сьогодні застосовують у різних галузях людської діяльності, а останнім часом все активніше в активізуванні найважливіших домінант комунікативних процесів, зокрема - прийняття управлінських рішень.

Література

1. Ходаківський Є. І, Богоявленська Ю.В, Грабар Т. П. Психологія управління. Центр учбової літератури. 2008., 608 с.

2. Петрик В.М., Гнатюк С.О., Черненко О.Є., Гурєєв В.О. Сучасні технології нейролінгвістичного програмування. ВД «Сварог». 2020., 200 с.
3. Р.Ділтс, Т. Халбом, С. Сміт. Зміна переконань. Психотехнології рівня NLP-майстер. М.: Незалежна асоціація психологів-практиків, 1997., 192 с.
4. Комінко С.Б. Психологія в менеджменті. Тернопіль, 1999, 400с.

Філон А.С.
курсант Навчально-наукового гуманітарного інституту
Національної академії Служби Безпеки України

КОМУНІКАТИВНІ ТРАДИЦІЇ УКРАЇНСЬКОГО КОЗАЦТВА

На героїну добу Козаччини випала низка перешкод. Період кінця XV століття та першої половини XVII століття в Україні характеризувався складними політичними та соціально-економічними умовами. Відсутність єдиної держави та постійні війни сприяли розвитку специфічної системи комунікацій у козацькому середовищі. Козацтво, що складалося з маленьких груп, повинне було підтримувати ефективно зв'язок між собою, а також із владою та населенням.

Козацьке середовище кінця XV століття і першої половини XVII століття характеризувалося розвиненою системою комунікацій, що була необхідною умовою для успішної організації козацького співтовариства. Основними напрямами розвитку комунікацій у цей період були:

1. Усна комунікація. Козацька ораторська майстерність, що розвивалася на базі усного народного мистецтва, була важливим інструментом міжособистісних та міжкультурних комунікацій. Усні традиції передавалися з покоління в покоління, що забезпечувало їх життєздатність та розвиток.
2. Писемна комунікація. У період розквіту козацтва у другій половині XVI століття з'явилися перші письмові джерела – листи, розсилки, грамоти, універсали, які були обов’язковими для всього населення, а також перші газети та книги. Розквіту набула і зовнішня комунікація із сусідніми державами Московією та Річчю Посполитою через листи, звернення до влади. У XVII столітті козацька писемність розвинулася до значного рівня. Перші друковані видання з'явилися в Гетьманській Україні на початку XVIII століття.
3. Візуальна комунікація. У козацькому середовищі розвивалися візуальні форми комунікації, такі як символіка, малюнки на зброї, візерунки на одязі та предметах побуту. Ці засоби сприяли формуванню колективної свідомості та були основою комунікації безпосередньо на полі бою. Візуальні жести слугували особливий шифром, який був здатний проінформувати козацьку спільноту, не набуваючи розголосу для ворога. Наприклад вагомим засобом візуальної комунікації на полі бою був Військовий Прапор, з підняттям якого

козацькі полки були проінформовані про наступ. Крім того, козаки використовували спеціальні позначки, які допомагали їм зорієнтуватися на місцевості та передавати важливі повідомлення.

У період кінця XV ст. - 1649 р. основними засобами комунікації були пошта, кур'єри, сигнальні вогні та димові сигнали, які використовувалися для передачі важливих повідомлень та сигналів на значні відстані. Завдяки засобам зв'язку, козаки можливо були швидко реагувати на небезпеку та організовувати збройні операції. Крім того, велику роль відігравала усна традиція, яка передавалася від покоління до покоління.

Одним з головних напрямів розвитку комунікацій у козацькому середовищі було встановлення тісного зв'язку між козаками та їхніми лідерами. У зв'язку з цим, було розроблено спеціальні форми комунікації, такі як збори, ділові бесіди та інші форми обговорення важливих питань. Сформували Генеральну старшинську раду, яка вирішувала найважливіші політичні, адміністративні, фінансові, судові та військові питання, проводила дипломатичні переговори.

З появою Гетьманату у 1649 році, з'явилась можливість відносно ефективної комунікації між гетьманом та його підлеглими. Гетьмани використовували послів для комунікації з іншими країнами, а також мали своїх емісарів, які пересувалися по території країни та передавали інформацію. Важливими комунікативними функціями був наділений Генеральний писар, якого іноземці називали канцлером. Він опікувався дипломатією: приймав іноземних послів, брав участь у складанні міжнародних договорів, вів дипломатичне листування.

У цей період засобами комунікації стали газети, листи, повістки, брошури, публічні виступи та збори, які дозволяли залучати громадськість до державних справ та збільшувати свідомість населення про події в країні. Так, перша газета в Україні "Київський телеграф" була видана в 1776 році у Києві. Також у цей період виникла та активно розвивалася книжкова культура. Книги друкуються не тільки на латиниці, але й на кирилиці. У 1632 році Мелетій Смотрицький опублікував "Граматику", що стала першою книгою друкованою кирилицею в Україні.

Колосальною трагедією як для процесу розвитку комунікацій так і для розвитку національної культури стало створення російським імператором Петром І Малоросійської колегії, у повноваження якої входив тотожний контроль дій та зв’язків гетьмана. Таким чином обмежувалась влада гетьмана та про його наміри завжди були донесені московському правителю. У свою ІІ чергу Малоросійська колегія активніше діяла проти гетьманської автономії, маючи за мету цілковите знищення політичної незалежності, закріпачення селян, контроль за економічним станом. Проводилась масова пропаганда серед народу на користь «квітучої» Російської імперії. Крім того, урядом, за допомогою якого російська імператриця здійснювала вплив на стан справ на теренах України, було Правління гетьманського уряду. Клопотами стали численні переслідування та арешти, придушення будь-яких опозиційних російському правлінні поглядів.

Таким чином, слід зазначити, що незважаючи на надскладні політичні умови, соціально-економічне становище, козаки зуміли сформувати структуру комунікацій задля результативності та успішності дій. У процесі комунікації використовували три напрями: усний, писемний, візуальний. Однак на стан комунікативного процесу активно вплинули російські монархи, зацікавлені у деструкції політичного устрою на теренах України та загарбленні території під свій контроль.

Харченко К.А.
курсант Національної академії Служби безпеки України

РОЛЬ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ В УМОВАХ ВІЙНИ

В умовах війни державі особливо необхідно підтримувати зв'язок з населенням, адже суспільна паніка здатна справити сильний негативний вплив на успішність проведення оборонних дій. Враховуючи пряму агресію збоку російської федерації, Радою національної безпеки та оборони України було прийнято рішення «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану», яке підкреслює важливість ролі стратегічних комунікацій у досягнені успіху. В рішенні вказано, що "реалізація єдиної інформаційної політики є пріоритетним питанням національної безпеки" [1]. Ворог вже довгий час проводить інформаційні атаки, спрямовані на українське населення. Їх метою є дестабілізація патріотичних настроїв та поширення страху й паніки.

Варто погодитись із авторами, які зазначають, що "головним інструментом боротьби України проти російської дезінформації під час воєнного стану є правда, яку потрібно доносити не лише до внутрішньої, а й до закордонної аудиторії" [2, с. 29]. Діалог з іншими країнами теж є важливою складовою, адже їх матеріальна підтримка неабияк важлива для України.

Порівнюючи з початком 2000-х років, Україна вже досягла чималого успіху в просвітницькій діяльності. Це видно як з підтримки світової спільноти, так і з більшої обізнаності власне громадян. У зв'язку з тривалим перебуванням України в складі СРСР багато українців почали втрачати свою національну ідентичність. Через це культурно-просвітницька діяльність відіграє важливу роль в забезпеченні державної цілісності та суверенітету. Згідно з опитуванням, проведеним Соціологічною групою «Рейтинг» в перший місяць повномасштабного вторгнення, 88% опитуваних вірили в те, що Україна зможе відбити напад Росії [3]. Віра у власні сили підвищує моральний дух населення, в тому числі і військовослужбовців, що позитивно впливає безпосередньо на воєнний аспект конфлікту.

Підбиваючи підсумки, слід наголосити на потребі подальшого розвитку сфери стратегічних комунікацій задля удосконалення захисту від впливу проросійської пропаганди. Також необхідно посилювати співпрацю з державами-партнерами шляхом видобування довіри та донесення правдивої інформації про дії російських загарбників.

Література

1. Про рішення Ради національної безпеки і оборони України від 18 березня 2022 року "Щодо реалізації єдиної інформаційної політики в умовах воєнного стану": Указ Президента України від 19 березня 2022 року № 152/2022. URL: https://zakon.rada.gov.ua/laws/show/152/2022#Text (дата звернення: 17.03.2023).

2. Сіленко А., Залевська І. Реалізація цілей стратегії інформаційної безпеки України в умовах воєнного стану. Сучасні політичні процеси: глобальний та національний виміри : матеріали II Міжнар. наук-практ. Інтернет-конф. (м. Одеса, 29 квіт. 2022 р.) / МОН України, Нац ун-т «Одес. юрид. акад.». Одеса : 2022. С. 28-34.

3. Загальнонаціональне опитування: Україна в умовах війни (1 березня 2022). Сайт соціологічної групи “Рейтинг”. URL: https://ratinggroup.ua/research/ukraine/obschenacionalnyy_opros_ukraina_v_usloviyah_voyny_1_marta_2022.html?fbclid=IwAR2LvNLxicdO0OIdLoQF3NvHPpAfi7PbbV2GjlHv2IzTSinKBF74u6Gzfz4 —.

Цимбрила А.Ю.,
курсант,
Чубаєвський Н.В.,
курсант,
Лихотоп О.Б.,
курсант
Національна академія Служби безпеки України

ОСОБЛИВОСТІ ДІЯЛЬНОСТІ СПЕЦСЛУЖБ УКРАЇНИ У СФЕРІ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ПРОТИБОРСТВА

Спецслужби — не офіційна узагальнена назва державних органів і органів, покликаних здійснювати оперативно-розшукову діяльність, розвідку та контррозвідку, спеціальні операції та диверсії в інтересах держави [1].

Спецслужби можна умовно поділити на дві групи діяльності: розвідка та внутрішня безпека. Завдання спецслужб – отримання важливої інформації та дезінформації про подібні структури ворожих країн. Органи внутрішньої безпеки

гарантують безпеку громадян і стабільність органів державної влади.

Спеціальна гарантія обслуговування:

– аналіз усіх сфер, що стосуються національної безпеки;

– раннє попередження кризових явищ;

– національне кризове управління;

– забезпечення інформаційного забезпечення оперативного планування Міністерства оборони;

– захищати власну конфіденційну інформацію та інформацію інших державних органів;

- впливати на суспільні процеси в національних інтересах.

В Україні функції спеціальних служб покладаються на такі органи, як Головне управління розвідки Міністерства оборони (воєнна розвідка) та Службу безпеки України (контррозвідка та внутрішня безпека).

Розвідувальні органи Генерального штабу Збройних Сил України здійснюють отримання розвідувальної інформації та сприяють реалізації державної політики України, зміцненню національної обороноздатності, економічному та науково-технічному розвитку України. Спільно з розвідувальними та правоохоронними органами України зазначений підрозділ бере участь у боротьбі з міжнародною організованою злочинністю, зокрема тероризмом, незаконним обігом наркотиків, нелегальною імміграцією, незаконним обігом зброї та її виготовленням.

Служба безпеки України є спеціальним органом державної влади України у сфері контррозвідки. Завданням контррозвідки СБУ є добування, аналіз, обробка та використання інформації, у тому числі ознак і фактів про організації, осіб, групи осіб, а також розвідувально-підривну діяльність іноземних спеціальних служб, терористичну та іншу діяльність, спрямовану на заподіяння шкоди національній безпеці України. СБУ здійснює контррозвідувальний захист життєво важливих національних інтересів, закордонних представництв, технологічного потенціалу, промисловості, енергетики, зв'язку, транспорту, Збройних Сил та інших військових формувань, військово-технічного співробітництва. Підрозділ розвідувально-аналітичного забезпечення СБУ здійснює збір, аналіз та систематизацію інформації, необхідної для нормального функціонування держави та державних інституцій СБУ, розвиває національну розвідувально-аналітичну діяльність СБУ, сприяє керівництву України [2].

Основні цілі спецслужб України у сфері інформаційної безпеки. Основними цілями державної політики у сфері інформаційної безпеки забезпечення інформаційного суверенітету, збереження духовних і культурних цінностей Українського народу, утвердження національної самоповаги та цивілізаційної єдності, створення в Україні розвиненого інформаційного суспільства та національного інформаційного простору, перетворення України на інформаційно розвинену державу та повноправну участь у житті європейського і світового співтовариства, створення національного інформаційного суспільства та

національного інформаційного простору.

Вирішення проблеми інформаційної безпеки має здійснюватися шляхом:

- створення повноцінної національної інформаційної інфраструктури та забезпечення захисту її ключових елементів;
- підвищення рівня координації діяльності державних органів щодо виявлення, оцінки та передбачення загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їх наслідків, розвитку міжнародного співробітництва з цих питань;
- удосконалення законодавчої бази щодо забезпечення інформаційної безпеки, особливо захисту та протидії інформаційним ресурсам;
- правоохоронної діяльності у сфері комп'ютерної злочинності, захисту персональних даних та інформації;
- розгортання та розвитку системи національної таємниці, комунікації, як сучасної захищеної база трафіку, здатної інтегруватися, бути географічно розподіленою інформаційною системою, та базою конфіденційна інформації.

Спецслужби в інформаційно-психологічному протиборстві відіграють важливу роль, оскільки мають доступ до значної кількості інформації та засобів, які дозволяють їм діяти в цій сфері. Інформаційно-психологічне протиборство полягає в тому, що сторони конфлікту намагаються впливати на мислення, поведінку та дії опонента, використовуючи різні методи та техніки [3]. Для досягнення цієї мети спецслужби можуть використовувати різні інструменти, такі як дезінформація, маніпуляція інформацією, психологічний тиск та інші .

Важливим аспектом роботи спецслужб в інформаційно-психологічному протиборстві є збір та аналіз інформації про можливі загрози, що стоять перед державою. Вони повинні бути в змозі прогнозувати можливі наслідки дій опонента та реагувати на них відповідним чином. У сучасних умовах, коли значна кількість інформації надходить через Інтернет, спецслужби мають велику відповідальність щодо охорони безпеки та конфіденційності даних в Інтернеті. Це стає особливо важливим, оскільки інформація, що надходить через Інтернет, може містити особисті дані, які можуть бути використані для крадіжки, шахрайства та інших злочинів [4]. У багатьох країнах існують спеціальні служби безпеки, які займаються контролем за інформаційною безпекою та боротьбою з кіберзлочинністю. Ці служби використовують спеціальні технічні засоби для виявлення та перешкоджання незаконним діям в Інтернеті, таким, як хакерство, фішинг, розповсюдження шкідливих програм тощо.

Загалом, забезпечення безпеки та конфіденційності даних в Інтернеті - це важлива проблема, яка потребує співпраці між користувачами та спецслужбами. Тільки за умови спільної співпраці можна забезпечити безпеку та конфіденційність даних в Інтернеті. Однак, така співпраця повинна ґрунтуватися на довірі та взаємному порозумінні між сторонами.

Користувачі повинні розуміти, що їхні дії в Інтернеті мають наслідки, і що

вони повинні дотримуватися правил та норм, що регулюють використання Інтернету. Крім того, користувачі повинні бути обізнані з методами захисту своїх даних в Інтернеті та використовувати надійні паролі, шифрування даних та інші технології захисту.

Спецслужби, зі свого боку, повинні працювати на користь громадян, забезпечуючи безпеку та захист їхніх даних. Вони повинні бути обізнані з останніми технологіями та методами захисту даних, щоб бути ефективними у боротьбі з кіберзлочинцями та іншими загрозами в Інтернеті [5].

Співпраця між користувачами та спецслужбами повинна бути заснована на взаємній довірі та взаємному розумінні. Це допоможе забезпечити безпеку та конфіденційність даних в Інтернеті та дозволить зменшити кількість кіберзлочинів.

