**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
**ІНСТИТУТ МОДЕРНІЗАЦІЇ ЗМІСТУ ОСВІТИ**

**НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ**

**НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ІНФОРМАТИКИ І ПРАВА**
**НАЦІОНАЛЬНОЇ АКАДЕМІЇ ПРАВОВИХ НАУК УКРАЇНИ**

# АКТУАЛЬНІ ПРОБЛЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ

**XI Всеукраїнська науково-практична конференція**

**Збірник тез наукових доповідей**
**(Київ, 15 травня 2020 року)**

*Електронне видання*

**Київ**
**2020**

УДК 341.123(045)(0.034.2PDF)

**Організаційний комітет конференції**

***Кудінов С. С***. – співголова, ректор Національної академії Служби безпеки України, доктор юридичних наук, доцент; ***Пилипчук В. Г.*** – співголова, директор Науково-дослідного інституту інформатики і права Національної академії правових наук України, доктор юридичних наук, професор, член-кореспондент Національної академії правових наук України, заслужений діяч науки і техніки України; ***Сафонов Ю. М.*** – співголова, заступник директора з наукової та методичної роботи Інституту модернізації змісту освіти Міністерства освіти і науки України, доктор економічних наук, професор; ***Фальченко С. Л***. – проректор з наукової роботи Національної академії Служби безпеки України, кандидат юридичних наук, доцент; ***Мамченко С. М.*** – директор Навчально-наукового інституту інформаційної безпеки Національної академії Служби безпеки України, доктор педагогічних наук, професор; ***Гребенюк В.М.*** – заступник директора науково-організаційного центру Національної академії Служби безпеки України, доктор юридичних наук; ***Гуз А. М.*** – т. в. о. заступника директора інституту (з навчальної і наукової роботи) Навчально-наукового інституту інформаційної безпеки Національної академії Служби безпеки України, доктор історичних наук, професор; ***Воскобойніков С. В.*** – т. в. о. завідувача кафедри Навчально-наукового інституту інформаційної безпеки Національної академії Служби безпеки України, кандидат педагогічних наук; ***Давидова Т. О.*** – т. в. о. начальника організаційно-наукового відділу науково-організаційного центру Національної академії Служби безпеки України, кандидат юридичних наук

**Актуальні** проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. (Київ, 15 травня 2020 р.). [Електронне видання]. – Київ : НА СБУ, 2020. – 363 с.

У збірнику висвітлюються актуальні проблеми, пов’язані з цифровою трансформацією суспільства та держави; управлінням інформаційною безпекою; розглядаються питання покращання змісту вищої освіти фахівців з інформаційної безпеки держави, а також висвітлюється питання управління інформаційною безпекою держави очима молодих вчених і здобувачів вищої освіти.

Для працівників органів державної влади, науковців, викладачів, фахівців з інформаційної та кібернетичної безпеки, широкої громадськості.

Тези доповідей публікуються в авторській редакції.

Організаційний комітет залишає за собою право не поділяти думку авторів.

**УДК 341.123(045)(0.034.2PDF)**

# ВІТАЛЬНЕ СЛОВО

XI Всеукраїнська науково-практична конференція ***«Актуальні проблеми управління інформаційною безпекою держави»*** вже традиційно присвячена нагальним питанням забезпечення безпеки людини, суспільства і держави в інформаційній сфері.

Про актуальність та значущість заходу свідчить той факт, що вона відбувається за активної участі представників органів державної влади, суб'єктів сектору безпеки і оборони, провідних наукових установ і навчальних закладів та громадських організацій, за сприяння та безпосередньої участі Науково-дослідного інституту інформатики і права Національної академії правових наук України та Інституту модернізації змісту освіти Міністерства освіти і науки України. Цей щорічний, уже одинадцятий, науковий форум переконливо засвідчив, що він є ефективною платформою обміну досвідом та пошуку оптимальних шляхів вирішення найбільш вагомих проблем і завдань управління інформаційною безпекою держави.

Цьогоріч у заході взяли участь представники Верховної Ради України, Міністерства внутрішніх справ України, Державної служби спеціального зв'язку та захисту інформації України, Національного інституту стратегічних досліджень, Інституту проблем реєстрації інформації Національної академії наук України, представники близько двадцяти провідних закладів вищої освіти з різних регіонів України.

В сучасних умовах міжнародного збройного конфлікту та цифрових трансформацій, за оцінками експертів і вчених, до пріоритетних напрямів забезпечення інформаційної та кібернетичної безпеки передусім слід віднести захист національного інформаційного простору від інформаційних та психологічних операцій на шкоду людині і суспільству, запобігання кіберпосяганням на об'єкти критичної інфраструктури держави, захист персональних даних та приватності життя людини в інформаційній сфері.

З урахуванням положень Конституції України щодо європейської і євроатлантичної інтеграції також є актуальною проблема вивчення відповідного досвіду країн-членів ЄС і НАТО та імплементації у національне законодавство положень «Пакету захисту даних» та інших правових актів ЄС з питань інформаційної та кібербезпеки.

Протягом останніх років парадигма інформаційної безпеки нашої держави суттєво змінилася. Насамперед, переосмислено саму природу, а відповідно і стратегічний вимір концепції управління інформаційною безпекою.

Національна академія Служби безпеки України одним із стратегічних пріоритетів своєї діяльності визначила теоретичне та прикладне осмислення актуальних питань управління інформаційною безпекою держави, підтвердженням чого є активна співпраця з провідними вітчизняними

установами і закладами, зокрема, з Національним університетом оборони України імені Івана Черняхівського, Національною академією Державної прикордонної служби України імені Богдана Хмельницького, Національним університетом «Острозька академія», Національним юридичним університетом імені Ярослава Мудрого, Науково-дослідним інститутом інформатики і права та Секцією права національної безпеки і військового права Національної академії правових наук України, іншими.

При цьому, спільно опрацьовувався комплекс проблем щодо викликів і загроз національній безпеці в контексті розвитку інформаційного суспільства та сучасних цифрових трансформацій, формування і реалізації державної політики у сфері інформаційної безпеки, розбудови системи стратегічних комунікацій сектору безпеки і оборони, розвитку національного законодавства у цій сфері та інші актуальні питання інформаційної безпеки людини, суспільства і держави.

Сучасні карантинно-обмежувальні заходи, пов'язані з пандемією та поширенням захворювання коронавірусом COVID-19, наочно засвідчили актуальність вказаних та інших проблем, а також зростання залежності суспільства від стійкого функціонування інформаційно-комунікаційних систем і мереж та виняткову важливість захисту національних інтересів в інформаційній сфері, як складової національної безпеки України.

Тож для майбутнього України вкрай актуальною постає проблема формування і реалізації ефективної державної інформаційної політики і політики забезпечення національної, державної та інформаційної безпеки. Водночас, захист життєво важливих інтересів людини, суспільства й держави від внутрішніх і зовнішніх загроз, державного суверенітету і територіальної цілісності України, забезпечення безпеки критичної інформаційної інфраструктури та розвитку інформаційно-комунікаційних технологій, участь України в міжнародній системі інформаційної безпеки є важливим напрямом діяльності Служби безпеки України і Національної академії Служби безпеки України, низки державних і недержавних органів, установ та організацій.

Ефективне вирішення вказаних та інших питань потребує подальшої наукової розробки та пошуку науково обґрунтованих шляхів їх вирішення. При цьому забезпечення інформаційної безпеки вбачається наразі одним із визначальних напрямів державної політики, від якого залежатиме подальший розвиток суверенної України, її національна безпека та місце у світовому співтоваристві. Саме на розв'язання цих та низки інших нагальних питань інформаційної безпеки зосереджена увага учасників нашої конференції.

***З повагою***
***організаційний комітет конференції***

*УДК 34:004*

**Баранов О. А.**
доктор юридичних наук, с.н.с.,
НДІ інформатики і права НАПрН України

# ЦИФРОВА ТРАНСФОРМАЦІЯ ЯК ДЖЕРЕЛО ПРАВОВИХ ПРОБЛЕМ

Світова цивілізація, як і будь яка динамічна система (біологічна, технічна чи соціальна), розвивається в умовах постійних зовнішніх та внутрішніх впливів різної природи та різноманітних форм. Негативні впливи здатні суттєво погіршувати стан функціонування динамічної системи (ДС) і навіть доводити її до руйнування. Тому базовою умовою існування і розвитку ДС є наявність у неї такої фундаментальної атрибутивної властивості як самозбереження. Самозбереження забезпечується функціонуванням певної підсистеми адаптації ДС. Саме підсистема адаптації задля нейтралізації негативних впливів може ініціювати необхідну реакцію ДС.