Таким чином, **і**нформаційна безпека в суспільстві та державі характеризується підвищенням стійкості ключових сфер життєдіяльності до впливу небезпечної інформації. Інформаційна безпека визначається здатністю нейтралізувати такі впливи. Загальноприйняте визначення інформаційної безпеки - це стан, при якому захищені життєво важливі інтереси громадян, суспільства і держави в інформаційній сфері.

Інформаційно-психологічне протиборство є дуже ефективним інструментом для досягнення політичних, військових, економічних та інших цілей. Це може бути важливим фактором в боротьбі між державами або навіть внутрішньо в межах однієї країни. Проте, інформаційно-психологічне протиборство також може мати негативні наслідки. Воно може сприяти поширенню фейкової та недостовірної інформації, а також призводити до подальшого розшарування суспільства та збільшення рівня дезінформації. Отже, хоча інформаційно-психологічне протиборство є важливою складовою політичної та військової стратегії, необхідно зберігати баланс між використанням його ефективності та запобіганням негативних наслідків.

Література

1. Доктрина інформаційної безпеки України: Затверджена Указом Президента України від 25 лютого 2017 року № 47/2017. Веб-сайт URL: http://zakon.rada.gov.ua/laws/show/47/2017?lang=ru.

2. Лужецький В.А. Інформаційна безпека. Вінниця: УНІВЕРСУМ-Вінниця, 2009. 240с.

3. Комп’ютерна злочинність і інформаційна безпека. Мінськ: АРІЛ, 2000. 552 с.

4. Вронська Т. В. Інформаційно-психологічні операції в діяльності військової розвідки: теоретико-історичний екскурс. *Вісник воєнної розвідки*. Київ, 2017. № 46. С. 106–111.

5. Карпенко А. Антиукраїнські тенденції в українській державі. веб сайт URL:

http://www. ukrlife.org/main/karp/ without.html (дата звернення: 21.05.2020).

Цілина М.С.
студент НА СБ України

СИСТЕМА ПРОТИДІЇ НЕГАТИВНОМУ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОМУ ВПЛИВУ НА ОСОБОВИЙ СКЛАД ЗБРОЙНИХ СИЛ УКРАЇНИ

Загальні тенденції розвитку інформаційного простору як середовища для проведення інформаційних та психологічних операцій (ІПсО) (впливів) свідчать про зростання рівня загроз в інформаційному просторі.

Аналіз сучасного стану інформаційного протиборства свідчить про те, що війська та населення постійно знаходяться під негативним інформаційним (психологічним) впливом (ІПВ), який здійснюється як в мирний час, так і в загрозливий період та в ході конфлікту [1, с.252].

Потреби військ в ефективних способах протидії негативному інформаційно-психологічному впливу, а також відсутність законодавчої бази щодо здійснення протидії інформаційно-психологічному впливу з боку протидіючих сил під час виконання службово-бойових завдань свідчить про необхідність розроблення проблеми протидії особового складу негативному інформаційно-психологічному впливу в ході виконання службово-бойових завдань.

Результатами негативного інформаційно-психологічного впливу на співробітників сил охорони правопорядку можуть бути порушення психологічної стійкості, професійної спрямованості особистості співробітника у вигляді дезорієнтованості в соціальних і кримінальних явищах, викривленого сприйняття подій і своєї участі в них, деморалізації, ослаблення професійної мотивації, а з іншого боку – загострення індивідуально-психологічних проблем співробітників, таких як дезадаптація, зростання тривожності й страху, поява невмотивованої агресії, туги, апатії, безпечності [2, с.7].

Основним об’єктом впливу з боку противника є психіка особового складу сил сектору безпеки та оборони і цивільного населення держави, а розвиток інформаційних технологій суттєво загострюють і підсилюють проблему психологічної небезпеки. Результати аналізу ведення бойових дій на початку Антитерористичної операції (АТО) на сході України свідчать, що головним фактором, який негативно впливав на особовий склад, була масова загибель та поранення військовослужбовців військової частини, що спричиняло зневіру у власних силах, рівні підготовки командирів, з’являвся фактор невизначеної небезпеки та страху за власне життя, перевищення оцінки рівня бойового вишколу незаконних збройних формувань. Особовий склад виказував незадоволення рівнем

особистої підготовки, рівнем матеріально-технічного забезпечення, рівнем підготовки сержантського та офіцерського складу, наголошував на відсутності довіри до керівного складу військової частини та вищого керівництва. Найбільш негативно на морально-психологічний стан особового складу впливала відсутність ефективного керівництва у низовій ланці (відділення, взвод) управління.

Основними причинами недостатньої ефективності протидії негативному ІПВ на особовий склад на початку АТО можна вважати неготовність на той час керівного складу військових частин і підрозділів організовувати бойову діяльність в умовах негативного ІПВ та слабку систему захисту особового складу та населення від негативного ІПВ противника та відсутність дієвої ієрархічно побудованої структури планування та виконання заходів інформаційно-психологічної протидії.

Тому, протидія негативному ІПВ є одним із основних завдань щодо забезпечення високого морально-психологічного стану особового складу збройних сил.

Необхідність набуття спроможностей з протидії негативному ІПВ потребує удосконалення процедур планування та підготовки заходів з протидії негативному ІПВ, тому пропонується методичний підхід до визначення підрозділу (підрозділів) для здійснення протидії негативному інформаційному (психологічному) впливу противника на основі оцінювання його (їх) спроможностей за методикою DOTMLPFI [3, с.16-17].

Методика DOTMLPFI використовується в країнах-членах НАТО для оцінювання спроможностей підрозділів і прийнята в Україні для оборонного планування в Міністерстві оборони України та Збройних Силах України [4, с.29].

Наведені спроможності оцінюються за базовими, основними та додатковими вимогами відповідно до методики DOTMLPFI (Doctrine, Organization, Training, Material, Leadership, Personnel, Facilities, Interoperability), що визначає базові компоненти (складові) спроможності.

Методика DOTMLPFI передбачає оцінювання за наступними критеріями (показниками):

– D – керівні документи (чинні доктринальні документи);

– O – організація (організаційна структура і склад наявних підрозділів);

– T – підготовка (рівень підготовки особового складу до виконання завдань за призначенням);

– M – ресурсне забезпечення (забезпеченість необхідним зразками матеріально-технічних засобів для виконання завдань);

– L – якість управління та освіта (наявність належного рівня професійної підготовки особового складу, що забезпечує функціонування і розвиток);

– P – персонал (наявність кваліфікованого та вмотивованого особового складу);

– F – інфраструктура (наявність відповідної інфраструктури та здатність

забезпечити виконання завдань за призначенням);

– I – взаємосумісність (рівні доктринальної, оперативної та технічної сумісності з відповідними підрозділами сил НАТО та країн-партнерів).

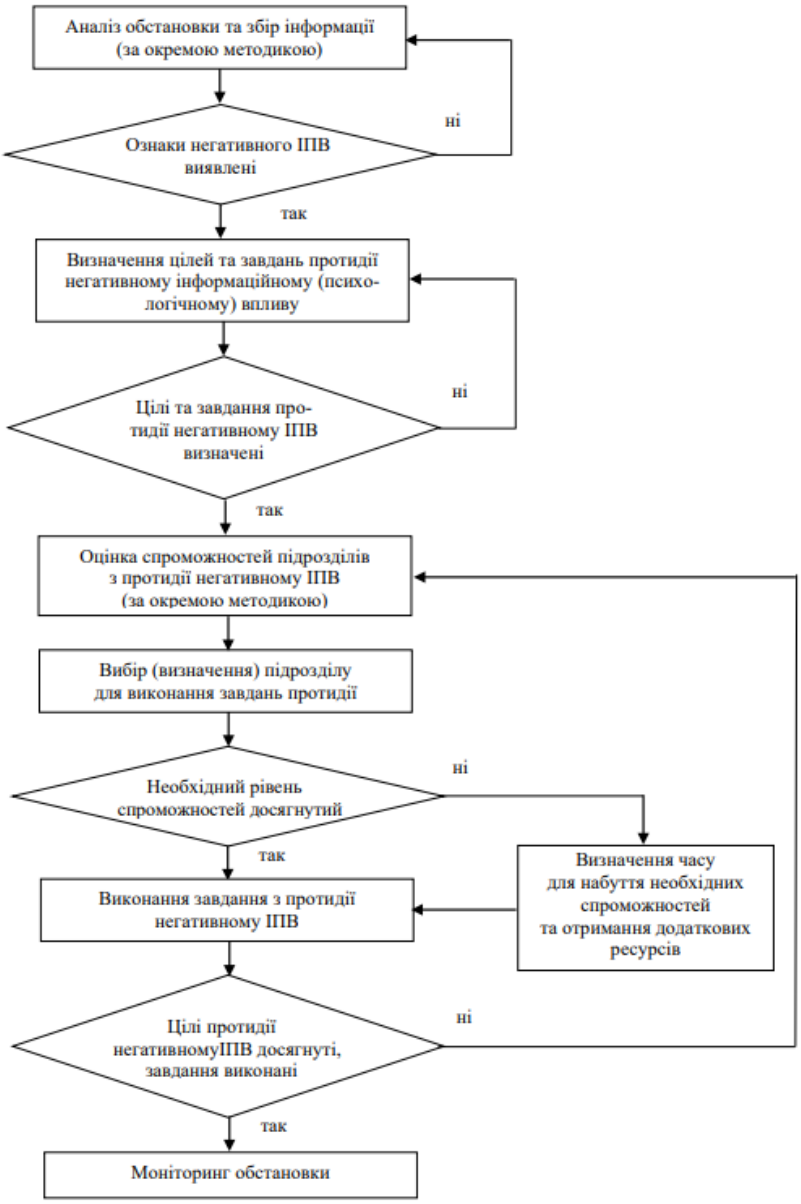


Рис. 1. Схема процедур планування протидії негативним ІПВ на основі оцінювання спроможностей підрозділів

Схема процедур планування протидії негативним ІПВ на основі оцінювання спроможностей підрозділів представлена на рис. 1 [3, с.18-19].

Отже, системний підхід до протидії негативним ІПВ дає можливість державі та її Збройним Силам ефективно протистояти інформаційним загрозам та реалізовувати свої стратегічні інтереси в сучасному інформаційному просторі.

Література

1. Інформаційно-психологічні операції: планування, протидія, технології : монографія / Пєвцов Г. В. , Залкін С. В., Сідченко С. О., Хударковський К. І.

Харків : ДІСА ПЛЮС, 2020. 252 с.
2. Інформаційно-психологічна протидія в Національній гвардії України (психологічний аспект) : монографія / Воробйова І. В. та ін. Харків : Національна акад. НГУ, 2016. 7 с.
3. Г.В. Пєвцов , С.В. Залкін, П. Пацек, О.В. Ревін, С.О. Сідченко, К.І. Методичний підхід до визначення підрозділів для здійснення протидії негативному інформаційному (психологічному) впливу противника на основі оцінювання їх спроможностей. Наука і техніка Повітряних Сил Збройних Сил України, 2021, № 4(45) С. 16-23. URL: https://doi.org/10.30748/nitps.2021.45.02 (дата звернення: 18.03.2023).
4. Рекомендації з оборонного планування на основі спроможностей в Міністерстві оборони України та Збройних Силах України : затверджено Міністром оборони України 12.06.2017 р. Вид. офіц. Київ, 2017. 29 с.

Чорнуха Р.Л.,
курсант
Федан Н.О.,
курсант
Національна академія Служби безпеки України

КОМУНІКАТИВНІ ПІДХОДИ ДО ФОРМУВАННЯ ІМІДЖУ СПЕЦСЛУЖБ

Актуальність теми полягає втому, що спеціальні служби, такі як розвідка, правоохоронні органи та служби безпеки, мають вирішальне значення для безпеки держави та її громадян. Ці організації відіграють важливу роль у забезпеченні національної безпеки, боротьбі з тероризмом, запобіганні організованій злочинності та захисті національних інтересів. Розвідувальні органи відповідають за збір та аналіз внутрішньої та зовнішньої розвідувальної інформації про загрози національній безпеці. Розвідувальні органи надають політикам інформацію, необхідну для прийняття обґрунтованих рішень з питань національної безпеки. Правоохоронні органи відповідають за дотримання закону, підтримання громадського порядку та захист громадян від злочинів. Вони працюють над запобіганням, розслідуванням і притягненням до відповідальності за злочинні дії, а також забезпечують правосуддя і громадську безпеку. Силові структури, такі як збройні сили та Національна гвардія, відповідають за захист країни від зовнішніх загроз, охорону кордонів та забезпечення суверенітету країни. Загалом, наявність спеціальних сил у країні є необхідною для підтримання правопорядку, захисту національної безпеки та сприяння добробуту і безпеці її громадян. Без цих організацій країна була б вразливою до різних внутрішніх і зовнішніх загроз, що ставило б під загрозу життя і добробут її громадян.

Комунікативні підходи до формування іміджу спецслужб Спецслужби, такі як розвідувальні та правоохоронні органи, відіграють важливу роль у підтримці національної безпеки та захисті від зовнішніх і внутрішніх загроз. Однак ці служби часто оповиті таємницею, що призводить до підозр і недовіри з боку громадськості. Щоб вирішити цю проблему, спецслужбам необхідно використовувати комунікаційний підхід для створення позитивного і прозорого іміджу в очах громадськості.

Першим кроком у створенні позитивного іміджу є визнання занепокоєння і скептицизму громадськості. Розвідувальні служби повинні усвідомлювати, що їхня діяльність може сприйматися як нав'язлива і надмірна, і тому вони повинні прагнути бути максимально прозорими. Це може передбачати регулярну публікацію звітів і статистичних даних про діяльність спецслужб, проведення громадських слухань і співпрацю з організаціями громадянського суспільства для забезпечення відповідності їхньої діяльності правовим і етичним стандартам. Іншим важливим аспектом комунікаційного підходу є використання соціальних мереж та інших цифрових платформ для взаємодії з громадськістю. Розвідувальні служби можуть використовувати ці платформи для інформування громадськості про свою діяльність, відповідати на питання і занепокоєння, а також надавати інформацію про свої методи і стратегії. Це може допомогти прояснити реальність їхньої розвідувальної діяльності і сприяти зміцненню почуття довіри і прозорості серед громадськості.

Крім того, спецслужби можуть використовувати інформаційно-просвітницькі програми для взаємодії з громадськістю і побудови відносин, заснованих на взаємній довірі і повазі. Нарешті, спецслужби також повинні прагнути до створення позитивного іміджу своїми діями і словами. Це передбачає застосування найкращих практик збору та аналізу розвідувальної інформації, повагу до прав людини і громадянських свобод, а також професійну і чесну поведінку. Будь-які неправомірні дії або зловживання владою можуть мати негативний вплив на імідж спецслужб і повинні розглядатися оперативно і прозоро.

Формування корпоративної культури розвідувальних спецслужб. Розвідувальні служби відіграють важливу роль у забезпеченні національної безпеки та захисті від загроз для Батьківщини. Однак їхній успіх залежить не лише від можливостей збору розвідувальної інформації, а й від розвитку сильної корпоративної культури. Корпоративна культура, яка наголошує на доброчесності, командній роботі, професіоналізмі та лояльності, має важливе значення для ефективної та результативної роботи розвідувального співтовариства.

Побудова сильної корпоративної культури починається з верхівки, з керівництва розвідувального співтовариства. Лідери повинні задавати тон в організації, створюючи культуру довіри, поваги і досконалості. Лідери повинні

забезпечити, щоб цінності, місія і бачення розвідувальної організації були добре донесені і зрозумілі всім співробітникам. Керівники також повинні подавати приклад і демонструвати бажану поведінку і ставлення, яких вони очікують від своїх співробітників.

Розвідувальному співтовариству необхідно приділяти першочергову увагу набору і утриманню висококваліфікованого персоналу, який поділяє цінності і місію розвідувального співтовариства. Важливо мати суворий і прозорий процес відбору, який зосереджується на навичках, кваліфікації і характері кандидатів. Співробітники повинні проходити підготовку і навчання, щоб забезпечити наявність у них навичок і знань, необхідних для ефективного виконання своїх обов'язків. Необхідно також впроваджувати програми постійного навчання та розвитку, щоб працівники були в курсі новітніх технологій, навичок та передового досвіду. Командна робота є ще одним ключовим елементом сильної корпоративної культури в розвідувальних службах. Співробітники повинні чітко розуміти свої ролі та обов'язки і нести відповідальність за свої дії. Комунікація має важливе значення, і необхідно заохочувати обмін інформацією для того, щоб усі співробітники були обізнані з пріоритетами і завданнями розвідки.

Доброчесність і професіоналізм також є ключовими компонентами сильної культури.. Співробітники повинні демонструвати найвищий професіоналізм у своїй поведінці, словах і діях, як під час виконання своїх обов'язків, так і поза ними. Конфіденційність і розсудливість мають вирішальне значення, і співробітники повинні бути навчені захищати конфіденційну інформацію в будь-який час. Нарешті, лояльність є важливим елементом сильної культури в розвідувальній організації. Співробітники повинні бути віддані своєму відомству, своїм колегам і своїй країні.

Таким чином, розбудова сильної культури в розвідувальній спецслужбі вимагає узгоджених зусиль як з боку керівництва, так і з боку персоналу. Підкреслюючи свою місію і цінності, інвестуючи в навчання і розбудову потенціалу, розвиваючи сильне лідерство, сприяючи чіткій комунікації, дотримуючись етичних стандартів і поважаючи різноманітність та інклюзивність, ці організації можуть створити культуру, яка підтримуватиме їхню місію і сприятиме зміцненню довіри до людей, яким вони служать.

Висновок. Підсумовуючи сказане , створення позитивного іміджу розвідувальних служб має важливе значення для збереження довіри і підтримки з боку громадськості. Це вимагає комплексного підходу, який включає в себе прозорість, залучення, інформаційно-пропагандистську діяльність і професіоналізм. Застосовуючи ці комунікаційні підходи, розвідувальні служби можуть побудувати міцні, позитивні відносини з громадськістю, що є запорукою успіху розвідувальних служб у забезпеченні національної безпеки, а побудова сильної корпоративної культури має важливе значення для забезпечення успіху розвідувальних служб у захисті національної безпеки. Нижче наведені деякі з

ключових елементів сильної корпоративної культури. Культура, яка цінує чесність, командну роботу, професіоналізм і лояльність, необхідна для того, щоб співробітники працювали ефективно і результативно. Лідери повинні задавати напрямок, а співробітники повинні бути набрані, навчені та розвинені так, щоб поділяти цінності та місію агентства. Важливість сильної культури в розвідувальному співтоваристві неможливо переоцінити, і вона повинна бути головним пріоритетом для всіх відомств.

Література

1. Ф.Шреер. Комунікативні підходи до формування іміджу спецслужб. веб-сайт. URL: https://pidru4niki.com/82972/politologiya/komunikativna_imidzheva_kompetentnist_fahivtsiv_sektoru_bezpeki_oboroni_sutnist_stan_napryami_formuvannya (дата звернення: 16.03.2023).

2. Ф.Шреер. Трансформування розвідувальних служб: як зробити їх більш сильними та динамічними. веб-сайт. URL: https://pidru4niki.com/82981/politologiya/korporativniy_imidzh_institutiv_sektoru_bezpeki_oboroni_tehnologiyi_formuvannya (дата звернення: 16.03.2023).

3. Лісовський П. М., Подоляка С. А., ЛісовськаЮ. П. Спецслужби держав світу: ентропія, балістика, логістика. Київ.: Видавничий дім «Кондор», 2019., 212 с

4. Сідак В.С. Національні спецслужби в період Української революції 1917-1921 рр (невідомі сторінки історії). Київ «Альтернативи», 1998. С. 150-154.

5. Цибулькін В. В., Рожен Л. М., Вєдєнєєв Д. В. Нариси з історії розвідки суб'єктів державотворення на теренах України. Київ: «Преса України», 2011. С. 283.

Чигвінцев В.Д.
студент ННІ ІБСК НА СБ України
Козюра В.Д.
кандидат технічних наук, доцент
Національна академія Служби безпеки України

ВПРОВАДЖЕННЯ АПАРАТНИХ ЗАКЛАДОК У МІКРОСХЕМИ

Апаратні закладні пристрої (закладки), які розуміються як спеціальні пристрої в електронних схемах, таємно вводяться в елементи комп'ютерної техніки (зокрема, в процесорні мікросхеми, мікросхеми пам'яті, комунікаційні мікросхеми тощо) здатні втручатися в обчислювальні процеси, перехоплювати дані, що оброблюються (в тому числі параметри ідентифікації та автентифікації). Результатом їх функціонування може бути повне зруйнування комп'ютерної

системи, порушення її нормального функціонування, несанкціонований доступ до інформації, зміна вмісту оброблюваних даних або блокування доступу до них, тобто порушення всіх властивостей, що захищаються, - конфіденційності, цілісності, доступності, а також спостережності та керованості.

Відносна простота впровадження апаратних закладок в сучасні цифрові мікросхеми викликає занепокоєння у фахівців із кібербезпеки. Подібні зловмисні модифікації можуть бути внесені в апаратуру як на етапі розробки, так і в процесі виробництва, включаючи такі стадії, як специфікація, проектування, верифікація та виготовлення. Більше того, апаратна закладка може бути впроваджена у вже виготовлену інтегральну схему (ІС).

Сучасні тенденції в напівпровідникової промисловості характеризуються поділом основних етапів процесу розробки та виготовлення ІС на підетапи, які виконуються декількома фабриками, розкиданими по всьому світу, переважно в Азії. Залучення сторонніх співвиконавців притаманно як при виготовленні ІС, але й при проектуванні: розробники користуються стороннім програмним забезпеченням, широко використовують вже готові стандартні блоки (IP-блоки), спроектованими третьою стороною. IP-блоки часто поставляються у цифровому вигляді та проектуються сторонніми фірмами, що спеціалізуються на певних технічних проектах. Тому апаратна закладка може виглядати як начебто незначне зміною параграфа в специфікації на мікросхему або, додатковим рядком у вихідному коді, написаному мовою високого рівня опису апаратури, або модифікацією конструкції кремнієвого кристала (наприклад, невелика зміна топології одного з сотень мільйонів транзисторів).

Проблема апаратних закладок всебічно досліджується у світі. Агентство з перспективних оборонних науково-дослідних розробок США (DARPA) ініціювало у 2007 році спеціальну програму із забезпечення автентичності мікросхем, що використовуються у військових системах США, та фінансує цілий ряд НДДКР з розвитку методів та нових технологій виявлення апаратних закладок.

Вплив апаратних закладок може змінюватись від простих цільових атак до складних комбінованих атак, які забезпечують «точку опори» наступним програмним атакам ще вищого рівня.

До цільових відносяться наступні атаки:

- зміна біта інформації, що порушує цілісність даних, що зберігаються;
- ослаблення функціональності криптографічних ядер;
- атаки, які призводять до витоку конфіденційної інформації.

Система може бути інфікована навіть не однією, а декількома апаратними закладками, які спільними діями підривають її безпеку.

Для розуміння впливу апаратних закладок на системи та розробки методів виявлення необхідно вивчити механізми внесення зміни інформації при впровадженні закладок, а також можливі механізми їх активації.

Розробка та виготовлення ІС включає такі етапи, як специфікація ІС, її розробка, виготовлення, тестування та складання. Вони повинні розглядатися як стадії, на яких порушник може впровадити апаратну закладку.

Повний цикл проектування та виробництва ІС має бути всебічно досліджений з розглядом як стратегій ефективної профілактики впровадження закладок, так і технологій їх виявлення.

Закладки можуть впроваджуватись у будь-які елементи комп'ютерної системи. Локалізація закладки може обмежуватися окремим компонентом систем, а може бути розосереджена на декількох компонентах, таких як процесор, пам'ять, схеми входу-виходу, джерела живлення або синхронізації. Особливість локалізації визначається складністю конкретного проекту ІС, складністю застосування і тим ефектом, який повинна викликати апаратна закладка. А для цього потрібно знати всі можливі механізми роботи апаратних закладок.

Апаратні закладки можуть бути впроваджені не тільки в ІС спеціалізованого призначення (ASIC) (хоча в більшості випадків вони для цього призначені), але і в комерційні електронні компоненти, що знаходяться у вільному продажу (COTS – Commercial Of The Shelf), це мікропроцесори, цифрові сигнальні процесори або у вигляді програмних змін у «прошивці» ПЛІС (FPGA).

Апаратні закладки, що змінюють функціональність ІС через впровадження додаткової логічної схеми або за допомогою вимкнення частини існуючої логіки, безпосередньо ставлять під загрозу цілісність та збереження комп'ютерної системи. Зміна даних у пам'яті, вплив на обчислювальні операції чи комунікаційний канал є характерними цілями аналізованого застосування. Модифікації функціональності можуть мати різноманітний характер; впливи цього класу апаратних закладок обмежені лише ресурсами системи, уявою та кваліфікацією порушника. Наприклад, у запропонований сценарій, в якому відносно проста деструктивна апаратна закладка може вставити помилку в алгоритм на основі відомої китайської теореми про залишки при обчисленні криптографічного алгоритму з відкритим ключем (RSA), що в результаті призводить до компрометації RSA-ключа.

Спеціальні апаратні закладки можуть розроблятися для забезпечення можливості зміни порядку виконання команд центрального процесора, для організації витоку даних через побічні канали, для зміни вмісту постійної пам'яті, що програмується, що найбільш небезпечно для мікросхем спеціального призначення.

Зміна функціональності системи може бути використана для підтримки ширших атак. Очевидно, що можливості заподіяння шкоди безпеці суттєво збільшуються при спільному використанні апаратної та програмної атаки. Як приклад, в наведені внесені несанкціоновані зміни в центральному процесорі, що підтримують атаку на програмне забезпечення, в результаті якої надання доступу до пам'яті та модифікація програми сприяють розширенню несанкціонованих

повноважень з можливістю подальшого доступу в систему через «чорний вхід» та атакою з крадіжкою пароля.

Наступний клас апаратних закладок охоплює різні апаратні модифікації, створені для організації потайної передачі конфіденційних даних від комп'ютерної системи порушнику. Така передача здійснюється без безпосередньої участі системи та без відома користувача системи. Механізми передачі можуть задіяти як існуючі внутрішні та зовнішні канали системи, і побічні (спеціальні) канали. Наприклад, витік інформації може відбуватися по радіочастотному, оптичному або тепловому побічним каналам.

Інформацію також можна отримати, аналізуючи величину споживаної потужності ІС, її специфічні шумові характеристики, а також будь-які інші функціональні та фізичні характеристики. Стандартні інтерфейси RS-232 і JTAG також можуть бути використані як несанкціоновані канали витоку інформації. Наприклад, апаратна закладка дозволяє легко визначати будь-які ключі шифрування в каналі бездротової передачі лише по зміні амплітуди сигналів або частоти, що виникають через варіації технології виготовлення ІС.

Системна модифікація фізично надає широкий спектр можливостей для реалізації помилки типу «відмова в обслуговуванні» (DoS), які варіюються від часткової прояви помилки до повного та остаточного відключення системи впровадженням так званого «вбиваючого ключа» (kill switch). Апаратна закладка може бути розроблена з метою впливу на керування сигналом роздільної здатності запису в пам'ять, перезаписуючи існуюче значення випадковою величиною. Це веде до некласифікованих операторами збоїв у роботі служб або часткового (і навіть повного) відключення електронної системи управління.

Апаратні закладки загрожують порушенням цілісності даних та функцій, що виконуються будь-якою обчислювальною та керуючою електронною системою, що містить інтегральні електронні компоненти. Суть цих реальних загроз полягає в несанкціонованих функціональних та технічних модифікаціях характеристик ІС, витоку конфіденційної інформації, а також організації успішних атак типу «відмова в обслуговуванні». Для запобігання можливості таких загроз необхідна розробка комплексних технічних методів та ефективних стратегій боротьби з подібними апаратними закладками, їх попередження та своєчасного виявлення, а також ефективних заходів протидії їм.

Шайхет С.О.
к.н.держ.упр.
Національний університет оборони України імені Івана Черняховського

АНАЛІЗ УМОВ І ЧИННИКІВ, ЯКІ ВПЛИВАЮТЬ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ ЗАХОДІВ МІЖНАРОДНОГО ВІЙСЬКОВО-ТЕХНІЧНОГО СПІВРОБІТНИЦТВА

Принципи інформаційного впливу на інформаційну безпеку Міністерства оборони України постійно з успіхом використовує рф. Це створює умови за яких інформаційний вплив буде основним засобом впливу, а бойові дії відіграють підлеглу сервісну роль. Що змінює зміст планів і відповідно зі сценарієм піар-впливу на власних громадян, на громадян політичних союзників і опонентів і на міжнародне співтовариство в цілому [1].

Питання здійснення ефективного інформаційного впливу на заходи військово-технічного співробітництва, як інформаційний обмін, проведення переговорів, укладення міжнародних договорів та зовнішньоекономічних договорів постало в період широкомасштабної збройної агресії рф.

Виходячи із зазначеного, метою тез доповіді є аналіз умов і чинників, які впливають на інформаційну безпеку заходів міжнародного військово-технічного співробітництва.

Для вирішення зазначеної проблеми за конкретних історичних внутрішніх обставин і зовнішніх чинників формуються політичні цілі та завдання.

1. Система військово-технічного співробітництва виступала, насамперед, як інструмент зовнішньої політики держави, що призначений забезпечувати присутність держави (політичну, економічну, технологічну, військову) в тому або конкретному регіоні формувати партнерські відносин. Це призвело до того, що військово-технічне співробітництво розглядалось, як лише комерційне явище. Оскільки фактор негайної комерційної вигоди того чи іншого контракту в ті часи був основним, порівняно з довгостоковим його ефектом. Безумовно, якщо брати до уваги кризовий стан радянського оборонно-промислового комплексу, що вимагало необхідність мати додаткові фінанси на його утримання.

2. Однак система військово-технічного співробітництва була розрахована на стабільне існування упродовж тривалого часу (принаймі на строк “життєвого циклу” зразків озброєння, які постачаються) і не могла слугувати лише конкретній політичній кон’юнктурі.

3. При здійсненні військово-технічного співробітництва пріоритет був відданий, з одного боку інтересам держави, а не комерційним структурам, а з іншого боку – геополітичним наслідкам розвитку військово-технічного співробітництва з тією чи іншою країною. З політичної точки зору інтереси однієї

з частин суспільства не можуть і не повинні стояти вище інтересів суспільства у цілому.

4. Питання військово-технічного співробітництва із зарубіжними країнами були водночас і питанням підтримки власного виробництва та стимулювання науково-технічного прогресу. Постачання озброєння та військової техніки виконувались, насамперед, в інтересах підтримки державних інтересів.

На даний час всі заходи інформаційної підтримки в інтересах військово-технічного співробітництва згруповані за напрямами:

моніторинг інформаційного простору в інтересах військово-технічного співробітництва;

спростування неправдивої інформації;

інформаційна підтримка цивільного населення;

інформаційна підтримка особового складу, який виконує спеціальні завдання;

інформаційно-психологічний вплив на закордонні засоби масової інформації з метою маніпулювання свідомістю лідерів держав внесення розколу в їхні дії, спонукання їх до вироблення хибних рішень та створення умов для проведення спеціальних дій – занепокоєння та паніки, переконання, тощо;

інформування міжнародної спільноти з метою здійснення інформаційного впливу на цивільне населення.

Під час моніторинг інформаційного простору в інтересах військово-технічного співробітництва виявляється інформація про новітні зразки озброєння і військової техніки [2].

При виявленні неправдивої інформації негативного змісту, яка впливає, в даному разі на успішність проведення інформаційної операції, готується її спростування. До спростування залучаються представники мас-медіа, експерти, безпосередні учасники тих чи інших подій.