Необхідно зауважити, що для забезпечення ефективності самозбереження підсистема адаптації має встигнути ініціювати необхідну реакцію на певний параметр негативного впливу, а ДС – реалізувати цю реакцію раніше ніж відбудеться наступна зміна параметру негативного впливу. Але реальні ДС та їх підсистеми адаптації принципово не можуть виконати зазначену умову тому, що вони мають низку обмежень щодо ініціювання та реалізації вчасної реакції, серед яких головними є: інформаційні, енергетичні, структурні, часові, просторові, ресурсні, організаційні, управлінські та, навіть, інтелектуальні обмеження.

Таким чином, можемо констатувати те, що в будь-який ДС забезпечення функції самозбереження як основи існування і розвитку відбувається в умовах наявності більш чи менш гострого протиріччя між необхідністю вчасно реагувати на негативні впливи та об’єктивним існуванням обмежень для гарантування необхідної якості такого реагування.

Одним з найбільш ефективних шляхів вирішення зазначеного вище протиріччя є трансформація ДС з метою мінімізації або повного уникнення наявних обмежень забезпечення ефективності реагування на негативні впливи.

Отже, ДС та її підсистема адаптації мають бути спроможними виконувати наступні завдання: ідентифікація впливів, подальше спостереження та прогнозування їх розвитку; аналіз наслідків дії впливів на показники функціонування ДС; синтез «пропозицій» щодо вдосконалення ДС, зок-

рема щодо зміни правил поведінки (вдосконалення дотеперішніх або створення нових) задля мінімізації наслідків негативних впливів; формування «пропозицій» щодо шляхів, методів, способів та засобів забезпечення вдосконалення ДС, зокрема, формування вдосконалених правил поведінки; аналіз наслідків негативних впливів на показники функціонування вдосконаленої ДС; за необхідності корекція попередніх «пропозицій» щодо вдосконалення ДС.

В останні роки широко використовується термін «соціальна трансформація», метою якої є забезпечення покращення ефективності (вдосконалення) функціонування суспільства або окремих його частин.

На наш погляд, ***соціальна трансформація*** *це корінне перетворення мети, структури та функцій суспільства або його окремих частин заради адаптації до суттєвих змін внутрішніх та зовнішніх умов, які є загрозою ефективності його подальшого розвитку*.

В той же час, дослідники та експертне середовище вважають, що один з панівних методів соціальної трансформації – це техніко-економічний метод, базовим критерієм якого э ефективність. Історично доведено, що техніко-економічні методи реалізуються через промислові (технологічні) революції, які розуміють як революційні зміни в продуктивних силах суспільства і в організації його діяльності у самому широкому сенсі.

Промислова революція є завжди відповіддю на цивілізаційний виклик, який обумовлено виникненням системного протиріччя між необхідністю забезпечення самозбереження цивілізації та між наявністю цивілізаційних системних обмежень щодо нейтралізації дії негативних впливів, які стають загрозою існуванню самої цивілізації.

На початку XXI століття сформувалася певна система змістовно нових цивілізаційних викликів: виснаження планетних ресурсів; погіршення екології, зміна клімату; надзвичайно високі темпи соціальних процесів; великі обсяги інформації та велика кількість об’єктів та суб’єктів, які є дотичними до певного соціального процесу; обмеженість когнітивних здібностей людини для прийняття рішень адекватних сучасному стану соціальних процесів, внутрішніх та зовнішніх впливів тощо.

Відповіддю стала четверта промислова революція, до досягнень якої відносять: Інтернет речей, Індустрію 4.0, штучний інтелект, робототехніку, великі дані, хмарні обчислювання, нано- та біотехнології, генну інженерію, електронні комунікації тощо. Сумісне застосування цих досягнень створює надпотужний синергетичний ефект підвищення ефективності будь-якої діяльності, різкої економії ресурсів, покращення якості життя людей тощо.

Впровадження зазначених вище досягнень потребує проведення певної соціальної трансформації або в межах окремої країни чи групи країн, або в межах всієї цивілізації тому, що цивілізаційний ефект від нових тех-

нологій збільшується в геометричній прогресії за умови їх різкого масштабування та широкого використання інформаційних комп'ютерних технологій (цифрових технологій).

Тому під терміном ***цифрова трансформація*** *будемо розуміти суспільну трансформацію, яка відбувається завдяки застосуванню Інтернет речей, Індустрії 4.0, штучного інтелекту, робототехніки, великих даних, хмарних обчислювань, нано- та біотехнологій, генної інженерії, електронних комунікацій тощо на базі максимального використання цифрових технологій.*

Соціальна чи цифрова трансформація, призводить до зміни змісту і складу системи суспільних відносин, зміни парадигми функціонування держави, соціуму та його окремих сегментів, переходу до інноваційних бізнес моделей і бізнес мислення тощо, тому все це беззаперечно потребує зміни соціальної моделі суспільства.

Як правило, застосування чинної правової моделі регулювання суспільних відносин до нової соціальної моделі суспільства призводить до виникнення правових проблем. Отже, цифрова (соціальна) трансформація, оскільки вона є джерелом виникнення правових проблем у різних галузях права, має супроводжуватись відповідними змінами законодавства.

Таким чином, до питання виникнення і вирішення будь-яких правових проблем необхідно підходити з системних, інтегральних позицій вивчення мети, завдань та наслідків цифрової (соціальної ) трансформації всього суспільства.

*УДК 34:004*

**Бежевець А. М.**
Національний технічний університет України
«КПІ імені Ігоря Сікорського»

## ЕЛЕКТРОННЕ ПРАВОСУДДЯ ЯК НЕОБХІДНИЙ ЕЛЕМЕНТ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ СУСПІЛЬСТВА ТА ДЕРЖАВИ

Відповідно до статті 129 Конституції України однією із основних засад судочинства є гласність судового процесу та його повне фіксування технічними засобами [1]. Стаття 7 Цивільного процесуального кодексу України визначає, що суд під час розгляду справи в судовому засіданні здійснює повне фіксування його перебігу за допомогою відео- та (або) звукозаписувального технічного засобу [2].

Безумовно, закріплені в законодавстві сучасні засоби здійснення судочинства повинні в першу чергу забезпечити зручність, прозорість, відкритість та доступність правосуддя, а інтеграція інформаційних техноло-

гій в процес здійснення правосуддя має відбуватись з урахуванням принципів верховенства права. Завдяки розвитку і впровадженню нових технологій і сучасних телекомунікаційних засобів стали можливими такі процесуальні дії, як: створення Єдиного Державного реєстру судових рішень, проведення засідань в режимі відеоконференції, аудіо- та відеофіксація судових засідань, транслювання перебігу судового засідання в мережі Інтернет, електронна подача процесуальних документів.

Відповідно до ч. 1, 4, 8 ст. 14 ЦПК України у судах функціонує Єдина судова інформаційно-телекомунікаційна система (далі – ЄСІТС). З її допомогою забезпечується обмін документами в електронній формі між судами, між судом та учасниками судового процесу, між учасниками судового процесу, а також фіксування судового процесу і участь учасників судового процесу у судовому засіданні в режимі відеоконференції. Реєстрація в ЄСІТС не позбавляє права на подання документів до суду в паперовій формі.

Особи, які зареєстрували офіційні електронні адреси в ЄСІТС, можуть подати процесуальні, інші документи, вчинити інші процесуальні дії в електронній формі виключно за допомогою ЄСІТС з використанням власного електронного цифрового підпису, прирівняного до власноручного підпису відповідно до Закону України «Про електронний цифровий підпис» [2].

Відповідно до наказу Державної судової адміністрації України від 22.12.2018 № 628 «Про проведення тестування підсистеми «Електронний суд» у місцевих та апеляційних судах» [3] з 22.12.2018 у місцевих та апеляційних судах розпочалась експлуатація підсистеми «Електронний суд» в тестовому режимі. Вона дозволяє подавати учасникам судового процесу до суду документи в електронному вигляді, а також надсилати таким учасникам процесуальні документи в електронному вигляді, паралельно з документами у паперовому вигляді відповідно до процесуального законодавства.

Право доступу до електронних документів, які надійшли на адресу суду, надається суддям, у провадженні яких перебувають відповідні судові справи.

Однак, на теперішній час підсистема «Електронний суд» працює лише в тестовому режимі та не передбачає технічної можливості судів здійснювати розгляд даної справи в електронній формі.