Якщо вдається спрогнозувати наступні кроки інформаційної кампанії противника, застосовується спосіб надання власної інформації на випередження.

Для інформаційної підтримки заходів військово-технічного співробітництва для конкретної території, перш за все, організовується робота з визначення тематик інформування (створення певних меседжів), розробляються комунікаційні можливості та створюються поточні новини в сегментах інформаційного простору. Крім того, для соціальних мереж розробляються імітатори думок (бот мережі), які створюють певне враження для цільових аудиторій.

Заходи інформаційної підтримки військово-технічного співробітництва полягають в об’єктивному інформуванні ЗМІ про дії та наміри керівництва держави, зміни міжнародної обстановки тощо.

Інформаційно-психологічний вплив на лідерів думок або військово-політичне керівництво країни, як правило в цей період не проводиться. А за необхідності може здійснюватися шляхом відповідної роботи в близьких до них

групах соціальних мереж Фейсбук, Твіттер, Одноклассники, ВКонтакте; підготовки та розповсюдження необхідної дезінформації.

Інформування міжнародної спільноти здійснюється шляхом збору, узагальнення та демонстрації фактів, які приховують справжні наміри військово-технічного співробітництва.

Проведення аналізу "гібридної війни", яку здійснює рф у межах довготривалої інформаційної кампанії проти України, дає змогу виокремити основні напрями та методи здійснення заходів, що зачіпають основні сфери національної безпеки України та становлять загрозу національним інтересам у:

зовнішньополітичній сфері – перешкоджання євроінтеграції України у спосіб формування упередженого ставлення світової спільноти до української влади, поширення недостовірної, неповної та викривленої інформації про Україну, висловлювання недоцільності євроінтеграції України;

внутрішньополітичній сфері – формування образу ворога – українця серед російськомовних громадян України та росіян, а також спроби формування упередженого ставлення світової спільноти до патріотичних рухів в Україні у спосіб поширення викривленої, недостовірної та упередженої інформації щодо становища в Україні росіян та інших етнічних груп, статусу російської мови;

сфері державної безпеки – посягання на державний суверенітет і територіальну цілісність України у спосіб порушення питань про приналежність АР Крим (відбувалося впродовж усіх років незалежності), наразі – про доцільність федералізації України та формування "Новоросії" на Сході України;

воєнній сфері – витіснення України зі світового ринку зброї у спосіб поширення недостовірної інформації щодо участі України у незаконному розповсюдженні зброї, оборонних технологій та низької якості української військової техніки тощо; на сьогодні – формування негативної громадської думки серед української та світової спільноти про дії Збройних сил України на Сході України у спосіб поширення недостовірної інформації про застосування військовими зброї проти мирного населення;

економічній сфері – витіснення України зі світового та російського ринків у спосіб розповсюдження недостовірної інформації про якість окремих груп товарів чи низький рівень наукових розробок у певних галузях; перешкоджання реалізації та дискредитація здійснених заходів Україною щодо зниження енергетичної залежності від рф, зокрема завдяки маніпулюванню інформацією щодо цін на енергоносії;

соціальній та гуманітарній сферах – протидія переосмисленню власної історичної спадщини, нівелювання українських культурних цінностей і формування проросійських настроїв у суспільстві у спосіб насаджування міфу про спільний "русский мир", заперечення існування окремої від росіян української нації з власною мовою, культурою та історією, ставлення під сумнів права української нації на самовизначення й утворення національної держави.

Таким чином, на інформаційну безпеку заходів міжнародного військово-технічного співробітництва найбільше впливають чинники, які спричинені методами використання пропаганди, агітації, тенденційної інформації, напівправди та відвертої неправди (“фейку”).

Література

1. Global Information Technology Report 2015. World Economic Forum. http://reports.weforum.org/globalinformation-technology-report-2015.

2. Горбулін В. П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: Монографія / В. П. Горбулін, О. Г. Додонов, Д. В. Ланде. – Київ: Інтертехнологія, 2009. – 164 с.

Штефан В.Й.
Національна академія СБ України

МОРАЛЬНО – ПСИХОЛОГІЧНЕ ЗАБЕЗПЕЧЕННЯ В КОНТЕКСТІ ЗБРОЙНОЇ АГРЕСІЇ рф ПРОТИ УКРАЇНИ

Збройна агресія російської федерації проти України, що почалася в 2014 році, стала великим випробуванням не лише для української армії, але й для морально-психологічного стану громадян України. Нового масштабу агресія росії проти України набула 24.02.2022 року, коли почався повномасштабний наступ з метою окупації всієї території нашої держави. Цей наступ став складною і болісною проблемою для громадян України.

Тому сьогодні аналізуючи різні джерела та засоби масової інформації, можна зазначити, що актуальними питаннями морально-психологічного забезпечення в умовах збройної агресії рф проти України є:

1. **Підвищення рівня стресу та тривоги.** Війна створює психологічний тиск на громадян України, особливо коли рф вночі наносять ракетних ударів по нашій території вночі. Вмикається повітряна тривога, яка перериває сон з метою дестабілізації психологічного стану населення, від цього в громадян загострюється та підвищується тривожність, страх та роздратованість. А також, перебування в зоні бойових дій може призвести до серйозного психологічного стресу, особливо у військовослужбовців та осіб, які мають непрямий стик зі збройним конфліктом, таких як медичні працівники, журналісти, рятувальники і т.д. [1].
2. **Психологічна підтримка бійців.** Військовослужбовці, які перебувають в зоні бойових дій, потребують особливо моральної та психологічної підтримки. Для вирішення цієї проблеми може бути надана короткочасна відпустка для зустрічі з рідними, що покращить їх морально-психологічний стан.

3. **Психологічна адаптація бійців після повернення до мирного життя.** Повернення військовослужбовці з передової до мирного життя може бути складним через відчуття некомфортності на території України де не ведуться бойові дії. Для того щоб військовослужбовці краще адаптувались до мирного життя, треба створювати для них центри морально-психологічної підтримки [2].

4. **Психологічна підтримка мирного населення.** Велика кількість громадян України, які живуть в місцях де проходять бойові дії, а також в місцях де рф здійснює регулярні ракетні атаки, знаходяться в постійній тривозі та стресі. Тому, держава та волонтери, намагаються надавати психологічну підтримку, а також здійснюють лікування людей, які постраждали від психічного травмування в результаті збройної агресії.

5. **Використання ефективної системи інформаційної роботи та підвищення рівня інформаційної культури населення.** Для вирішення цієї проблеми необхідно організувати масштабні кампанії з популяризації інформації про те, що відбувається в країні, про причини та наслідки конфлікту, про історичний контекст подій, а також про міжнародні зусилля з врегулювання конфлікту.

6. **Протидія дезінформації та пропаганді.** З початку повномасштабної агресії російська «пропагандистська машина» намагається вплинути на українське суспільство та змусити його відмовитися від своїх цінностей. Тому влада України, всіляко протидіє дезінформації та пропаганді забезпечуючи правдиву інформацію та розповсюджуючи її [3].

7. **Підтримка ветеранів та їх родин.** На сьогодні дуже гостро стоїть питання підтримки ветеранів та їх родин, тому держава намагається, забезпечити їх всім необхідним.

Для подолання цих проблем розглянемо основні шляхи, що можуть включати такі заходи:

- **Підтримка соціального захисту та забезпечення безпеки населення.** Важливо забезпечити безпеку та захист для українського населення в умовах війни, а також забезпечити надійне функціонування системи правоохоронних органів та армії. Укладення міжнародних договорів з іншими державами може забезпечити міжнародну підтримку, а також можна розробити програми соціальної підтримки інвалідів, пенсіонерів та інших груп населення, які зазнали військової агресії.

- **Проведення соціально-психологічної роботи з учасниками бойових дій та розвиток соціально-психологічних служб підтримки для військовослужбовців, добровольців, їх родин та всіх, хто постраждав від бойових дій.** Робота з психологами та соціальними працівниками може допомогти учасникам бойових дій зрозуміти свої почуття та емоції, а також знайти способи їх подолання. Постраждалі від бойових дій перебувають в особливих умовах під час конфлікту, відчувають великий психологічний тиск, відчуженість від соціуму,

стресові ситуації. Необхідно забезпечити психологічну підтримку, яка б допомагала їм відновитись після страхітних переживань, знайти підтримку та розуміння [4].

- **Організація соціальної реабілітації інвалідів та постраждалих внаслідок війни.** Важливо забезпечити ефективну реабілітацію для тих, хто постраждав від збройного конфлікту, включаючи військовослужбовців, цивільних осіб, біженців та внутрішньо переміщених осіб. Це може включати фізичну терапію, реабілітаційні послуги, роботу з психологами, а також підтримку з боку спільноти. Відновлення здоров'я та соціальної адаптації цих людей може сприяти підвищенню їхнього морально-психологічного стану.
- **Використання ефективної системи інформаційної роботи та підвищення рівня інформаційної культури населення.** Для цього необхідно організувати масштабні кампанії з популяризації інформації про те, що відбувається в країні, про причини та наслідки конфлікту, про історичний контекст подій, про міжнародні зусилля з врегулювання конфлікту тощо.
- **Створення умов для відновлення морально-етичних цінностей в суспільстві.** Необхідно активно протидіяти дестабілізуючим чинникам, які знижують рівень довіри та сприяють занепаду моральних цінностей, таким як корупція, беззаконня, відсутність відповідальності перед суспільством [5].

На завершення варто зазначити, що не всі проблемні питання морально-психологічного забезпечення в умовах збройної агресії рф проти України були розглянуті, тому що ця проблема є надзвичайно складною і вимагає комплексного підходу. Вона впливає на багато аспектів життя громадян України, включаючи їхнє психічне та фізичне здоров'я, соціальну адаптацію та загальну якість життя.

Література

1. Ягупов В.В. Морально-психологічне забезпечення. — К., 2002. http://medbib.in.ua/moralno-psihologichne-zabezpechennya.html
2. Скочиляс С. Особливості психологічного забезпечення адаптаційного періоду військовослужбовців строкової служби. Львів : Центр політичних досліджень, 2001. http://westukr.itgo.com/ad_period.html
3. Офіційний сайт Міністерства оборони України: https://www.mil.gov.ua/
4. Білошицький В.І., Гангал А.В., Стукан С.О., Бех С.М. Морально-психологічне забезпечення у Збройних Силах України https://ela.kpi.ua/bitstream/123456789/47264/1/MPZ_ZSU_2020.doc
5. Морально-психологічне забезпечення у Збройних Силах України підручник : у 2 ч. Ч. 1. вид. 2-е, перероб. зі змін. та допов. / Н. А. Агаєв, В. Г. Дикун, В. С. Чорний та ін.; за заг. ред. В. В. Стасюка./ 2020. 754 с. https://dovidnykmpz.info/wp-content/uploads/2021/10/mpz-u-zsu-2020.pdf

Шукалович М.Г.
курсант Національна академія Служби безпеки України
Атаманюк Н.О.
курсант Національна академія Служби безпеки України

АКТУАЛЬНІСТЬ ПРОБЛЕМИ ПІДГОТОВКИ ФАХІВЦІВ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ РОЗВИТКУ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

Народження та становлення незалежної України, молодої європейської держави, відбувалося в переломний момент розвитку сучасної цивілізації – переходу до інформаційного суспільства як нової суспільно-економічної формації. Узагальнюючи існуючі підходи до визначення глобального інформаційного суспільства, сьогодні під інформаційним суспільством розуміють наступне:

- це нове суспільство, що формується в результаті нової глобальної соціальної революції на основі вибухового розвитку і конвергенції інформаційних і комунікаційних технологій;
- суспільство знань, в якому знання, отримані завдяки вільному доступу до інформації та вмінню оперувати інформацією, є ключовою умовою добробуту кожної людини і держави;
- суспільство, в якому більше людей зайнято обробкою інформації, ніж переробкою сировини;
-глобальне суспільство, в якому обмін інформацією не має часових, просторових чи політичних кордонів, а наукова обробка даних і знання підтримують прийняття найбільш продуманих, обґрунтованих і своєчасних рішень, покращуючи якість життя в усіх аспектах;
- суспільство, яке, з одного боку, сприяє взаємопроникненню культур, а з іншого відкриває нові можливості для самореалізації кожної національної культури.

Проблема підготовки фахівців у сфері інформаційної безпеки стає все більш актуальною в умовах швидкого розвитку інформаційного суспільства. Зараз майже всі сфери діяльності пов'язані з обробкою інформації, тому зростає потреба у спеціалістах, які б могли забезпечувати захист цієї інформації. З одного боку, з появою нових технологій та засобів зберігання інформації, з'являються нові загрози для безпеки даних. Кібератаки, віруси, хакерські атаки та інші форми кіберзлочинності можуть призвести до витоку конфіденційної інформації, збоїв в роботі комп'ютерних систем та інших проблем. Це створює необхідність у спеціалістах, які б могли забезпечувати захист інформації та бути готовими до вирішення проблем у разі їх виникнення. З іншого боку, зростає кількість даних, які збираються і обробляються в різних сферах діяльності, від медицини та банківської справи до соціальних мереж та електронної комерції. Це створює

потребу у спеціалістах, які б могли забезпечувати захист даних та вмілим чином використовувати їх. Таким чином, підготовка фахівців у сфері інформаційної безпеки є актуальною проблемою, яка потребує уваги та інвестицій. Необхідно розвивати освітні програми, спрямовані на підготовку кваліфікованих кадрів, які б могли забезпечувати безпеку інформації.

Формування єдиного і достатньо захищеного національного інформаційно-комунікаційного простору як частини світового інформаційного простору, дозволить Україні на рівних брати участь у процесах інформаційної інтеграції та економічної інтеграції. На сучасному етапі світовий цивілізаційний процес характеризується глобалізацією, поступовим зростанням значення новітніх інформаційних технологій, підвищенням ролі інтелектуальних ресурсів та управління, соціальних, науково-технічних і гуманітарних чинників економічного прогресу та військового потенціалу держав. Всі ці цивілізаційні особливості визначають людський розвиток як головну мету, основний показник і головний важіль прогресивних змін, зумовлюють необхідність модернізації освіти та її пріоритетного розвитку. Освіта стає визначальним чинником політичного, соціально-економічного, культурного і наукового життя суспільства та важливим стратегічним ресурсом зміцнення держави, її авторитету, конкурентоспроможності на міжнародній арені, забезпечення її незалежності, національної оборони та національних інтересів. Проблеми підготовки фахівців для структур забезпечення інформаційної безпеки актуальні вже для багатьох країн світу. Першочерговий інтерес викликає досвід підготовки фахівців у США, Російській Федерації, КНР, деяких країнах ЄС та в Україні. У цих країнах основна увага приділяється підготовці фахівців з ІТ-технологій. Виявлено спільні проблеми у підготовці фахівців-юристів, які спеціалізуються на інформаційному праві, розслідуванні комп'ютерних злочинів тощо. Зростає тенденція до поєднання навчальних планів і змісту підготовки фахівців у конкретних галузях з елементами підготовки у суміжних галузях. Базова підготовка фахівців з інформаційної безпеки з вищою освітою у вищих навчальних закладах значною мірою доповнюється навчанням на курсах підвищення кваліфікації, яке в деяких країнах має переважно комерційний характер. США і Китай реалізують масштабні проекти з перепідготовки державних, бізнесових і військовослужбовців у сфері інформаційної безпеки. Китай здійснює широкі заходи з адаптації своїх громадян до інформаційного суспільства. Досить актуальними є такі питання, як відбір і підготовка фахівців, особливо у сфері професійної та освітньої діяльності, а також профілактика комп'ютерних злочинів серед фахівців з інформаційної безпеки. В цілому можна сказати, що збільшення кількісних показників розвитку систем підготовки фахівців гарантує певний якісний зсув, особливо на рівні прийняття рішень національними та міжнародними урядами щодо розвитку та забезпечення інформаційної безпеки. Україна, як і більшість країн світу, стикається зі значними викликами щодо підготовки фахівців у сфері інформаційної безпеки в умовах

розвитку інформаційного суспільства. Деякі з проблем, з якими стикається Україна, включають:

Недостатня кількість висококваліфікованих фахівців. Україна має недостатню кількість фахівців з інформаційної безпеки порівняно зі світовими лідерами в цій галузі.

Низький рівень підготовки. Більшість вишів в Україні пропонують програми з інформаційної безпеки, проте, рівень підготовки не завжди відповідає сучасним потребам і стандартам.

Недостатнє співробітництво з промисловістю. Більшість вишів в Україні не мають достатнього співробітництва з промисловістю, що ускладнює підготовку студентів та зменшує їх готовність до роботи в індустрії.

Недостатня практична підготовка. Більшість програм з інформаційної безпеки в Україні мають обмежену кількість практичних занять, що ускладнює підготовку студентів до роботи в реальних умовах.

Відсутність стандартів підготовки. Україна не має чітких стандартів щодо підготовки фахівців з інформаційної безпеки, що ускладнює порівняння різних програм та робить неможливим визначення рівня підготовки випускників.

Крім того, у зв'язку з швидким розвитком інформаційних технологій, з'являються нові загрози для інформаційної безпеки, що вимагає від фахівців постійного оновлення своїх знань та навичок. У бізнес-середовищі, де кожен день відбуваються мільйони транзакцій та обмінів даними, виток інформації може призвести до серйозних наслідків, що може знизити довіру до компанії та спричинити значні фінансові збитки.

Ось кілька кроків, які можна зробити для вирішення проблеми розвитку та забезпечення інформаційної безпеки:

1. Створення сприятливого середовища для розвитку інформаційної безпеки. Для цього необхідно сприяти створенню інноваційних технологій та інфраструктури для підтримки розвитку цієї галузі.

2. Розвиток вищої освіти. Для того, щоб підготувати кваліфікованих фахівців, необхідно забезпечити якісну вищу освіту з інформаційної безпеки. Університети повинні пропонувати спеціалізовані курси та програми навчання, які включають теорію та практичні навички.

3. Підвищення кваліфікації. Кваліфіковані фахівці з інформаційної безпеки повинні мати можливість підвищувати свої знання та навички. Для цього можуть використовуватися різні форми навчання, такі як курси, семінари, воркшопи, тренінги тощо.

4. Співпраця з приватним сектором. Приватний сектор може виступати як партнер для держави в питаннях підготовки фахівців з інформаційної безпеки. Зокрема, можливо створити програми стажування для студентів, спільні дослідницькі проекти тощо.

5. Забезпечення фінансування. На підготовку фахівців у сфері інформаційної безпеки необхідні значні фінансові ресурси.

Отже, підготовка кваліфікованих фахівців у сфері інформаційної безпеки є необхідною, щоб захистити конфіденційну інформацію, збереження репутації компаній та забезпечити безпеку користувачів в інтернеті. Таким чином, проблема підготовки фахівців у сфері інформаційної безпеки є дуже актуальною та потребує негайних дій.

Література

1. Козюра В. Д., Хорошко В.О., Шелест М.Є., Ткач Ю.М, Балюнов О.О. Захист інформації в комп'ютерних системах. Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2020. 236с.

2. Арістова І. В,. Сулацький Д. В. Інформаційна безпека людини як споживача телекомунікаційних послуг. НДІ інформатики і права НАПрН України. К.: Право України. 2013. 184 с.

3. Особливості підготовки фахівців у сфері інформаційної безпеки. Pidru4niki: веб-сайт. URL: https://pidru4niki.com/82999/politologiya/osoblivosti_pidgotovki_fahivtsiv_sferi_informatsiynoyi_bezpeki (дата звернення: 14.03.2023)

Шалигіна В.О.
студентка ННІ ІБ СК НА СБ України

ЗАХИСТ ІНФОРМАЦІЇ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ НА ПІДПРИЄМСТВІ

Забезпечення інформаційної безпеки держави вимагає використання комплексного підходу, що включає організаційні, технічні, програмні, соціальні механізми, які здатні реалізувати конституційні права і свободи людини та громадянина у сфері одержання інформації, користування нею з метою захисту конституційного ладу, суверенітету й територіальної цілісності, політичної, економічної й соціальної стабільності, законності та правопорядку, розвитку взаємовигідного міжнародного співробітництва в сфері інформаційної безпеки та інформаційного благополуччя.

Громадяни, юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, одержаною на власні кошти, або такою, яка є предметом їх професійного, діло- вого, виробничого, банківського, комерційного та іншого інтересу і не порушує передбаченої законом таємниці, самостійно визначають режим доступу до неї,

включаючи належність її до категорії конфіденційної, та встановлюють для неї систему захисту[1, с.11].

Безпека як функція (діяльність) організації передбачає виконання суб'єктами і силами безпеки конкретних видів діяльності, спрямованих на протидію, тобто запобігання загрозам і їх усунення [2, с.150]. Несанкціонований доступ - це протиправне навмисне оволодіння конфіденційною інформацією особою, що не має права доступу до охоронюваних відомостей[3].

Основними напрямами забезпечения інформаційної безпеки України в загальнодержавних інформаційних і телекомунікаційних системах є запобігання перехопленню, витоку та несанкціонованого доступу до інформації, яка обробляється чи зберігається в технічних засобах інформатизації, а також ліцензування, атестація і сертифікація об'єктів інформатизації та накладання територіальних, частотних, енергетичних, просторових і тимчасових обмежень у режимах використання технічних засобів[4, с.145].

Для того щоб створити надійну систему захисту інформації, потрібно визначити можливі способи отримання даних.

1) Способи доступу сторонніх до відомостей

Несанкціонований доступ до інформації (НСД) може бути отриманий різними способами. Пряме розкрадання документів або злом операційних систем комп'ютерів становлять лише малу частину можливих варіантів. Найбільш уразливими вважаються електронні засоби зберігання інформації, оскільки для них можуть бути використані віддалені методи управління і контролю.

Можливі варіанти отримання незаконного доступу:

- ◊ підключення до систем зв'язку (телефонні лінії, інтеркоми, дротові переговорні пристрої);
- ◊ розкрадання документації, зокрема її копіювання (тиражування) з ворожими цілями;
- ◊ безпосереднє використання комп'ютерів, зовнішніх накопичувачів або інших пристроїв, що містять інформацію;
- ◊ впровадження в операційну систему через Інтернет, зокрема з використанням шпигунських програм, вірусів та іншого шкідливого програмного забезпечення;
- ◊ використання співробітників компанії (інсайдерів) як джерел відомостей.

Ще одна внутрішня загроза - крадіжка носіїв із цінними відомостями, наприклад, програмним кодом, який є розробкою компанії. На це здатні лише довірені особи, які мають доступ до конфіденційних даних у фізичному або електронному вигляді.

2) Для чого робляться спроби доступу до чужої інформації

Основна мета несанкціонованого доступу до інформації - отримання доходу від використання чужих даних.

Можливі способи використання отриманих відомостей:

- ◊ перепродаж третім особам;
- ◊ підробка або знищення (наприклад, при отриманні доступу до баз боржників, підслідних, розшукуваних осіб тощо);
- ◊ використання чужих технологій (промислове шпигунство);
- ◊ отримання банківських реквізитів, фінансової документації для незаконних операцій;
- ◊ зміна даних з метою нашкодити іміджу компанії (незаконна конкуренція).

Конфіденційна інформація являє собою еквівалент грошових коштів. При цьому для самого власника відомості можуть нічого не означати. Однак ситуація постійно змінюється, і дані можуть раптово набути великого значення, і цей факт вимагатиме їх надійного захисту.

3) Методи захисту від несанкціонованого доступу

Створюючи систему захисту інформації (СЗІ) в організації, слід враховувати, наскільки велика цінність внутрішніх даних в очах зловмисників.

Для грамотного захисту від несанкціонованого доступу важливо зробити таке:

- ◊ відсортувати і розбити інформацію на класи, визначити рівні допуску до даних для користувачів;
- ◊ оцінити можливості передачі інформації між користувачами (встановити зв'язок співробітників один з одним).

У результаті цих заходів з'являється певна ієрархія інформації в компанії. Це дає можливість розмежування доступу до відомостей для співробітників залежно від роду їхньої діяльності.

Крім цього, програми, які компанія вирішила використовувати, повинні включати такі опції:

- ◊ аутентифікація та ідентифікація під час входу в систему;
- ◊ контроль допуску до інформації для користувачів різних рівнів;
- ◊ виявлення і реєстрація спроб НСД;
- ◊ контроль працездатності використовуваних систем захисту інформації;
- ◊ забезпечення безпеки під час профілактичних або ремонтних робіт.

4) Запобігання мережевим атакам

Комп'ютери, підключені до Інтернету, постійно піддаються ризику зараження шкідливим програмним забезпеченням. Нерідко віруси містяться в розсилках електронної пошти, потрапляють у систему через сумнівні мережеві ресурси або завантажені програми. Для захисту системи від шкідливих програм необхідно використовувати антивірусні програми, обмежити доступ до Мережі на певні сайти.

Отже, можна зробити висновок, вивчаючи властивості інформації з Державного стандарту України, що інформацію необхідно захищати Аналіз властивостей, які потребують захисту, показує, що з цієї точки зору, є два види інформації: відкрита, тобто така, яка призначена для ознайомлення усіх бажаючих,

наприклад, газети, журнали, телевізійне та радіомовлення, інформаційні сайти, реклама тощо, та інформація з обмеженим доступом, тобто така, ознайомитися з якою можна лише з санкції її власників або розпорядників. Згідно з Державним стандартом України, інформація з обмеженим доступом – це така інформація, права доступу до якої обмежено існуючими правилами та нормами[5, с.12].

Література

1. Рибальський О.В., Хахановський В.Г., Кудінов В.А. Основи інформаційної безпеки та те- хнічного захисту інформації. Посібник для курсантів ВНЗ МВС України. – Київ: Вид. Наці- ональної академії внутріш. справ, 2012. – 104 с.

2. Організація захисту інформації з обмеженим доступом: навч. посіб. / Гуз А.М., Касперський1.П., Князев С.О. та ін. - Київ: Нац. акал., СБУ, 2018. 252 с.

3. Інформаційна безпека. Навчальний посібник / С. В. Кавун В. В. Носов, О. В. Манжай. Харків: Вид. ХНЕУ, 200'.- 352 С.

4. Інформаційна безпека держави: навч. посіб. для студ. спец. 6.170103 «Управління інформаційно безпекою», 125 «Кібербезпека»/ В.І. Гур'єв, Д.В. Мсхол, 10. М. Ткач, 1.В. Фірсова. - Ніжин: ФОГу Лук' яненко В. В. ТПк «Орхідея», 2018.- 166 с.

5. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Харків : Вид. ХНЕУ, 2013. – 476 с.

Шевельова Т.Ю.
студентка ННІ ІБ СК НА СБ України

ВІД ВІДПОВІДНОСТІ ДО СТІЙКОСТІ: ПРІОРІТЕТНІ НАПРЯМКИ РОЗВИТКУ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В ДЕРЖАВІ

У сучасну цифрову епоху інформація є цінним активом, який потребує захисту від різних кіберзагроз. Держава, будучи зберігачем конфіденційної інформації, такої як національна безпека та дані громадян, несе відповідальність за забезпечення конфіденційності, цілісності та доступності своїх інформаційних систем. Щоб досягти цього, держава має вийти за межі відповідності та прийняти сталість у розвитку своєї системи управління інформаційною безпекою (СУІБ).

Відповідно до п.1 ч.4 ст. 8 Закону України «Про захист інформації в інформаційно-комунікаційних системах», Державні інформаційні ресурси та інформація з обмеженим доступом, крім державної таємниці, службової інформації та державних і єдиних реєстрів, створення та забезпечення функціонування яких визначено законами, можуть оброблятися в системі без застосування комплексної системи захисту інформації у разі виконання всіх

таких умов: підтвердження відповідності системи управління інформаційною безпекою за результатами процедури з оцінки відповідності національним стандартам України щодо систем управління інформаційною безпекою, яка проведена органом з оцінки відповідності, акредитованим національним органом України з акредитації чи національним органом з акредитації іншої держави, якщо і національний орган України з акредитації, і національний орган з акредитації такої держави є членами міжнародної або регіональної організації з акредитації та/або уклали з такою організацією угоду про взаємне визнання щодо оцінки відповідності [1].

Традиційно підходи, засновані на відповідності, використовувалися для забезпечення того, щоб інформаційні системи держави відповідали набору правових і нормативних вимог. Хоча відповідність є важливою, цього недостатньо для вирішення кіберзагроз, що постійно розвиваються, з якими стикається держава. Підходи, засновані на відповідності, як правило, зосереджені на дотриманні мінімальних стандартів, яких може бути недостатньо для забезпечення належного захисту від складних кіберзагроз. Відповідність також має тенденцію бути реактивним, зосереджуючись на виправленні проблем після їх виникнення, а не на проактивному усуненні вразливостей.

Щоб рухатися до стійкості, державі необхідно визначити пріоритети певних напрямків у розвитку своєї СУІБ. Перша сфера – управління ризиками. Держава має прийняти ризик-орієнтований підхід до інформаційної безпеки, коли ризики постійно оцінюються та управляються, а контроль запроваджується на основі рівня виявленого ризику. Такий підхід забезпечить належний захист інформаційних систем держави від найбільш серйозних загроз [2, С.54-58].

Другий напрямок – розвиток робочої сили. Держава має інвестувати в розвиток своєї робочої сили, щоб забезпечити її навички та знання, необхідні для ефективного управління ризиками кібербезпеки. Цього можна досягти за допомогою програм навчання та підвищення обізнаності, а також залучення кваліфікованих фахівців з кібербезпеки [3, С.14-15].

Третя сфера – співпраця. Кіберзагрози є глобальними, і жодна організація не може ефективно протистояти їм поодинці. Державі необхідно співпрацювати з іншими державами, організаціями приватного сектору та академічними колами для обміну інформацією та передовим досвідом, проведення спільних навчань з кібербезпеки та розробки спільних стандартів і рамок [4, С. 115-116].

Четвертий напрямок – інновації. Держава має впроваджувати інновації у розвиток своєї СУІБ. Це включає впровадження нових технологій, таких як штучний інтелект, машинне навчання та блокчейн, щоб підвищити здатність держави виявляти кіберзагрози та реагувати на них [5, С.14.].

Підсумовуючи, держава має вийти за межі відповідності та прийняти стійкий підхід до розвитку своєї СУІБ. Цей підхід вимагає пріоритетності управління ризиками, розвитку робочої сили, співпраці та інновацій. Таким чином держава

може забезпечити конфіденційність, цілісність і доступність своїх інформаційних систем і ефективно захистити себе від кіберзагроз, що постійно розвиваються.

Література

1. Закон України від 05.07.1994 №80/94-ВР «Про захист інформації в інформаційно-комунікаційних системах». URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

2. Іванова Л.Д. Інформаційна безпека в Україні: підручник / заг. ред. авт. Є.Д. Скулиш, Я.М. Жарков, Київ: Наук-видав. Відділ НА СБУ, 2019.150 с.

3. Лисенко С.О. Сучасні тенденції розвитку інформаційної безпеки як об'єкта правовідносин // Наук. Праці МАУП. Київ: МАУП, 2022. С. 20.

4. Коротун О.Г. Реалізація Директиви ЄС про захист персональних даних в Україні: проблеми та перспективи // Інформація і право. 2021. №3 (12). С. 113-125.

5. Лисенко С. О. Організаційні засади та прийоми моделювання і реконструкції при розслідуванні право-порушенн щодо інформаційної безпеки підприємств, установ та організацій // Наук. праці МАУП. Київ: МАУП, 2020. С. 24.