Крім цього, при прийнятті Закону України «Про електронні довірчі послуги» (05 жовтня 2017 року) Закон України «Про електронний цифровий підпис» визнано таким, що втратив чинність. Проте до сьогодні законодавець «забув» внести відповідні зміни до Цивільного процесуального кодексу.

Отже, через посилання у статтях 14 та 100 ЦПК України на нормативно-правовий акт, що втратив чинність, а також відсутність відповідних процесуальних норм та технічної можливості судів здійснювати розгляд справи в електронній формі, існує певна правова колізія, яка не дає можливості повноцінно функціонувати електронному суду та проводити електронні засідання.

Досліджуючи зарубіжний досвід впровадження електронного правосуддя, слід проаналізувати вже існуючі механізми створення та функціонування електронних судів та використання ними електронних доказів (в т.ч. створених з використанням блокчейн технологій) на прикладі Китайської Народної Республіки (далі – КНР), де вже декілька років функціонують три інтернет-суди в Ханчжоу, Пекині та Гуанчжоу.

Визначено, що інтернет-судам підсудні спори, пов'язані з: онлайн-продажем товарів і послуг, кредитуванням, авторським правом і суміжними правами, порушенням особистих немайнових прав та/або майнових прав через Інтернет, прав на доменні імена тощо.

Процес судового розгляду здійснюється виключно в режимі онлайн, включаючи обслуговування юридичних документів, подання доказів. Електронні докази можуть бути засвідчені за допомогою електронного підпису, перевірки хеш-значення, блокчейна. Інтернет-суди визнають законність блокчейн як способу зберігання і аутентифікації цифрових доказів, за умови, що сторони можуть довести законність технології, що використовується в процесі.

Інтернет-суди мають спеціальну платформу для розгляду справ. Сторони судового процесу повинні пройти аутентифікацію особистості за допомогою онлайн-аутентифікації і отримати спеціальний обліковий запис для використання онлайн-платформи судових розглядів.

Інтернет-суди використовують платформу для ведення електронних архівів одночасно зі справою. Таким чином, паперові архіви справ повністю перетворені в електронні архіви.

На підставі викладеного автор приходить до висновку, що на даному етапі реформування судової системи України є всі технічні і технологічні можливості для впровадження інформаційних технологій в процес здійснення правосуддя. Практика впровадження інтернет-судів в КНР показала реальний стан речей. Впровадження в судову систему інтернет-правосуддя підвищить ефективність захисту прав громадян, знизить судові витрати, вирішить проблему низької ефективності судових органів, сприятиме побудові системи соціальної довіри до судів.

**Література**

1. https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.
2. https://zakon.rada.gov.ua/laws/show/1618-15.
3. https://dsa.court.gov.ua/userfiles/media/628_18.pdf.

*УДК 004.056:5:378.1(045)*
**Бровко В. Д.**
кандидат технічних наук,
**Скубак О. М.**
кандидат технічних наук, доцент,
Національна академія СБ України

# СИСТЕМНИЙ АНАЛІЗ ІНФОКОМУНІКАЦІЙ

Інфокомунікація являється об'єднанням понять інформатизація та телекомунікації, при цьому останні розглядаються носіями не буденної, а важливої інформації, в одному ряду та є єдиним блоком збереження обробки та передачі інформації при виконанні цих двох функцій.

Таким чином, інфокомунікаційну систему можна розглядати як об'єднання двох важливих елементів телекомунікаційної інфраструктури та інформаційної системи. При цьому важко відокремити приорітетність кожної з них – вони обидві важливі.

Сучасні інфокомунікації надають користувачам багато зручностей, і разом з тим існуючі в них проблеми потребують використання різних методів їх розв'язання, в тому числі в першу чергу методів системного аналізу.

Що являє собою системний аналіз? Навіть серед спеціалістів, на жаль, немає одностайності в його означенні. Згідно «Вікіпедії» [1] «Системний аналіз – науковий метод пізнання, який представляє собою послідовність дій по встановленню структурних зв'язків між змінними або елементами системи, яку досліджуємо».

Суть системного аналізу полягає в використанні різноманітних процедур [2]:

– абстрагування і конкретизацію;
– аналіз і синтез, індукцію і дедукцію;
– формалізацію і конкретизацію;
– композицію і декомпозицію;
– лінеаризацію та виділення нелінійних складових;
– структуризацію і реконструктуризацію;
– реінжиніринг;
– моделювання та експеримент та інші.

Класифікація задач системного аналізу можна провести виходячи із різних принципів (складності, приналежності до галузі, методам розв'язання та тому подібного). Для галузі телекомунікації та інформатизації найбільш актуальними являються наступні класи задач:

– задачі розподілу ресурсів;
– задачі по управлінню запасами;
– задачі вибору маршруту та інші.

Окремий клас задач системного аналізу – оптимізація економічних параметрів систем.

Способи розв'язання задач шляхом дослідження операцій включає в себе:

– метод лінійного програмування (усі елементи моделі (або змінні) пов'язані між собою лінійною залежністю);

– метод нелінійного програмування – хоча б один зв'язок являється нелінійним;

– метод динамічного програмування (розв'язання задачі розбивається на етапи і на кожному наступному етапі використовуються результати попереднього);

– метод теорії масового обслуговування (моделі систем обслуговування, в яких запит на обслуговування надходить в випадкові моменти часу);

– методи теорії управління запасами, розв'язання яких забезпечує мінімальні сумарні затрати;

– методи теорії графів, в тому числі мережеве планування.

Звичайно, це не вичерпний список, але саме ці методи найбільш часто використовуються в галузі телекомунікацій та інформатизації.

Процедура прийняття рішень являється втіленням системного аналізу, його основним змістом і включає в себе формулювання проблемної ситуації, визначення цілі, пошук оптимального розв'язку, побудову моделей для обґрунтування розв'язків, реалізацію розв'язку.

Системний аналіз цілком прийнятний для вирішення задач галузі телекомунікацій та інформатизації. Його використання дозволяє досить успішно вирішувати проблеми пов'язані з забезпеченням зростання пропускної здатності каналів та трактів систем зв'язку, оптимізацію структури мереж, ефективного використання ресурсів мереж та інформаційних систем.

**Література**

1. Системный анализ. Википедия http://ru.wikipedia.org/wiki/

2. Дж. Мартин. Системный анализ передачи данных. Москва. Изд-во «Мир»,1975.

*УДК 323.28*

**Гельжинський А. Ю.**
Служба безпеки України

## ЦИФРОВА ВЗАЄМОДІЯ СУСПІЛЬСТВА ТА ДЕРЖАВИ У СФЕРІ ПРОТИДІЇ ТЕРОРИЗМУ

Все активнішим стає обговорення про реалізацію ідеї цифрової держави, «держави в смартфоні», основною метою якої є підвищення ефекти-

вності взаємодії громадян та держави завдяки ІТ-технологіям. Основними принципами цифрової держави є відкритість та зручність взаємодії людини з державними органами і надання інформації у зрозумілому вигляді, а також безпека і конфіденційність такої взаємодії. Ідея держави в смартфоні полягає у спрощеному та прискореному обміну інформацією людини з державою, зробивши цей процес електронним та автоматичним.

У зв'язку з цим, розвинуті держави намагаються якомога швидше реалізувати зазначену ідею щодо цифрової держави у різних сферах життя: медицина, освіта, фінанси та ін. Однак, в цьому напрямку для держави залишається пріоритетним завданням це забезпечення безпеки суспільства та кожного громадянина.

Після терактів у січні та листопаді 2015 року у Франції на вимогу Прем'єр-міністра Франції Міністерством внутрішніх справ та Інформаційною службою уряду був розроблений мобільний додаток SAIP (*Système d'alerte et d'information des population),* система тривожного оповіщення та інформування населення [1].

Уряд запустив зазначений додаток 8 червня 2016 року перед Чемпіонатом Європи з футболу, який проходив у Франції. «SAIP» став частиною заходів пов'язаних з розвитком культури безпеки суспільства та захисту громадян. Урядовий додаток мав на меті відправляти зареєстрованим користувачам миттєві повідомлення у вигляді попереджень, порад та іншої інформації на телефони у випадку вибуху, теракту чи іншої небезпечної ситуації, враховуючи їх місцезнаходження.

Щоб отримати оповіщення в районі, де виявлена загроза теракту, користувачам пропонувалося визначити свою геолокацію, в залежності від якої надсилались відповідні практичні вказівки.