Ісаєв А.М.
аспірант
Державний університет Житомирська політехніка
Довгалюк В.В.
кандидат економічних наук, доцент
Державний університет Житомирська політехніка

ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА ТА ІДЕНТИФІКАЦІЯ ЕКОНОМІЧНИХ ЗАГРОЗ

У сучасних умовах зростання конкуренції та розвитку інформаційних технологій, інформаційна безпека підприємства стає однією з найважливіших складових ефективного функціонування бізнесу. Інформаційна безпека – це забезпечення доступності, цілісності та конфіденційності інформації, що обробляється та зберігається в комп'ютерних системах підприємства [1].

Один з основних викликів інформаційної безпеки полягає в ідентифікації та прогнозуванні економічних загроз. Для цього необхідно забезпечити постійний аналіз економічного середовища та внутрішнього стану підприємства. За даними дослідження Живко О.М. [2], ключовими загрозами є корупція та підробка документів, а також кібератаки на інформаційні системи підприємства.

Щоб запобігти зазначеним загрозам, необхідно розробити та впровадити ефективні механізми контролю та захисту інформації. Зокрема, на підприємстві можна встановити систему контролю за доступом до конфіденційної інформації, а також застосовувати сучасні методи шифрування даних [3].

Крім того, важливим елементом інформаційної безпеки є відповідальність персоналу підприємства. За даними дослідження Викторової Л.М. та Шеремети І.А. [4], до ризиків належать необережність персоналу у використанні електронної пошти. та соціальних мереж, а також можливість витоку конфіденційної інформації через злочинні дії співробітників. Щоб зменшити ризик таких загроз, необхідно проводити регулярні навчання та інформування персоналу щодо правил безпеки використання інформаційних технологій.Крім того, ефективним способом зменшення економічних загроз є використання заходів інформаційної аналітики та моніторингу економічного середовища. За даними дослідження Кравчука Ю.Ю. [5], застосування аналітичних інструментів дозволяє виявляти потенційні ризики та вчасно реагувати на них.

Узагальнюючи, інформаційна безпека підприємства та ідентифікація економічних загроз є складними та багатоаспектними процесами, які вимагають постійного аналізу та контролю. Відповідальний підхід до цих питань дозволить зменшити ризики та забезпечити ефективне функціонування підприємства.

Література

1. Інформаційна безпека підприємства: сутність та основні складові / Науково-практичний журнал «Економіка і організація управління». URL: http://www.economy.nayka.com.ua/?op=1&z=3304.
2. Живко О.М., Економічна безпека підприємства: проблеми та шляхи вирішення: Центр учбової літератури, 2009. – 256 с.
3. Шевченко О.В., Інформаційна безпека в умовах інтернет-бізнесу: Наукові записки Університету «КРОК». Економіка. – 2015. – Т. 2. – С. 100–104.
4. Викторова Л.М., Забезпечення інформаційної безпеки підприємства: Вісник економіки транспорту і промисловості. – 2017. – № 57. – С. 23–27.
5. Кравчук Ю.Ю., Методологічні засади інформаційної безпеки бізнесу: Вісник Одеського національного університету імені І.І. Мечникова. Економіка. – 2017. – Т. 22. – Вип. 24 (2). – С. 205–212.

Ничитайло І.М.
к.ю.н., доцент,
НА СБ України;
Слаблюк І.В.
НА СБ України

ТЕНДЕНЦІЇ РОЗВИТКУ СОЦІАЛЬНИХ МЕРЕЖ В УМОВАХ ВОЄННОГО СТАНУ

Один з відомих сучасних теоретиків суспільства мережевих структур (англ. – network society) Мануель Кастельс стверджував, що нову соціальну морфологію розвинутих суспільств становлять саме мережі, а поширення "мережевої" логіки значною мірою позначається на ході й результатах процесів, пов'язаних з виробництвом, повсякденним життям, культурою та владою [1]. Соціальні медіа (англ. – social media) – набір он-лайнових технологій, які вможливлюють спілкування користувачів між собою в різноманітних формах – налагодження контактів, взаємодія один з одним, обмін думками, досвідом і знаннями, а також новинами, відео, фото, музикою і посиланнями є важливим елементом таких мережевих структур [2].

З часу повномасштабного вторгнення рф на територію України головним джерелом новим є соціальні мережі, які країна-агресор використовує як основний інструмент комунікації. Підтвердженням цьому є повідомлення, які дедалі частіше оприлюднюються в ЗМІ щодо викриття інформаційних операцій рф, які головним чином спрямовані на військовослужбовців ЗСУ а також членів їх сімей. Тож є підстави вважати, що у поточному році ця тенденція буде лише зростати. Особливо це стосується молоді, людей з відносно низьким рівнем освіти, а також тих, хто з об'єктивних причин мають обмежені можливості у використанні альтернативних ресурсів (наприклад, ті, хто перебуває на окупованих територіях, в польових умовах, тощо).

У 2022 році ресурс Telegram посів третє місце серед лідерів у таких країнах як Малайзія, Іран, Нідерланди, Бразилія та рф і тенденція зростання користувачів зберігається перш за все серед російськомовної аудиторії.

Зазначені тенденції чудово відомі у рф та активно використовувались та використовуються нею під час повномасштабного вторгнення. Так зростання інформаційної активності російських органів влади спостерігається безпосередньо на Telegram платформі. Така активність може бути пов'язаною з реалізацією «Стратегії національної безпеки рф» в частині посилення інформаційної безпеки російського суспільства.

Облікові записи у соціальних мережах широко використовуються рф для ескалації соціально-політичної нестабільності. З початку повномасштабного вторгнення в рамках проведення російських інформаційних операцій та з метою

поширення антиукраїнського контенту кількість таких облікових записів значно зросла.

Проаналізована активність в соціальних мережах засвідчила значне збільшення кількості російськомовних повідомлень антиукраїнського спрямування, в той час як показник аналогічних повідомлень англійською мовою лишився незмінним.

Керівництво російської федерації здійснює активні заходи і у нормативній площині. Прикладом може слугувати прийняття закону № 236-ФЗ «Про діяльність іноземних осіб в інформаційно-телекомунікаційній мережі Інтернет на території російської федерації», який спрямований на перешкоджання доступу населення країни до альтернативних джерел інформації [3].

Дія цього закону поширюється на більш ніж 20 платформ, серед яких Instagram, Twitter, Facebook, YouTube, Telegram, TikTok, WhatsApp, Google, Viber, тощо.

В найближчій перспективі основним викликом інформаційній безпеці держави лишатиметься поширення дезінформації та маніпулювання інформацією в соціальних мережах.

Очевидним є той факт, що в інтересах виправдання агресії проти України рф і надалі посилюватиме використання соціальних мереж як засобу реалізації своїх зовнішньополітичних цілей та дієвого інструменту власного інформаційного впливу.

З метою поляризації та порушення інформаційної стійкості українського суспільства використання псевдопатріотичних та антиінтеграційних облікових записів лишається основним методом поширення рф інформації. При цьому головні зусилля російських суб'єктів інформаційного впливу спрямовуються на створення недовіри до державних інституцій та поширення здебільшого антиукраїнських наративів, насамперед у США та країнах ЄС.

Зі офіційними даними профільного Департаменту СБ України на даний час по Україні працює більше 7 тисяч співробітників ФСБ рф. Протягом 2022 року було викрито понад 45 ботоферм та 15 мереж мережевих агітаторів, які наносили шкоду інформаційній безпеці держави, поширюючи через 150 тисяч акаунтів коментарі, оцінки подій та репости антиукраїнської спрямованості.

Проаналізувавши численні факти витоку інформації та її оприлюднення в соціальних мережах про діяльність військовослужбовців можна зробити кілька висновків. Здебільшого противник широко використовував службову недбалість та нехтування користувачами інтернету елементарними нормами безпеки. Також при обробці та поширенні службової інформації використовувались особисті гаджети, які були підключені до інтернету і водночас для аутентифікації використовувались надто прості паролі. Неконтрольована передача файлів, використання особистих поштових скриньок також є причиною витоку певної інформації.

Іншим вразливим місцем є ідентифікація українських військовослужбовців через публікацію ними чи членами їхніх родин здебільшого на приватних сторінках у соцмережах інформації, яка вказує на їхню приналежність до ЗСУ.

Всі перелічені випадки мали місце перш за все через нехтування правилами інформаційної гігієни. І хоч вони здебільшого завдали незначної шкоди щодо безпосередньому виконанню завдань, що стоять перед ЗСУ, проте мали певні наслідки, які проявлялись у вигляді антиукраїнських публікацій, які російська пропаганда використовувала та продовжує використовувати з метою дестабілізації політичної обстановки в нашій державі в цілому, зокрема для формування негативного іміджу української армії.

Література

1. Кастельс М. Становление общества сетевых структур / М. Кастельс – (Новая постиндустриальная волна на Западе. Антология). – М. : Academia, 1999. – С. 494-505;
2. Соціальні медіа. – Режим доступа : https://uk.wikipedia.org/wiki/%D0%A1%D0%BE%D1%86%D1%96%D0%B0%D0%BB%D1%8C%D0%BD%D1%96_%D0%BC%D0%B5%D0%B4%D1%96%D0%B0
3. https://armyinform.com.ua/2021/12/04/deyaki-tendencziyi-rozvytku-soczialnyh-merezh-abo-chomu-vijskovosluzhbovczyam-potribna-informaczijna-gigiyena/

Яїцька Д.І.
аспірантка кафедри адміністративного права
Національного юридичного університету
імені Ярослава Мудрого

ОНЛАЙН-УЧАСТЬ ГРОМАДЯН В УПРАВЛІННІ ДЕРЖАВНИМИ СПРАВАМИ В УМОВАХ ВОЄННОГО СТАНУ: ПИТАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Повномасштабне вторгнення рф на територію України спричинило зміни не лише в усіх сферах життєдіяльності людей, але й значною мірою вплинуло на порядок здійснення публічного управління. Попри всі жахи, які несе за собою збройна агресія держави-терориста, народ України продовжує демонструвати світу єднання навколо демократичних цінностей, засудження будь-якого насильства та несправедливості, а також бажання брати участь в управлінні державними справами, використовуючи всі можливості та ресурси.

«Участь в управлінні державними справами» є конституційним поняттям [1], яке досі не знайшло свого тлумачення в актах законодавства України. Крім того, на сьогоднішній день не прийнято нормативно-правового акта, який би регулював питання участі громадян в управлінні. Норми, що стосуються окремих

форм громадської участі у процесі прийняття управлінських рішень, а також інформування населення про діяльність публічної влади, містяться в різних актах національного законодавства та досі не зазнали систематизації. Так, частково регулюють участь громадян в управлінні державними справами Закон України «Про звернення громадян», Закон України «Про місцеве самоврядування в Україні», Закон України «Про доступ до публічної інформації» та ін. Ще більш складна ситуація виникає із засадами, формами, інструментами та механізмами участі громадян у публічному управлінні онлайн, адже наразі єдиною законодавчою нормою, яка передбачає електронну форму громадської участі, є стаття 23-1 Закону України «Про звернення громадян», що стосується електронної петиції [2].

Аналіз практики онлайн-участі громадян в управлінні державними справами в умовах воєнного стану дозволяє окреслити коло ключових проблемних питань для інформаційної безпеки нашої держави.

1. (Не) офіційні джерела.

В умовах воєнного стану в Україні спостерігається стрімке зростання популярності новинних каналів у месенджері Telegram [3]. На відміну від новин, які транслюються телевізійними каналами, офіційної преси, така форма поширення інформації про події в усіх сферах життєдіяльності, оновлення відомостей, привернення уваги громадськості до можливої небезпеки на території України, є найбільш оперативним способом розповсюдження новин. Отже, неможливо оспорювати право телеграм-каналів на існування та фактичного (а не юридичного) присвоєння їм статусу нового засобу масової інформації. При цьому, поширення новин у такий спосіб призвело до введення в щоденний вжиток поняття «фейк» (з англ. «fake» в узагальненому розумінні - неправдива інформація). Варто зазначити, що розповсюдження фейків завжди тягне за собою негативні наслідки, проте у виняткових випадках фейк може нести пряму загрозу інформаційній безпеці держави. Розуміючи тенденцію активного розвитку інформаційних технологій, сьогодні посадові особи органів публічної влади створюють власні телеграм-канали, куди дублюють офіційну інформацію. Так, головна порада для користувача новинних каналів у Telegram - перевіряти інформацію. Кожному громадянину необхідно критично ставитися до новин та застосовувати перше правило журналістики: шукати першоджерело і тільки потім робити висновки про достовірність даних.

2. Хто є адресатом?

Соціальні мережі та месенджери створили можливості для поширення не тільки новин про ситуацію в Україні, а також і онлайн-звернень до посадовців, індивідуальних та колективних вимог до публічної влади, а також розповсюдження відомостей про грошові збори на підтримку військовослужбовців України, осіб, що постраждали від війни, дітей, тварин тощо. Складно заперечувати ефективність такого способу публічного оголошення громадської

думки з того чи іншого питання управління, але як і у випадку з новинами, можливості мережі Інтернет створюють реальні загрози для інформаційної безпеки України, а також є ґрунтом для шахрайства. Перші місяці від початку повномасштабного вторгнення рф на територію України показали, серед іншого, що громадськість, знаходячись у стані страху, паніки та невизначеності, звернулась до всіх можливих способів повідомити державу про події, які відбулися в конкретних регіонах, містах і селах, щодо певних людей, будівель, проблем житлово-комунального забезпечення тощо. У вже відомих телеграм-каналах, а також у соціальних мережах Instagram, Facebook, Twitter почали з'являтися пости (від англ. «post» – публікувати) з безадресними вимогами, спрямованими на привернення уваги населення та влади України до локальних подій чи історій конкретних осіб. Як правило, такі повідомлення для широкого загалу містили емоційні заклики на кшталт «Не забувайте про (місто)!», «(Місто) щоденно знищують ракетами!», «Усі говорять тільки про (місто), а (інше місто) постійно потерпає!» і т.д. Подібні звернення підкріплювалися фотографіями, що зображують наслідки збройної агресії рф на території України, не містили конкретних вимог до визначеного адресата, і єдина мета, якої могли досягти автори – поширення паніки серед населення. Громадяни, що бачили такі звернення, як правило, розміщували їх на своїх сторінках (робили «репости»), і таким чином вони набували широкого розповсюдження. Звичайно, звернення, яке не містить чітких вимог та адресується невизначеному колу осіб, не є ефективним інструментом участі в публічному управлінні, допомоги тим, хто її потребує тощо, а лише створює загрозу для інформаційної безпеки держави, адже дає реальні можливості ворогу маніпулювати суспільною свідомістю населення України.

3. Цілі (не) виправдовують засоби.

Поставивши на меті активну участь в управлінні справами держави в умовах воєнного стану, громадяни стали частіше використовувати всі можливості для висловлення власної політичної позиції та оприлюднення інформації про осіб, позиція яких відрізняється від думки більшості, з метою досягнення публічного осуду та притягнення до юридичної відповідальності. Після першого етапу життя в умовах війни, розпочатої рф, коли питому вагу в публічному онлайн-просторі займали повідомлення про конкретні злочини держави-терориста, про збори коштів на підтримку військовослужбовців, цивільних осіб, сімей, регіонів тощо, суспільство перейшло до другого етапу, за якого значна увага стала приділятися елементам нашої державності, у першу чергу, мовному питанню. На ґрунті різниці в поглядах громадян України на можливість і необхідність переходу в усіх видах і сферах спілкування на державну мову почали виникати конфлікти не лише між окремими особами, організаціями, а й між регіонами заходу і сходу України. У якийсь часовий момент більша частина публічного онлайн-простору була присвячена виключно конфліктам щодо мовного питання. Не вдаючись до суб'єктивної оцінки аргументів обох сторін, зазначимо, що будь-які внутрішні

національні конфлікти в жодному разі не допомагають у захисті територіальної цілісності та незалежності держави, а завжди лише створюють можливості для інформаційних атак ворога, маніпуляцій, спрямованих на штучний розкол народу України та протиставлення людей першої групи переконань до тих, хто підтримує другу.