Додаток також дозволяв користувачам, навіть без визначення свого місцезнаходження, отримувати оповіщення про небезпечні ситуації у визначених заздалегідь користувачем географічних районах [2].

Щоб негайно привернути увагу користувача додатку, оповіщення про загрозу супроводжувалося звуком сирени. Відкривши мобільний додаток «SAIP», користувач отримував інформацію про наявність загрози та інструкції із заходів безпеки. Крім цього, з метою попередження та мінімізації ризиків для оточуючих користувач міг поширити зазначену інформацію через соціальні мережі «Twitter» та «Facebook».

Однак, у 2018 році французький уряд не продовжив контракт з розробником додатку через певні технічні несправності. У зв'язку з тим що, 14 липня 2016 року під час терористичних атак у Ніцці, повідомлення користувачам додатку почали надходити через 2 години після закінчення атаки. Іноді, повідомлення відправлялись без зазначення місця джерела загрози. Крім цього, в ході навчальної тривоги повідомлення надходили у вигляді реальної терористичної загрози [3].

Урядом Франції прийнято рішення створити в соціальній мережі «Twitter» відповідний обліковий запис для оповіщення подій, що впливають на безпеку суспільства та держави. Крім цього, Міністерство внутрішніх справ вирішило використовувати вже наявні інструменти «Facebook» та «Google» для поширення повідомлень [4].

Водночас, варто відмітити позитивний досвід Сінгапуру, уряд якого розпочав активно вести політику щодо захисту своїх громадян від терористичної загрози після терактів 11 вересня 2001 року у Нью-Йорку, а також підривів у Сінгапурі посольств США, Великої Британії та Ізраїлю.

У Сінгапурі успішно ведеться кампанія «Будьте насторожі – будьте об'єднаними – будьте сильними». Зазначена програма передбачає надання інструкцій для громадян у випадку загроз терористичного характеру *(вибух, захоплення заручників, застосування радіологічної, хімічної, біологічної та ядерної зброї та ін.)*.

Для громадян Сінгапуру пропонується мобільний додаток «SGSecure», завданням якого є навчання та мобілізація громадян з метою попередження та протидії тероризму. За допомогою вказаного додатку є можливість отримання повідомлення про загрозу терористичного характеру, надання правоохоронним органам інформації про підозрілу активність чи поведінку особи, яка може свідчити про загрозу вчинення нею теракту, спрощений режим звернення до правоохоронних органів *(телефонний дзвінок, СМС-повідомлення, режим тривожного оповіщення через мобільний додаток)*. Крім цього, у мобільному додатку містяться інструкції щодо надання першої медичної допомоги у разі вчинення теракту [5].

Уряд Сінгапуру рекомендує керівникам підприємств, громадських організацій, релігійних общин уповноважити своїх представників для реалізації програми «SGSecure» на місцях. На вказаних осіб покладено здійснювати контроль наявності мобільного додатку та його функціонування у представників організації, виконання рекомендацій уряду щодо реагування на терористичну загрозу та забезпечення заходів безпеки на місцях, а також розробка планів реагування на випадок терористичної загрози.

Враховуючи події в Україні, які мають місце протягом останніх 6 років – збройна агресія на території Донецької та Луганської областей, пожежі внаслідок диверсій на військових складах, постійні повідомлення про замінування державних закладів, будівель транспортної інфраструктури, ТРЦ та ін., схиляє нас до думки щодо необхідності розробки державної програми захисту громадян від таких загроз та відповідного мобільного додатку, який міг би забезпечити громадян необхідною інформацією та інструкціями у випадку перерахованих вище ситуацій, а також терористичної загрози.

**Література**

1. Brochure «Faire face ensemble. Vigilance, prevention et protection face a la menace terroriste», edition decembre 2016, pages 1-76. Secretariat general de la defense et de la securite nationale;

2. Офіційний сайт Міністерства внутрішніх справ Франції [Електронний ресурс]. – Режим доступу: https://www.interieur.gouv.fr/Alerte/Alerte-ORSEC/Qu-est-ce-que-le-SAIP;

3. Angelique Chrisafis. «France's Saip emergency smartphone app failed during Nice attack». The Guardian, 16 Jul. 2016. [Електронний ресурс]. – Режим доступу: https://www.theguardian.com/world/2016/jul/16/nice-terroist-attack-france-saip-emergency-smartphone-app-failed;

4. Lisa Korrigane. «SAIP, the French alert app, shuts down». Rude Baguette, 01 Jun. 2016. [Електронний ресурс]. – Режим доступу: https://www.rudebaguette.com/en/2018/06/saip-the-french-alert-app-shuts-down;

5. Офіційний сайт Міністерства внутрішніх справ Сінгапуру [Електронний ресурс]. – Режим доступу: https://www.sgsecure.sg/.

*УДК 342.951*

**Гончаренко Г. А.**
кандидат юридичних наук, доцент,
Інститут підготовки юридичних
кадрів для Служби безпеки України
Національного юридичного
університету імені Ярослава Мудрого

## ДОСВІД КРАЇН-ЧЛЕНІВ ЄС ЩОДО НІВЕЛЮВАННЯ СУЧАСНИХ ЗАГРОЗ ВІД ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

Стрімкий розвиток цифрової трансформації суспільства в реаліях сьогодення перестає бути лише економічною складовою, а стає одним з тих чинників, які вже сьогодні впливають, а в невдовзі стануть визначними напрямками в питаннях забезпечення безпеки як громадян, так і самої країни.

Щодо необхідності винесення цієї теми як реальної проблеми, що може вплинути на стан забезпечення безпеки держав та взагалі бути загрозою національним сувенітетам, наголошували учасники 56-ї MSC (Munich Security Conference/ Münchner Sicherheitskonferenz/ Мюнхенської конференції з безпеки), що пройшла у лютому 2020 року.

В підсумковому документі, Мюнхенському звіті про безпеку 2020, де проаналізовано поточні події політики безпеки в Китаї, Європі, Росії та США, а також розкрито розуміння тем космічної та кліматичної безпеки тощо, окремо виділені загрози, які створюють нові технології.

Так, зазначається, що, дискусія навколо технологій рідко – якщо взагалі – була настільки тісно пов'язана з обговоренням суверенітету національних держав, як сьогодні. В цьому ж аспекті, зазначено наступне. «Президент Франції Макрон зрозумів це минулого року, що технологія вже не сприймається як політично нейтральна: «Битва, з якою ми боремося, – це один із суверенітетів […]. Якщо ми не створимо власних чемпіонів у всіх сферах – цифрових, штучний інтелект – наш вибір буде продиктований іншими» [1]. Саме на цьому тлі Європа зі своєю історично сильною промисловою базою, бачить своєму економічному становищу дедалі більше викликів від інших світових держав [2]. США займають лідируючі позиції у багатьох галузях технологій, а Китай активізується. Це очевидний підйом китайських технологічних гігантів, таких як Huawei, Alibaba, і Xiaomi. Головний виклик для Європи полягає в її структурних недоліках по відношенню до Китаю та США, його фрагментарні ринки, включаючи ринки капіталу та управління стоять на шляху швидкого масштабування [3].

Шукаючи шляхи вирішення безпекових питань в інформаційній сфері та ефективного забезпечення європейської цифрової системи, учасники 56-ї MSC знайшли напрям для потенційно можливого вирішення цієї проблеми. Так, інновації з установкою «внаслідок чого різноманітні зацікавлені сторони Європи об'єднуються навколо спільної, конкретної та амбітної мети співпраці, в масштабі, може стати потенційним рішенням». Такі великі, амбітні місії Майбутнього можуть сприяти співпраці державно-приватного співробітництва для стимулювання інновацій. Сектор безпеки, оборони та космічного простору в Європі пропонує реальні та конкретні можливості для створення таких місій сьогодні. Як приклад, побудова «цифрового Галілея» (Galileo) – глобальної супутникової навігаційної системи ЄС для забезпечення європейської цифрової системи – цілеспрямований суверенітет і незалежність, що можуть потенційно розв'язати подібні об'єднавчі зусилля. Якби Європа скористалася цим шансом, це також продемонструвало б, що європейське співробітництво може принести відчутні перемоги в умовах швидкого розвитку технологічних змін [3].

Розглянемо, так чому ж країни-члени ЄС покладають такі сподівання щодо безпеки як на рівні людини-громадянина, так і на рівні державної безпеки, побудові «цифрового Галілея».

Galileo – це глобальна супутникова система навігації (GNSS) в Європі, що забезпечує покращену інформацію про позицію (розстановку) та хронометраж, і має значні позитивні наслідки для багатьох європейських служб та користувачів. Наприклад: (1) Galileo дозволяє користувачам знати їх точне положення з більшою точністю, ніж те, що пропонують інші доступні системи; (2) критичні, служби реагування на надзвичайні ситуації отримують надійність від системи Galileo; (3) продукти, якими користуються

люди щодня, від навігаційного пристрою у своєму автомобілі до мобільного телефону, наділені підвищеною точністю, яку забезпечує Galileo; (4) послуги Galileo зроблять європейські дороги та залізниці більш безпечними та ефективними; (5) це стимулює європейські інновації, сприяючи створенню багатьох нових продуктів та послуг, створюючи робочі місця тощо [4].

Питання запуску системи Galileo повною мірою пов'язане було з необхідністю забезпечення безпекових питань, навіть у окремих джерелах йдеться про те, що «основною метою програми Galileo є європейська незалежність».

Досі користувачі GNSS повинні були залежати від нецивільних американських GPS або російських сигналів GLONASS. З Galileo зараз користувачі мають нову надійну альтернативу, яка, на відміну від цих інших програм, залишається під цивільним контролем. Крім того, Galileo забезпечує європейським громадянам незалежність та суверенітет, низку екологічних переваг та декілька нових послуг, характерних для програми Galileo (Відкрита служба, Комерційна служба, Пошук та Рятування) [4].

Досвід пошуку ефективних шляхів нівелювання загроз, пов'язаних з цифровою трансформацією суспільства, саме з боку Європейського Союзу, беззаперечно, вартий розгляду та врахування в рамках пошуку шляхів забезпечення інформаційної безпеки нашої країни, в тому числі, враховуючи конституційно закріплений напрям України до членства в ЄС.

**Література**

1. «Macron Throws €5 Billion at Digital Start-ups,» 18 September 2019, http://www.rfi.fr/en/france/20190918-macron-throws-5-billion-digitl-startups.

2. Alan Beattie, «Technology: How the US, EU and China Compete to Set Industry Standards,» Financial Times, 24 July 2019, https://www.ft.com/content/0c91b884-92bb-11e9-aea1-2b1d33ac3271.

3. Munich Security Report 2020, https://securityconference.org/publikationen/munich-security-report-2020/.

4. Galileo is the European global satellite-based navigation system, https://www.gsa.europa.eu/european-gnss/galileo/galileo-european-global-satellite-based-navigation-system.

*УДК 343.102*
**Гриненко С. О.**
кандидат юридичних наук,
Інститут підготовки юридичних
кадрів для Служби безпеки України
Національного юридичного
університету імені Ярослава Мудрого

# ДО ПИТАННЯ ІНТЕГРАЦІЇ АНАЛІТИЧНОЇ, ОПЕРАТИВНОЇ ТА СЛІДЧОЇ РОБОТИ В СБУ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ СУСПІЛЬСТВА

Ми живемо в епоху інформаційного суспільства – новій історичній фазі розвитку цивілізації, в якій інформація та знання із засобів діяльності перетворилися на головні продукти виробництва. Ця обставина зумовлює розробку і необхідність впровадження інформаційних технологій, володіння якими дозволяє вивести роботу з інформацією на новий, вищий рівень. Нажаль Україна у цьому відношенні на сьогодні значно відстає від розвинутих (у тому числі з точки зору рівня впровадження інноваційних технологій) країн світу, що значно знижує здатність нашої держави гідно конкурувати й ефективно взаємодіяти як у бізнесовій сфері, так і у сфері забезпечення національної безпеки.

Спеціальним суб'єктом, який забезпечує державну безпеку України, є Служба безпеки України. Від її ефективної діяльності, спрямованої насамперед на попередження, своєчасне виявлення і запобігання зовнішнім та внутрішнім загрозам безпеці України, розвідувальним, терористичним та іншим протиправним посяганням спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на інтереси України, значною мірою залежить стабільність і спокій у державі, її суверенність.

Однією з основних функцій будь-якої спецслужби є інформаційно-аналітична робота в інтересах ефективного проведення органами державної влади та управління внутрішньої і зовнішньої діяльності, вирішення проблем оборони, соціально-економічного будівництва, науково-технічного прогресу, екології та інших питань, пов'язаних з національною безпекою України. У той же час, потужне інформаційно-аналітичне забезпечення є необхідною умовою ефективної роботи і самої спецслужби, її оперативних і слідчих підрозділів.

У структурі Служби діють спеціальні інформаційно-аналітичні підрозділи, для яких обробка інформації є основною функцією. Крім того, практично кожний співробітник на своїй ланці здійснює аналітичні функції. З огляду на відповідальність завдань, поставлених перед Службою безпеки України, якість виробленої інформації і достовірність отриманих на її основі знань є однією з найважливіших умов її ефективної діяльності.

Велика кількість джерел інформації, постійно зростаючі її обсяги, швидкість оновлення та передачі значно ускладнюють завдання її якісної обробки: систематизації, аналізу і узагальнення, інтерпретації і формування на її основі достатньо вірогідних прогнозів. Обсяг інформаційних потоків на сьогодні дозволяє впевнено говорити про недостатність для якісної інформаційно-аналітичної роботи лише загальної ерудиції, здорового глузду, знання законів логіки та життєвого досвіду.

Для належного виконання цієї роботи необхідним є використання новітніх, передових технологій пошуку і обробки інформації, оволодіння якими можливе лише за умови цілеспрямованої фахової підготовки спеціалістів у галузі інформаційно-аналітичної діяльності, цифрової криміналістики, кібернетичної безпеки тощо.

Крім того, виявлення протиправних діянь, їх документування, розкриття і розслідування необхідна тісна співпраця фахівців різного профілю у межах виконання одного завдання. Для повноцінного виконання завдань пошуку і опрацювання різноманітної інформації серед величезної кількості джерел, її аналітичної обробки та формування інформаційного продукту, придатного для використання в інтересах конкретного кримінального провадження і оперативної справи, на наш погляд, сьогодні недостатньо ресурсів і знань самого слідчого чи оперативного працівника, який би рівень фахової підготовки вони не мали.

Отже назрілим є питання впровадження організації слідчої і оперативної роботи у форматі хабу, в якому робота щодо конкретного прояву протиправної діяльності, віднесеного до компетенції СБ України, велася б «командою» декількох співробітників під єдиним керівництвом, кожен з яких виконує свій специфічний сегмент роботи, але всі вони відповідають за спільний результат: оперативний працівник відповідає за роботу з негласним апаратом, оперативне забезпечення; слідчий планує і реалізовує процесуальні заходи отримання і фіксації доказів; аналітик працює з базами даних, постачає необхідну інформацію та забезпечує прогнозну функцію.

*УДК 34.03:008.2*
**Доронін І. М.**
кандидат юридичних наук, доцент,
НДІ інформатики і права НАПрН України

## ЦИФРОВІЗАЦІЯ І ПЕРСПЕКТИВИ ДЛЯ ПРАВА

Останнім часом в соціальних науках запропоновано нове розуміння етапу розвитку людства, що характеризує сьогоднішній стан, під загаль-

ним найменуванням «інформаційної епохи». Інформаційна епоха хронологічно розглядається як постіндустріальний етап, у якому значення інформаційних технологій для людства є особливим. У межах розгляду інформаційної епохи доволі умовно (внаслідок відсутності чітких хронологічних меж для складових) можливо вести мову про:

– *«комп'ютерну епоху»* (яка характеризується виникненням та широким залученням персональних – стаціонарних та переносних індивідуальних або персональних засобів обробки інформації);

– *«мережеву епоху»* (основними рисами її є глобальне панування різних мереж, що постійно об'єднують засоби обробки інформації зі створенням відповідних спеціальних програм для постійного спілкування людей);

– *«цифрову» епоху»* (період, що характеризується відмовою від паперових носіїв інформації взагалі).

Таким чином, цифрова епоха, що вважається складовою епохи інформаційної, знаменує істотні трансформаційні зміни у суспільстві. Особливо це стосується його регуляції та перспектив подальшого розвитку. У загальному вигляді можливо розглядати наступні основні риси зазначеної цифрової епохи:

– лавиноподібне розповсюдження усіх соціальних комунікацій, що пов'язані із використанням глобальних комп'ютерних мережах (на відміну від історично традиційних об'єднань людей та подібних соціальних інститутів, що не булі зумовленими технологіями);

– скасування паперу та інших подібних («твердих» та «індивідуальних») технологій зберігання інформації як інформаційної основи;

– максимальне пришвидшення обміну інформації, а також пов'язані з цим явища – штучний інтелект, пряма комунікація між технічними пристроями з обмеженим втручанням людини, розвиток новітніх інформаційних технологій у різних сферах, який зумовлюється самими технологіями.