Незважаючи на значну кількість проблем, створених російською агресією на території України, що вчиняється в епоху розвитку інформаційних технологій, коли більшість громадян має доступ до можливостей мережі Інтернет, несправедливо було б ігнорувати безліч позитивних моментів. Так, завдяки інструментарію соціальних мереж, месенджерів, веб-сайтів і порталів сьогодні можна говорити про: 1) швидкість у поширенні новин та інформаційних матеріалів від представників органів публічного управління; 2) можливість публічного обговорення того чи іншого питання без організації офлайн-зборів громадськості, які є небезпечними в умовах воєнного стану та постійних атак держави-терориста; 3) можливість оперативного залучення великої кількості небайдужих громадян до матеріальної підтримки військовослужбовців та цивільних осіб, які постраждали від війни; 4) онлайн-звернення до посадових осіб органів публічної влади та військового керівництва як пріоритетну форму звернення громадян.

Підсумовуючи викладене, зазначимо, що в умовах воєнного стану, який було запроваджено в Україні в результаті збройної агресії рф, в епоху розвитку цифрових технологій, щоденно виникають нові загрози для інформаційної безпеки держави. Але незважаючи на складність підтримання порядку в національному онлайн-просторі, можливості, надані сьогодні українцям соціальними мережами і месенджерами, веб-сайтами і порталами, дозволяють оперативно та безпечно брати участь у вирішенні питань публічного управління, не виходячи з дому, не знаходячись на території України, не відриваючись від навчання, роботи тощо. Пріоритетні завдання держави та її органів у цьому напрямі: 1) створення нормативно-правової бази для легального використання можливостей мережі Інтернет як інструментів участі громадян в управлінні державними справами; 2) забезпечення своєчасного моніторингу відомостей, що потрапляють у мережу, на предмет законності, відсутності порушення державної таємниці, суб'єктів, якими розміщується інформація тощо, тобто підтримання інформаційної безпеки онлайн-середовища.

Література

1. Конституція України: Закон від 28.06.1996 № 254к/96-ВР. Відомості Верховної Ради України (ВВР), 1996, № 30, ст. 141 (дата звернення: 14.03.2023 року).

2. Про звернення громадян: Закон України від 02.10.1996 № 393/96-ВР. Відомості Верховної Ради України (ВВР), 1996, № 47, ст.256 (дата звернення: 14.03.2023 року).
3. Telegram. URL: https://web.telegram.org/k/.

Бідюк Ю.В.
аспірант ВАіД НА СБ України
Беседа Д.В.
к.ю.н., доцент КІБД НА СБ України

ІНФОРМАЦІЙНІ СИСТЕМИ ЄВРОПЕЙСЬКОГО ПОЛІЦЕЙСЬКОГО УПРАВЛІННЯ ЯК ІНСТРУМЕНТ БОРОТЬБИ З ОРГАНІЗОВАНОЮ ЗЛОЧИННІСТЮ

Європейське поліцейське управління (ділі – Європол) є правоохоронною організацією ЄС, основна мета якої полягає у підвищенні ефективності взаємодії компетентних органів країн-членів ЄС у сфері боротьби з міжнародними тяжкими злочинами і тероризмом.

Аналіз – основна діяльність Європолу. Для того, щоб партнери більш глибоко розуміли стан і загрозливі тенденції організованої злочинності, Європол щорічно проводить моніторинг стану організованої злочинності, на підставі якого здійснюється перспективна комплексна її оцінка, що надає можливість формувати варіативну частину прогнозу злочинності і тероризму в ЄС.

Як організація, Європол еволюціонував від збирання інформації та її аналізу до підтримки розслідувань на всіх рівнях та стадіях – від початку до реалізації справи й далі за її результатами.

На сьогодні відбувається уніфікація правоохоронної політики країн-членів ЄС, що ґрунтується на спільно визначених підходах, керівних принципах, розроблених Європолом. Останньою тенденцією в розвитку цієї організації стало створення мобільних офісів для підтримки розслідувань. На сьогодні вони діють у Греції та Італії в рамках спільних заходів із протидії нелегальній міграції.

У рамках Європолу створено систему накопичення та аналізу даних, орієнтовану на покриття потреб країн-членів (Europol’s Crime Analysis System, ECAS). Ця система кримінального аналізу містить потужні інструменти, що мають на меті створення та розповсюдження аналітичних продуктів для більш ефективної ідентифікації, локалізації та нейтралізації загроз транснаціонального характеру на загальноєвропейському рівні. Система продовжує розвиватися і включатиме в себе нові продукти, спрямовані на удосконалення інформаційного обміну та забезпечення потреб поточних розробок, що здійснюються правоохоронними органами країн-членів.

Останній нормативно-правовий акт, що регулює діяльність Європолу, прийнятий у травні 2017 р. [1]. Так, відповідно до Регламенту Європолу його завданням є підтримка дій правоохоронних органів країн-членів, співробітництва між ними на дво- та багатосторонньому рівнях. На сьогодні до штату Європолу входить понад 1000 співробітників, а їхня інформаційна система забезпечує обмін 40000 повідомлень на рік.

Європол не має виконавчої влади, тобто його співробітники не можуть здійснювати арешти, проводити власні операції та розслідування, ініціювати правоохоронні дії. Країни-члени залишаються власниками інформації, яку вони надають до Європолу, що визначає можливості її подальшого використання. Оскільки Європол не має повноважень на самостійне здійснення правоохоронної діяльності, він не може самостійно збирати інформацію і має покладатися на дані, надані країнами-членами. Водночас він здійснює прямий чи опосередкований (через нормативно-правові акти Європейської Комісії та Парламенту) вплив на визначення національних стратегій і формулювання правил здійснення інформаційного обміну, у тому числі шляхом управління базами даних, такими як Шенгенська інформаційна система.

У структурі Європолу діє три основні центри – з питань протидії організованій злочинності, з питань протидії кіберзлочинам та з питань протидії тероризму.

Основними базами даних, що діють у Європолі, є його Інформаційна система (Europol's Information System, IS), Європейська система даних із обліку бомб (European Bomb Data System, EBDS) та Європейська аналітична система (Europol Analysis System, EAS) [1].

IS використовується передусім для підтримки конкретних розслідувань й орієнтована на накопичення та оцінювання інформації, зібраної країнами-членами та переданої до Європолу. Її функції включають пошук, візуалізацію інформації та виявлення зв'язків. Останнє дає змогу встановлювати зв'язки між даними щодо різних об'єктів та їхню класифікацію. Дані, що вносяться до цієї бази, мають бути стандартизованими відповідно до єдиного шаблону.

Діяльність інформаційних мереж Європолу ґрунтується на принципі доступності, що означає здатність будь-якої країни-члена мати доступ до даних. Цей принцип є ключовим для забезпечення швидкого обміну інформацією між країнами-членами ЄС.

Інформаційна система Європолу на сьогодні відіграє важливу роль у правоохоронній діяльності країн-членів ЄС, у яких навіть поліцейські, котрі працюють на вулицях, мають доступ до окремої інформації з баз даних Європолу.

Захищена система передачі інформації (SIENA) виступає основним механізмом обміну даними в мережі Європолу. Вона використовується для обміну стратегічними й оперативними матеріалами правоохоронного характеру.

Система введена в експлуатацію 1 червня 2009 р., і на сьогодні до неї підключені правоохоронні органи країн ЄС, а також Євроюст та Інтерпол. Вона також має абонентські пункти в Австралії, Канаді, Норвегії, Ліхтенштейні, Молдові, Швейцарії, США та Україні [1].

SIENA також забезпечує функціонування регіональних ініціатив, таких як Центр з аналізу та операції проти незаконного переміщення наркотиків морським каналом (Maritime Analysis and Operations Centre – Narcotics), центри взаємодії митних та правоохоронних органів, підрозділи із обміну даними щодо пасажирів авіарейсів, підрозділи фінансової розвідки.

За останні три роки обмін інформацією цією системою зріс на 40-50% щорічно. У 2022 р. вона використовувалася 1200 компетентними органами 47 країн та 10 міжнародних організацій [1].

Інформаційна система Європолу використовується передусім для підтримки конкретних розслідувань та орієнтована на накопичення й оцінювання інформації, зібраної країнами-членами та переданої до Європолу. Її функції включають пошук, візуалізацію інформації та виявлення зв'язків. Останнє дає змогу встановлювати зв'язки між даними щодо різних об'єктів, їх класифікувати. Дані, що вносяться до цієї бази, мають бути стандартизованими відповідно до єдиного шаблону.

Оперативний департамент Європолу здійснює інформаційний обмін через SIENA з країнами ЄС, третіми країнами, а також офіцерам зв'язку при Європолі. Вона є єдиним способом обмінюватися персональними даними.

Інша система – Європейська інформаційна система (EIS)

– в автоматичному режимі перевіряє наявність інформації в базі даних та

будує схему зв'язків, забезпечує прямий доступ до інформації для країн-членів ЄС [1].

До інших інформаційних систем також відносяться Поточний аналітичний проект (Current Analysis Project), що використовується для проведення аналітичної роботи.

У SIENA існує можливість закрити запити на інформацію. Так, інші країни дізнаються, що Україна робила запит щодо певної інформації лише зі згоди української сторони.

Також діє Електронна платформа для експертів, доступ до якої відкривається за запрошенням від її менеджменту. Ця система не є захищеною і призначена для обговорення різних питань правоохоронного характеру між експертами.

Через систему SIENA може здійснюватися обмін даними на двосторонньому рівні, при цьому Європол не зможе прочитати цю інформацію, якщо не існує відповідної авторизації. Тобто Україна може направити інформацію через цю систему, наприклад, до Молдови, при цьому Європол не зможе її прочитати. Водночас експерти Європолу зазначають, що найкраще надавати йому таку авторизацію, оскільки так інформація буде краще використана.

Підготовлені Європолом інформаційні продукти використовуються всіма правоохоронними органами країн ЄС, а також багатьма структурами інших країн.

Окрім планових інформаційних продуктів, аналізуються й конкретні проблеми, зокрема вплив на організовану злочинність, розширення зони євро, візової лібералізації, проведення певних масштабних заходів (наприклад, Олімпійських ігор), щодо ситуації в окремих регіонах (наприклад, Західні Балкани, Афганістан), а також щодо окремих організованих злочинних угруповань (китайська, італійська, латиноамериканська організована злочинність).

Як правило, акцент робиться на прогностичній роботі – звіт має вказувати тенденції розвитку ситуації та пропонувати напрями реагування на зміни.

На 2022 р. в інформаційних системах Європолу містяться 637153 інформаційні об'єкти і дані на 28000 осіб. У першому кварталі 2023 р. в цих системах виконано 587000 пошукових запитів [1].

Для внесення інформації до баз даних та передачі інформації передбачається використання універсального формату повідомлень (UMF), який визначає їхнє структурування. На сьогодні цей стандарт ще застосовується не всіма країнами-членами на національних рівнях. У системі SIENA він використовується для інформації щодо осіб.

У рамках організації також діє система Платформа Європолу для експертів (Europol Platform for Experts), що являє собою захищене середовище для взаємодії експертів з правоохоронних питань. На сьогодні в його роботі беруть участь 1500 експертів із 85 країн світу. Доступ до системи здійснюється за запрошеннями від національних підрозділів Європолу.

Для обміну інформацією між підрозділами Європолу використовується власна мережа CT SIENA, що діє окремо від мережі SIENA. Її учасниками є 46 країн – члени ЄС і треті країни. При цьому суттєва увага приділяється аналізу відкритих джерел, із яких отримується до 80% інформації. Ще 15% інформації отримується технічним шляхом і 5% – від агентурних джерел. Підрозділом цього Центру є Відділ з моніторингу Інтернету (Internet Referral Unit), що відслідковує випадки пропаганди насильства через Інтернет [1].

Резюмуючи викладене, можна зробити висновок про те, що впровадження підходів, що реалізуються Європолом в інформаційній сфері, в нашій країні має розглядатися як важливий напрям реалізації політики європейської інтеграції. Це сприятиме суттєвому підвищенню ефективності діяльності національний правоохоронних органів та забезпечить їх інтеграцію до загальноєвропейського правоохоронного простору.

Література

1. Europol, Europol. About Europol. Europol's structure and purpose. [Електронний ресурс]. – Режим доступу: https://www.europol.europa.eu .

Скляренко Є.Є.
курсант групи НБ-211 НА СБ України
Кононова Д.В.
канд. філол. наук, доцент НА СБ України

СУЧАСНІ ТЕНДЕНЦІЇ ПРОТИДІЇ СУЧАСНИМ ВИДАМ КІБЕРЗАГРОЗ ТА КІБЕРАТАК рф

Від початку російсько-української війни в 2014-му році на ряду з бойовими діями, що розпочались на землі, у повітрі та на морі, українська система забезпечення кібербезпеки вступила у глобальну кібервійну. Цілями російських хакерів стали вразливі місця в інформаційному забезпеченні об'єктів критичної інфраструктури. Так, у грудні 2015 року Україну атакували російські хакери, які зуміли здійснити кібератаку на енергетичну інфраструктуру країни. Атака призвела до того, що більше 200 тисяч людей залишилися без електропостачання.

Саме тому метою цього дослідження є усвідомлення стану і положення української системи кібербезпеки у сфері забезпечення захисту об'єктів критичної інформаційної інфраструктури, яка гарантує забезпечення достатнього рівня життя громадян.

Актуальність цього питання полягає у тому, що в умовах повномасштабної війни практично всі українці відчувають наслідки кожної такої атаки. Надзвичайно гостро подібна реакція відчувалася зовсім нещодавно, під час цілеспрямованих ракетних ударів зс рф по енергетичній інфраструктурі, яким завжди передували кібератаки.

Тож спершу хотілося б розповісти про походження подібного підходу держави-агресора до ведення бойових дій у кіберпросторі. Дезінформація, пропаганда, атаки на системи зв'язку і передачі інформації – це не просто акції, що застосовуються агрессором рідко і локально, насправді ж – це тактика, яку зс рф взяли на озброєння досить давно. Ця тактика була відпрацьована державою-агресором у попередніх збройних конфліктах зокрема, під час агресії проти Грузії). Це означає, що вивчення та ефективне протистояння їй – зможе запобігти подальшому її використанню проти інших держав. Росія має отримати гідну відповідь на всі свої агресивні дії сьогодні, адже завтра вона повернеться з ще більш зухвалими атаками, які не будуть обмежуватися лише Україною.

Поширеною є думка, що кібератаки – це зброя майбутнього. Однак війна в Україні доводить, що це майбутнє вже настало. Оборонна доктрина і міжнародне право повинні швидко адаптуватися до вже реалізованих і поки що потенційних загроз з боку подібних явищ.

Багатовимірна війна, тобто нестандарний підхід до ведення бойових дій – це новий виклик безпеці (який є передбачуваним, але до якого ще не готові належним чином). Росія, звичайно, не єдина загроза міжнародній безпеці. Інші

авторитарні режими можуть розглядати все це як уроки і використовуватимуть цей підхід у майбутньому.

Цікавим може бути той факт, що традиційні види агресії можуть з часом поступитися кібератакам за своїм негативним впливом. Сьогодні приклад російської агресії показує, що хакери можуть атакувати все, що завгодно. Однак є певні речі, які мають пріоритет.

- Урядові інституції (як центри прийняття рішень для підтримання внутрішньої стабільності),

- Цивільна інфраструктура та енергетика (росія є державою-терористом, що хоче збільшити страждання мирних громадян, не досягаючи нічого на полі бою)

- ЗМІ та комунікації (ці атаки посилюють російську пропаганду, яка зарекомендувала себе як перевірена зброя путінського режиму).

Основні цілі російських хакерів змінилися з початку війни. Напередодні вторгнення і в перший місяць війни кібератаки були спрямовані на комунікації, щоб обмежити функціонування української армії та уряду, але після перших невдач на лінії фронту російські зловмисники зосередилися на завданні максимальної шкоди цивільному населенню. Ця зміна стратегії очевидна в усіх аспектах агресії. Атаки на енергетичну інфраструктуру є яскравим прикладом. Вони є добре продуманими з точки зору вибору часу і цілей. Зрештою, перша велика атака на енергетичну інфраструктуру відбулася взимку, щоб створити додатковий тиск на цивільне населення, якому набагато важче пристосуватися, ніж військовим.