Останні два роки внаслідок уведення до публіцистичного обороту похідного терміну «диджиталізація» (повна англомовна калька слова «цифровізація», що також є штучним конструктом), на рівні документів державної політики здійснюється активне переосмислення процесів супроводження розвитку окремих технологій та їх державного супроводження. Загалом, термінологічно «цифровізація», як явище і процес, визначена на рівні нормативно-правових актів.

Так, розпорядженням Кабінету Міністрів України від 17.01.2018 № 67-р схвалено Концепцію розвитку цифрової економіки та суспільства на 2018-2020 роки. Метою Концепції фактично є «впровадження відповідних стимулів для цифровізації економіки, суспільної та соціальної сфер, усвідомлення наявних викликів та інструментів розвитку цифрових інфраструктур, набуття громадянами цифрових компетенцій, а також визначає

критичні сфери та проекти цифровізації, стимулювання внутрішнього ринку виробництва, використання та споживання цифрових технологій». Значення терміну «цифровізація» наведено у тій же Концепції як «насичення фізичного світу електронно-цифровими пристроями, засобами, системами та налагодження електронно-комунікаційного обміну між ними, що фактично уможливлює інтегральну взаємодію віртуального та фізичного, тобто створює кіберфізичний простір».

Надані у тексті Концепції дефініції дозволяють у загальних рисах розуміти соціальне явище, хоча і не є досконалими.

Оскільки право є універсальним регулятором суспільних відносини, то можливо визначити низку загальних перспектив для нього за таких умов.

На нашу думку подальший розвиток права буде відбуватись за умови необхідності вирішення наступних основних проблем:

1) Виникнення та розвиток технологій забезпечення примусу, зокрема, внаслідок реалізації різних варіантів «смарт-контрактів», означає, що виконання буде забезпечуватись автоматично за настання заздалегідь визначених умов, при цьому існує значний потенціал для розвитку технології за межі лише угод.

2) Технологічне забезпечення примусу до виконання зобов'язань може поставити під сумнів питання тлумачення права, оскільки програмний код має технічно описувати і встановлювати межі поведінки.

3) Технічні засоби за відсутності так званих «твердих» засобів фіксації вже призвели до виникнення та розвитку технологій засвідчення фактів та «вічних» реєстрів і записів у них, що має як позитивні так і негативні моменти.

4) Проблема виникнення технологічних засобів засвідчення ставить під сумнів усі традиційні концепції юридичних доказів, оскільки засвідчення факту відбувається технологічно.

5) Ідентифікаційна проблема набуває особливої ваги, оскільки традиційне право, виробивши певні ознаки правосуб'єктності для фізичних і юридичних осіб, потребуватиме нових механізмів як у випадку фізичної особи (у контексті співвідношення особи і «аккаунта» або «технологічної персони») так і новітніх правових реалій на кшталт децентралізованих автономних організацій, що не підпадають під традиційні корпорації.

*УДК 004.056*
**Козюра В. Д.**
кандидат технічних наук, доцент,
Національна академія Служби безпеки України
**Бровко В. Д.**
кандидат технічних наук,
Національна академія Служби безпеки України

# СТРАТЕГІЇ ПОБУДОВИ IDS В СИСТЕМАХ, ЩО ВИКОРИСТОВУЮТЬ ХМАРНІ ТЕХНОЛОГІЇ

У зв'язку з постійним збільшенням кількості шкідливих атак на мобільні пристрої виникла необхідність розробки і впровадження ефективних контрзаходів. Основним механізмом захисту від будь-яких загроз безпеці мобільних пристроїв (конфіденційності, цілісності і доступності) є використання IDS (Intrusion Detection System – система виявлення вторгнень). Потрібно мати на увазі, що реалізація IDS для мобільних пристроїв є складним завданням через обмежені енергетичних і обчислювальних ресурсів останніх. На сьогоднішній день існує чотири основних типи стратегій побудови IDS для мобільних пристроїв:

1. Система виявлення вторгнень на основі сигнатур заснована на вилученні сигнатур поведінкових патернів, отриманих з аналізу поведінки відомих шкідливих програм. Ці сигнатури порівнюються з сигнатурами нових вторгнень. Приклад, багаторівневий детектор аномалій для Android (MADAM – Multilevel Anomaly Detector for Android Malware), що моніторить системні виклики, SMS, критичні API, активність користувачів і метадані застосувань. Після виявлення певних поведінкових патернів MADAM перехоплює і блокує шкідливі програми, застосовуючи всі заздалегідь певні процедури для користувача і пристрою.

2. Система виявлення вторгнень на основі аномалій не вимагає побудови сигнатур для виявлення вторгнень і дозволяє ідентифікувати невідомі атаки. Підхід до виявлення аномалій заснований на побудові моделі нормального поведінку системи. Будь-яке відхилення від цієї моделі вважається аномальним і свідчить про вторгнення шкідливого ПЗ. При виявленні мобільних шкідливих програм використовуються статистичні підходи, методи інтелектуального аналізу даних і методи машинного навчання.

3. Хмарна система виявлення вторгнень виявляє підозру поведінку або шкідливу активність на смартфонах і планшетах шляхом встановлення невеликої за обсягом пам'яті програми-агента на мобільні пристрої і їх реєстрації в онлайн-хмарному сервісі (вказується інформація про ОС, використовувані застосування та інша відповідна інформація про пристрій).

Далі в хмарі в віртуальній машині емулюється мобільний пристрій за допомогою проксі, який в свою чергу дублює вхідний трафік на пристрії, а потім перенаправляє трафік на платформу емуляції (місце виявлення вторгнення). Агент, встановлений на зареєстрованому пристрої користувача, перевіряє всю файлову активність системи. Всякий раз, коли користувач виконує будь-які дії щодо передачі даних, агент перенаправляє трафік в хмару через проксі-сервер. Ця процедура дозволяє виконувати кілька механізмів виявлення паралельно, розміщуючи їх на імітованому пристрої.

4. Ручний аналіз виконується професійним аудитором для виявлення мобільних шкідливих програм на сервері, що надає хмарні послуги. Цей метод вважається повільним, крім того він неточний, що веде до безлічі помилкових спрацьовувань. Сучасні шкідливі програми використовують складні методи маскування, щоб уникнути стратегій виявлення. Потрібно чимало часу, щоб накопичити необхідний досвід для виконання такого роду роботи.

Для захисту від вторгнень самих хмарних систем, проектуються власні IDS:

1. Мережеві IDS засновані на захопленні мережевого трафіку і його аналізі для виявлення будь-яких потенційних вторгнень (DoS-атаки, сканування портів, ботнети тощо). Усередині мережі для ідентифікації вторгнень використовується сигнатурний підхід (порівняння зібраної інформації з базою даних сигнатур) або підхід на основі аномалій (порівняння поточного поведінки системи з моделлю нормальним поведінки).

2. IDS на базі хоста (HIDS – Host-based intrusion detection System) заснована на зборі інформації від підключених хостів і аналізі їх для виявлення шкідливих дій. Зібрана інформація може бути файлом системного журналу, структурами даних ОС, запущеними процесами, доступом до файлів і їх модифікацією, конфігурацією системи і додатків або системними викликами. Така ідентифікація використовується для захисту цілісності системи хмарних обчислень.

3. IDS на основі гипервизора (гипервизор – програмний компонент, що відповідає за спільне використання ресурсів віртуальних машин в системі хмарних обчислень). Атаки, запущені на рівні гипервизора, ведуть до порушення нормальної роботи хмарної інфраструктури, що вимагає пошуку ефективних стратегій захисту. Архітектура такої системи включає блок управління, сервер VMIDPS, ядро IDPS і гипервизор (рис. 1).

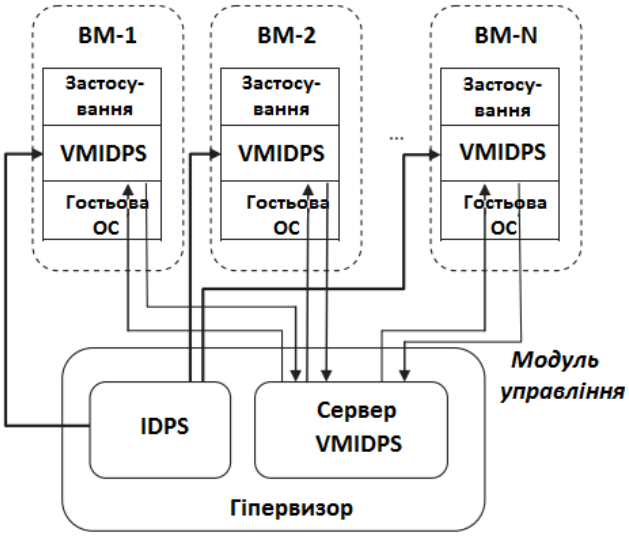


Рис. 1

VMIDPS відповідає за сканування всієї віртуальної машини, щоб переконатися, що система знаходиться в безпечному і неінфікованій стані. Віртуальні машини можуть дати дозвіл на виконання функції тільки в тому випадку, якщо вона підтверджена як безпечна (надійна) системна функція; в іншому випадку VMIDPS викличе сигнал тривоги, щоб вживати відповідні заходи, щоб повернути віртуальну машину в нормальний стан. VMIDPS інтегрує різні методи вторгнення, такі як перевірка цілісності файлів, виявлення вторгнень на основі сигнатур і на основі аномалій.

4. Розподілена IDS для хмарних обчислювальних систем заснована на розгортанні IDS по мережі для перевірки трафіку на наявність інтрузівної поведінки. Кожен IDS включає два компоненти: виявлення вторгнення і менеджера кореляції. Компонент виявлення відповідає за перевірку поведінки системи і відправку зібраних даних після подання їх в стандартному форматі менеджеру кореляції. Менеджер кореляції, в свою чергу, збирає дані з різних IDS і видає високорівневі оповіщення, які стимулюють реакцію на атаку. На аналізу використовуються сигнатурні методи і методи виявлення аномалій для реагування на відомі і невідомі атаки.

**Висновки**

1. Хмарні обчислення і мобільні пристрої – це дві сучасні технології, які спрямовані на те, щоб зробити життя людей простіше і зручніше. Забезпечення безпеки в цих двох середовищах – одна з основних задач проектування систем виявлення вторгнень (IDS).

2. Розробники систем виявлення вторгнень повинні продовжувати розробляти методи, оскільки атаки на обчислювальні системи стають все більш витонченими. IDS шукають вторгнення, і вторгнення використовують методи ухилення, щоб уникнути виявлення IDS. Таким чином, це можна вважати гонкою озброєнь між розробниками шкідливих програм / вторгнень і розробниками виявлення вторгнень.

*УДК 004.056*
**Козюра В. Д.**
кандидат технічних наук, доцент,
Національна академія Служби безпеки України
**Решетніков О. В.**
Національна академія Служби безпеки України

# КІБЕРАТАКИ НА ХМАРНІ ТЕХНОЛОГІЇ

За оцінками фахівців число користувачів мобільних комп'ютерних систем (смартфонів и планшетів) в світі к 2020 року досягло близько 6 млрд. Люди використовують гаджети для ведення бізнесу, спілкування, організації свого приватного життя, навчання, документування, онлайн-банкінгу та багатьох інших цілей. Крім того, нові мобільні пристрої відрізняються простотою використання, що робить можливими нові способи обробки даних. В результаті великі провайдери інтернет-послуг виявили, що хороший спосіб збільшити прибуток полягає в наданні ресурсів потужних обчислювальних систем користувачам, що використовують віртуальні машини. Ця технологія називається хмарними обчисленнями. Технологія віртуалізації надає можливість спільного використання апаратних ресурсів для запуску ізольованих гостьових операційних систем (ГОС), а також дозволяє мільйонам користувачів зберігати свої дані за допомогою додатків, що надаються хмарною системою. Корисність хмари полягає в її здатності зберігати багато інформації і робити її доступною для мобільних пристроїв на вимогу. Таким чином, відбувається безперервна передача інформації між мобільними пристроями і хмарним середовищем. Ця інформація цінна; тому вона становить інтерес для порушників.

Можна виділити такі цілі в атаці на хмарну систему: 1) дані (в системі зберігаються особиста інформація, дані, які важливі для ведення бізнесу, до яких зловмисники намагаються отримати доступ); 2) ідентифікація (у хмарних системах міститься ідентифікаційна інформація, пов'язана з їх власниками, оволодіння якої з боку порушників може поставити під загрозу особу власника або організації); 3) доступність (порушники можуть обмежити доступ до системи і перешкодити її використання законними користувачами).

Будь-яка атака, яка зачіпає хмару, може вплинути на мобільні пристрої, підключені до цієї хмари. І навпаки, заражений шкідливим ПЗ мобільний пристрій може вплинути на хмару, з якої він отримує свої послуги.

Основним ворогом мобільних пристроїв і хмарних технологій є шкідливе програмне забезпечення, що маскується під звичайні і корисні застосування, які користувачі можуть завантажувати і використовувати, але насправді вони містять приховані скрипти, які виконують різні дії в фоново-

му режимі і загрожують безпеці користувача. Після зараження мобільного пристрою порушник може записувати всі розмови між користувачем та іншими людьми, красти зображення і відео і відправляти цю інформацію розробнику атаки, отримати доступ до особистої інформації, видалити особисту інформацію з зламаного гаджета або професійні дані, перетворити мобільний пристрій в зомбі-машину, зробити його непридатним для використання, пошкодити ОС, видаливши завантажувальні скрипти, зробити його непридатним для використання, викрасти конфіденційну інформацію і т.д.

У всіх випадках шкода має бути ідентифікована, щоб можна було знайти ефективні контрзаходи.

При аналізі атак на хмарні системи слід враховувати сервіси, які останні надають користувачам. Існують три різні моделі хмарних обчислень: 1) SaaS (Software-as-a-Service – програмне забезпечення як послуга – хмарних послуг надає користувачеві ПЗ, яке виконується і розгортається в хмарної інфраструктурі, наприклад, Google Maps; 2) PaaS (Platform-as-a-Service – платформа як послуга – постачальник надає споживачеві платформу для розгортання створених користувачем застосувань, наприклад, Google App Engine, Microsoft Azure; 3) IaaS (Infrastructure-as-a-Service – інфраструктура як послуга – постачальник надає користувачеві можливості обробки, зберігання, мережі та інші необхідні обчислювальні ресурси, що дозволяють йому запускати своє програмне забезпечення, наприклад, Amazon Web Service, Eucalyptus, OpenNebula.

Джерелом атак на мобільні пристрої є професіонали (комерційні або військові, що прагнуть атакувати конфіденційність, цілісність, доступність хмарних систем), кримінал (використовують вкрадені персональні дані для отримання доходу), так звані «чорні хакери» (націлені на порушення доступності та крадіжку даних з пристроїв за допомогою розробленого шкідливого ПЗ), «сірі хакери» (виявляють уразливості пристроїв).

Основні типи атак в хмарні обчислювальні системи: 1) атаки з віртуальної машини (порушники змінюють синтаксис і семантику структури даних ядра віртуальної машини при роботі в гостьовому режимі); 2) атаки з віртуальної мережі (порушники, використовуючи вразливості, організують великомасштабні DDoS-атаки з метою порушити доступність хмарних сервісів); 3) атаки з боку шкідливого гипервизора (якщо порушникам за допомогою бекдор вдається скомпрометувати гипервизор, то це веде до катастрофічного пошкодження хмарних обчислювальних систем); 4) атаки з-за меж хмарного середовища (порушники відправляють величезну кількість запитів на доступ до віртуальних машин, відключаючи доступність віртуальних машин для законних користувачів).

До основних класів мобільних шкідливих програм, що атакують мобільні пристрої, відносяться: Botnet (атакує пристрій віддаленим бот-

майстром); Backdoor (відкривається на скомпрометованому пристрої, змушуючи його чекати команди, що надходять із зовнішнього сервера); Rootkit (створює переповнення буфера для отримання привілеїв суперкористувача на пристрої); Worms (хробак, що створює копії самого себе і поширює ці копії через мережу і знімні носії); SMS Trojan (відправляє таємні SMS-повідомлення без відома користувача, спам-повідомлення всім контактам користувача, а також використовується в механізмах автентифікації для банківських установ шляхом відправки SMS-повідомлень з метою вирішення несприятливих транзакцій; Spyware (маскується під корисний додаток, але здійснює приховану шкідливу діяльність – виявлеє конфіденційну інформацію на мобільному пристрої і відправляє її на зовнішній сервер); Installer – (автоматично встановлює шкідливі програми); Ransomware (блокують доступ користувача до пристрою і вимагають від користувача заплатити певну суму грошей, щоб видалити шкідливу програму, або шифрують персональні дані, а потім запитують викуп для отримання ключа дешифрування); Trojan (будь-які шкідливі програми, поведінка яких відрізняється від попередніх класів, наприклад, можуть змінювати або видаляти дані з мобільного пристрою без згоди власника, або заражують будь-який комп’ютер через USB).