Розвиток інформаційних технологій тягне за собою появу нових видів кібер-атак. Відповідно, інформаційна безпека стає одним з основних компонентів національної безпеки. Україна почала робити активні кроки в цьому напрямку. Забезпечення інформаційної безпеки вимагає не тільки створення стійкої до кібератак інфраструктури (одним з елементів розв'язання цієї проблеми можуть стати квантові комп'ютери), а й цифрового суверенітету (розробка українського програмного та апаратного забезпечення). Також необхідно прискорити міжнародне співробітництво з протидії кібератакам терористичних організацій і держав та використання кіберзброї для боротьби з ними. Однак на сучасному етапі найперспективнішим напрямом підвищення інформаційної безпеки засобів управління і зв'язку та інформації в рамках наявних технологій є багаторівневий багатопозиційний захист (МЛЗ), для якого характерним є використання апаратних та програмних засобів і методів захисту засобів та інформації.

Загалом, можна зробити такі висновки:

Кіберпростір має стати інструментом асиметричної відповіді на агресію і бути спрямованим на контроль не лише власних засобів, а й засобів супротивників.

Кібербезпека сьогодні стає новою галуззю військово-промислового комплексу, спрямованою на забезпечення національної безпеки, тому своєчасне

планування та реалізація заходів із забезпечення кібербезпеки та інформаційної війни на глобальному та регіональному рівнях є одним із пріоритетів держави. Україна може і повинна перестати концентруватися виключно на оборонних заходах. Володіючи одним із провідних у світі людським потенціалом ІТ-фахівців, здатністю працювати швидко й ефективно та високою мотивацією протистояти зовнішній агресії, держава повинна робити ставку не тільки на оборонні, а й на наступальні технології, включно з кіберзброєю.

Література

1. Кібератаки, артилерія, пропаганда. Загальний огляд вимірів російської агресії [Редакція від 17.01.2023 р.] : https://cip.gov.ua/ua/news/kiberataki-artileriya-propaganda-zagalnii-oglyad-vimiriv-rosiiskoyi-agresiyi

2. Інформаційна безпека в умовах гібридної війни (2017) // Міжнародна науково-практична конференція (16-17 листопада 2017 року) : https://nadpsu.edu.ua/wp-content/uploads/2021/07/3nadpsu_3_03_2017.pdf

3. Шевченко В. Як відбувається перша світова кібервійна. https://armyinform.com.ua/2023/02/01/yak-vidbuvayetsya-persha-svitova-kibervijna/

Картавцева К.О.
курсант НА СБ України
Сидоренко С.М.
ст.викладач НА СБ України

СУЧАСНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ

Результати бойових дій у кіберпросторі є визначальними для загального розвитку бойових дій у сучасних протистояннях. Кібератаки та кібервторгнення можуть спричинити хаос, або завдати значної шкоди критичній інформаційній інфраструктурі. Це стосується в першу чергу кібератак на енергетичні, транспортні та військові об'єкти. Протягом цього періоду виведенні з ладу об’єкти управління постачанням, управління логістикою тощо. Починаючи з 2014 року спостерігаються напади протягом усього протистояння з Російською Федерацією.

У ніч масового військового вторгнення російських загарбників на територію України 24 лютого 2022 року, здійснені масовані атаки на українську інформаційну мережу. Завдяки завчасним заходам кіберзахисту наслідки зведені до мінімуму. З останніх подій – напади на банківські установи. Збитки завдані, однак через швидке реагування системи кіберзахисту, втрати були незначними. Також, кібератакам піддавалися сайти державних установ та центральних органів влади, де зловмисники розміщували провокаційну рекламу, або відключали її за допомогою DDoS-атак.

Основні способи кібератак пов’язані з використанням шкідливого коду та спробами використання вразливостей системи для проникнення. Шкідливий код проникає найчастіше через порушення користувачем кібергігієни – перехід на небезпечні сайти, відкриття вкладень у підозрілих електронних листах. Ступінь успішності вторгнення визначається якістю системи захисту.

Неналежний захист каналів фінансових операцій в Інтернеті є найпоширенішою причиною витоку особистої інформації. Зокрема, громадяни України здійснюють ризиковані закупівлі у неперевірених інтернет-магазинах, або відвідують нелегальні онлайн-казино.

Ігрова індустрія є висококонкурентною галуззю. Нелегальні компанії прагнуть отримати перевагу над ліцензованими представниками грального бізнесу. Сумнівні казино купують хакерські послуги через нездатність надати клієнтам високий рівень обслуговування та якісне програмне забезпечення.

Хакери використовують отримані особисті дані для проникнення в електронну пошту та банківські рахунки користувачів. Інформація може бути передана третім особам, або використана злочинцями у корисливих цілях. Втрата даних пов’язана зі значним репутаційними ризиками для ігрових компаній – падає довіра клієнтів.

Система виявлення вторгнень. Система виявлення вторгнень – це програмний або апаратний засіб, призначений для виявлення факту несанкціонованого доступу до комп'ютерної системи чи мережі, або виявлення несанкціонованого управління, переважно через Інтернет.

Система SIEM збирає інформацію про будь-яку активність зловмисного програмного забезпечення, або про перерви у нормальній роботі. Системи SIEM обробляють дані з багатьох джерел і використовують методи фільтрації сповіщень, щоб відрізнити несанкціоновану активність від помилкових спрацьовувань.

Деякі системи виявлення вторгнень можуть виявити початок мережевої атаки, інші здатні виявляти атаки, раніше невідомі. Така система називається системою запобігання вторгненням. IPS не обмежується сповіщеннями, а також виконує різні заходи, спрямовані на припинення атак.

На практиці, програмно-апаратні рішення часто поєднують функціональність обох систем. Їх об'єднання називають IDPS (IDS і IPS).

Хоча існує багато типів IDS – від одного комп’ютера до великої мережі – найпоширенішими класифікаціями є системи виявлення вторгнень у мережу та на основі хосту. Прикладом HIDS є система, яка відстежує важливі файли операційної системи, а прикладом NIDS є система, яка аналізує вхідний мережевий трафік. IDS також можна класифікувати за методами виявлення загроз: найбільш відомими є виявлення на основі сигнатур і виявлення аномалій.

Виявляти вразливі місця в програмних і апаратних системах. Вразливості програмного забезпечення є основною мішенню для атак, які можуть завдати

шкоди роботі та репутації мільйонів систем у всьому світі та призвести до величезних фінансових втрат. Тому для виявлення вразливостей у програмному забезпеченні та системах, апаратне забезпечення є одним із основних завдань кібербезпеки. Інструменти виявлення вразливостей уже давно використовується в системах розробки програмного забезпечення, а також в окремих системах тестування. Виявлення вразливостей розглядається, як на рівні вихідного коду, так і на рівні двійкового коду мов програмування високого рівня.

Системи розробки програмного забезпечення забезпечують виявлення вразливостей на основі несправних фрагментів коду, що дає можливість створювати так звані експлойти. Експлойт — сценарій поведінки та пов'язані з ним дані, які зловмисник може використати для здійснення вторгнення, щоб скомпрометувати систему, скомпрометувати особу, або захопити контроль над системою.

Основним недоліком використання фрагментів програмного коду є те, що такий підхід не гарантує відсутність інших вразливостей. Наприклад, вразливості можуть бути у бібліотеках, які використовує програма, і жоден аналіз на рівні вихідного коду їх не виявить. Зокрема, це відбувається у випадках некоректного використання бібліотек.

Виявлення вразливих фрагментів коду може бути неправильним, тобто виявлена вразливість ніколи не працюватиме під час виконання програми.

Ще один спосіб представлення вразливостей – їх формальні шаблони. Також, використовуються методи моделювання коду, хоча вважається, що вони забезпечують досить низьке покриття.

Обидва методи використовують системи для виявлення вразливостей у двійковому коді. У цьому випадку виникає проблема адекватного представлення вразливостей на рівні двійкового коду з мови програмування, на якій написана програма.

У випадках виявлення вразливості важливі подальші дії. Якщо на рівні програмування на мові високого рівня пропонується замінити помилкові фрагменти більш безпечними, розглядається можливість застосування методів автоматичного виправлення помилок на рівні двійкового коду.

З одного боку, автоматичне виправлення помилок може призвести до непередбачуваної поведінки програми, а з іншого – виправлення може бути правильним, якщо воно еквівалентне, тобто не змінює поведінку програми. Але це необхідно перевіряти формальними методами.

Висновок. Сучасні системи захисту інформації у корпоративній мережі дозволяють вибрати найбільш ефективний і дієвий спосіб захисту інформації, що проходить через ІТС. Власники ІТС мають можливість вибирати зі свого бюджету необхідні механізми захисту, починаються з антивірусного програмного забезпечення і закінчуючи системою виявлення та запобігання вторгненням.

Кінцевою метою власника ІТС є розробка повної системи захисту інформації, в тому числі – інформації з обмеженим доступом.

Література

1. Даник Ю.Г., Воробієнко П.П., Чернега В.М. Основи кібербезпеки та кібероборони – Одеса, 2019. 320 с.

2. Богуш В.М., Богуш В.В., Бровко В.Д., Настрадін В.П. Основи кіберпростору, кібербезпеки та кіберзахисту – Київ, 2020. 532 с.

3. Ніколаюк С.І., Никифорчук Д.Й., Томма Р.П., Барко В.І. Протидія злочинам у сфері інтелектуальної власності. Київ., 2006. URL https://science.lpnu.ua/sites/default/files/journal-paper/2019/sep/18399/23.pdf (дата звернення 14.03.2023 р.)

РЕКОМЕНДАЦІЇ
XIV Всеукраїнської науково-практичної конференції «Актуальні проблеми управління інформаційною безпекою держави»

30 березня 2023 року Національною академію Служби безпеки України спільно з Інститутом модернізації змісту освіти Міністерства освіти і науки України проведено XIV Всеукраїнську науково-практичну конференцію «Актуальні проблеми управління інформаційною безпекою держави».

Участь у конференції прийняло більше 60 осіб очно та 400 осіб в онлайн режимі.

Основними напрямками роботи конференції були:

1. Проблеми протидії інформаційним, психологічним та когнітивним впливам рф на особовий склад збройних формувань структур сектору безпеки і оборони України.
2. Проблеми забезпечення кібернетичної безпеки об’єктів критичної інформаційної інфраструктури.
3. Проблемні питання захисту інформації з обмеженим доступом в умовах збройної агресії рф.
4. Пріоритетні напрямки розвитку системи управління інформаційною безпекою держави.

У рамках конференції відбувся круглий стіл «Перша в світі кібервійна. Вплив першої світової кібервійни на стан національної безпеки України», де у дискусії прийняли участь: заступник Секретаря Ради національної безпеки і оборони України, генерал поліції 3-го рангу Сергій ДЕМЕДЮК, народний депутат України, член Комітету Верховної Ради України з питань національної безпеки, оборони та розвідки Олександр ФЕДІЄНКО, заступники Міністра оборони України з питань цифрового розвитку, цифрових трансформацій і цифровізації Віталій ДЕЙНЕГА, начальник Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Служби безпеки України Ілля ВІТЮК, начальник Департаменту кіберполіції Національної поліції України Юрій ВИХОДЕЦЬ, віце–президент Київської торгово-промислової палати Володимир КОЛЯДЕНКО, заступник Голови з питань цифрового розвитку, цифрових трансформацій і цифровізації Держспецзв'язку Віктор ЖОРА, заступник начальника управління Головного управління радіоелектронної та кіберборотьби Генерального штабу Збройних сил України, майор Володимир МАМЧУР, професор кафедри стратегії національної безпеки і оборони Національного університету оборони України імені Івана Черняхівського Василь ТЕЛЕЛИМ, керівник по роботі з державним сектором ТОВ «Майкрософт Україна» Євген КАХАНОВСЬКИЙ, технічний директор Представництва «Cisco Systems менеджемнт Б.В. в Україні» Олексій БЕСАРАБ.

Учасники конференції за результатами обговорення питань конференції та наукової дискусії рекомендували:

1. Визначити нагальною потребою проведення всебічного дослідження першої кібервійни та її впливу на національну безпеку України. Дослідження провести в формі комплексної міжвідомчої науково-дослідної роботи з обґрунтування теоретичних засад забезпечення національної безпеки в інформаційній та кібер сферах в умовах кібервійни на замовлення Ради національної безпеки і оборони України.

Метою науково-дослідної роботи є обґрунтування завдань суб'єктів сектору безпеки і оборони із забезпечення кібероборони держави.

Основними завданнями науково-дослідної роботи є:

синтез термінологічного апарату «кібервійни»;

визначення учасників (комбатантів) кібервійни;

обґрунтування форм та способів протиборства в інформаційній сфері та кіберпросторі;

обґрунтування завдань суб'єктів сектору безпеки і оборони із забезпечення кібероборони держави.

*Результатами науково-дослідної роботи мають стати***:**

модель кібервійни. Тлумачний словник термінів (понятійний апарат) кібервійни;

форми та способи застосування сил та засобів у кібервійни. Класифікатор дій кібервійни;

перелік сил та засобів складових сил оборони, які залучаються до ведення дій кібервійни;

система управління веденням кібервійни: структура органів управління, повноваження;

візія системи підготовки персоналу сектору безпеки і оборони із забезпечення кібероборони держави;

рекомендації щодо змін до нормативно-правової бази із забезпечення національної безпеки в кіберпросторі, кібероборони держави.

2. Складовим сектору безпеки і оборони України продовжити роботу з підвищення рівня медіа-грамотності, інформаційної безпеки та кібер гігієни військовослужбовців та працівників структур Сектору безпеки і оборони України.

3. Створити на базі НА СБУ постійно діючу платформу з обміну досвідом між представниками органів державної влади, науковими установами та профільними громадськими організаціями щодо налагодження ефективного співробітництва для забезпечення національної безпеки (на рішення ректора НА СБУ).

4. Вважати за доцільне розгортання навчально-практичного ситуаційного центру для:

підвищення якості підготовки здобувачів вищої освіти зі спеціальності «Національна безпека (кіберзахист, забезпечення державної безпеки в інформаційній сфері) 256.04;

забезпечення проведення підвищення кваліфікації співробітників підрозділів інформаційно-аналітичного забезпечення СБ України;

відпрацювання алгоритмів, методик ситуаційного аналізу оперативної обстановки, виявлення найбільш ефективних методів стратегічного аналізу.

5. Профільному міністерству (Міністерству оборони України) доопрацювати положення проєкту Закону України «Про безпеку класифікованої інформації» в частині щодо безпеки інформації з урахуванням безпекової практики держав-членів НАТО та ЄС, створення уніфікованої системи забезпечення безпеки інформації шляхом поєднання державної таємниці та службової інформації в єдину категорію інформації, перегляду засад віднесення відомостей до класифікованої інформації, зокрема військової таємниці.

6. Вважати актуальним напрямок діяльності суб'єктів забезпечення інформаційної безпеки щодо організації розробки та впровадження у практичну діяльність інструментарію експертно-аналітичної підтримки системи управління інформаційною безпекою.

7. Вважати за доцільне в НА СБУ розроблення та впровадження в освітній діяльності програмного забезпечення моделювання процесів управління інформаційною та кібербезпекою, віртуальних середовищ колективних фахових знань.

ЗМІСТ

СЕКЦІЯ 2
ПРОБЛЕМИ ПРОТИДІЇ КІБЕРНЕТИЧНИМ АТАКАМ рф НА ОБ'ЄКТИ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

СЕКЦІЯ 3
ПРОБЛЕМНІ ПИТАННЯ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ В УМОВАХ ЗБРОЙНОЇ АГРЕСІЇ рф

СЕКЦІЯ 4
ПРІОРИТЕТНІ НАПРЯМКИ РОЗВИТКУ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ ЗА ОЦІНКАМИ МОЛОДИХ ВЧЕНИХ, ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