Технології вторгнення в хмарні обчислювальні системи: 1) розвідувальні технології (рекогносцировка) припускають збір максимально можливої нформації про жертву перед початком атаки (соціальна інженерія, збір сміття, збір даних з веб-сайтів компаній, з соціальних мереж тощо); 2) розвідка системи доменних імен (DNS-сервер може бути хорошим місцем для хакерів, щоб зібрати важливу інформацію, таку як адреса поштового сервера, адреса веб-сервера, інформацію про операційну систему і т.д.); 3) відмова в обслуговуванні (споживання системних ресурсів шляхом відправки величезної кількості незаконних запитів понад межі, яку може обробити хмарна система); 4) злом облікового запису (порушник використовує спеціальні інструменти і методи для злому хешированного файлу паролів); 5) впровадження мови структурованих запитів (порушник об’єднує рядки запитів на мові структурованих запитів зі змінними, призначеними для SQL-серверів, на яких виконуються вразливі додатки баз даних); 6) використання міжсайтових сценаріїв (ін’єкція шкідливих скриптів типу JavaScript, VBScript, ActiveX, HTML або flash на вразливу активну веб-сторінку і запуск їх в браузері жертви); 7) ін’єкція шкідливих програм (атака використовує обмін метаінформацією в хмарних обчислювальних системах і запускає шкідливі служби).

*УДК 004.056*
**Козюра В. Д.**
кандидат технічних наук, доцент,
Національна академія Служби безпеки України
**Хорошко В. О.**
доктор технічних наук, професор,
Національний авіаційний університет

# ВИБІР ПОКАЗНИКІВ ЯКОСТІ IDPS В ТЕХНОЛОГІЯХ ХМАРНИХ ОБЧИСЛЕНЬ

Реалізуючі кіберзагрози у хмарних технологіях порушники використовують різноманітні методи і засоби таємного проникнення і впровадження шкідливого коду, приховані канали управління і впливу, спеціальні прийоми і техніки обману і обфускації. Для протидії цим загрозам необхідний випереджальний розвиток сучасних методів і засобів кіберзахисту. Перспективним напрямком є створення та використання систем виявлення і протидії кіберзагрозам (СВПК) як на стороні кінцевих користувачів, що використовують хмарні технології, так і на стороні провайдерів цих послуг. СВПК інтегрують функції відразу декількох засобів захисту і здатні успішно протистояти сучасним атакам.

Проблемними питаннями, які необхідно вирішити при створенні нових або виборі з числа існуючих СВПК, є задачі обґрунтування складу і структури вимог до функціональних і технічних характеристик (ФТХ) СВПК та оцінювання якості їх реалізації. Основними напрямками рішення цих завдань є обґрунтування систематизованого комплексу вимог до ФТХ СВПК, що максимально повно і точно враховує особливості середовища і умови їх застосування, а також розробка методів і засобів вимірювання, розрахунку і оцінювання якості реалізації ФТХ.

Якість СВПК проявляється в процесі її використання за призначенням і виражається в формі оцінки ефективності її функціонування, що відображає ступінь досягнення поставлених перед нею цілей з урахуванням витрат ресурсів і часу. Цільовим призначенням СВПК є реалізація операцій збору даних про події ІБ з різних джерел, виявлення і реагування на атаки до ресурсів, що захищаються, в реальному часі. Для оцінювання ефективності вирішення цих завдань з використовуються показники повноти, точності і оперативності, а також вартості.

Слід мати на увазі, що жоден з провайдерів хмарних обчислень не розкриє статистику атак (успішних і неуспішних) на свої ресурси, тому оцінку показників якості СВПК можна отримати на імітаційних моделях або стендах-імітаторах в складі кіберполігонів.

В результаті проведення $N$ експериментів з оцінюваної СВПК будується матриця рішень, що відображає результати реакції системи на обробку шкідливих і нормальних програм:

| Класифікується як / Справжня класифікація | Шкідлива програма | Нормальна програма |
|---|---|---|
| Шкідлива програма | $N_{TN}$ | $N_{FN}$ |
| Нормальна програма | $N_{FP}$ | $N_{TP}$ |

$N_{TN}$ – кількість шкідливих програм, що правильно розпізнані СВПК як шкідливі програми (True Negative) – правильне розпізнавання шкідливої програми.

$N_{FN}$ – кількість шкідливих програм, що помилково розпізнані СВПК як нормальні програми (False Negative) – пропуск шкідливої програми;

$N_{TP}$ – кількість нормальних застосувань, які були правильно розпізнані СВПК як нормальні (True Positive) – правильне розпізнавання нормального застосування.

$N_{FP}$ – кількість нормальних застосувань, які були неправильно розпізнані СВПК як шкідливі програми (False Positive) – помилкова тривога.

На основі результатів, що представлені в матриці рішень, можна визначити різні показники ефективності СВПК [1, 2, 3], в залежності від переслідуваних цілей.

Введемо наступні позначення: $N_N = N_{TN} + N_{FN}$ – кількість атак, здійснених шкідливими програмами; $N_P = N_{TP} + N_{FP}$ – кількість запитів, що надійшли від нормальних застосувань; $N_R = N_{TN} + N_{NP}$ – кількість правильно прийнятих рішень СВПК; $N_E = N_{FP} + N_{FN}$ – кількість помилкових рішень, прийнятих СВПК.

Очевидно, . $N = N_N + N_P = N_{TN} + N_{FN} + N_{TP} + N_{FP}$

Для оцінки якості (ефективності) СВПК можуть бути використані наступні показники:

Інтегрована ймовірність правильного розпізнавання або точність: є відсоток правильно класифікованих застосувань (шкідливих і нормальних) в порівнянні із загальним числом експериментів:

$$\text{Точність} = \frac{N_{TN} + N_{TP}}{N_{TN} + N_{TP} + N_{FN} + N_{FP}} = \frac{N_R}{N}.$$

2. Ймовірність виявлення шкідливих програм (ЙВШП): відсоток вірно класифікованих шкідливих програм в порівнянні із загальною кількістю шкідливих програм:

$$P_{\text{йвшп}} = \frac{N_{TN}}{N_{TN} + N_{FN}} = \frac{N_{TN}}{N_N}.$$

3. Ймовірність помилковості спрацьовувань (помилковості тривоги) (ПТ): відсоток нормальних застосувань, неправильно класифікованих як шкідливі програми, в порівнянні із загальним числом нормальних додатків:

$$P_{\text{ПТ}} = \frac{N_{\text{FP}}}{N_{\text{TP}} + N_{\text{FP}}} = \frac{N_{\text{FP}}}{N_{\text{P}}}.$$

4. Ймовірність пропуску шкідливих програм (ЙПШП): відсоток шкідливих програм, неправильно класифікованих як нормальні, в порівнянні із загальною кількістю шкідливих:

$$P_{\text{йпшп}} = \frac{N_{\text{FN}}}{N_{\text{TN}} + N_{\text{FN}}} = \frac{N_{\text{FN}}}{N_{\text{N}}}.$$

5. Ймовірність правильного розпізнавання нормальних застосувань (ЙПРН): відсоток правильно класифікованих нормальних застосувань в порівнянні із загальним числом нормальних додатків:

$$P_{\text{йпрн}} = \frac{N_{\text{TP}}}{N_{\text{TP}} + N_{\text{FP}}}.$$

7. Коефіцієнт помилок детектування шкідливих програм:

$$\text{Err} = \frac{N_{\text{FP}} + N_{\text{FN}}}{N_{\text{TN}} + N_{\text{TP}} + N_{\text{FN}} + N_{\text{FP}}} = \frac{N_{\text{E}}}{N}.$$

СВПК для мобільних пристроїв і хмарних обчислень використовують загальний спосіб вимірювання ефективності. Єдина різниця полягає в тому, що в мобільних пристроях IDS шукає шкідливі програми, тоді як в хмарних обчисленнях IDS шукає вторгнення або атаки. В обох середовищах IDS зазвичай конкурують у виявленні максимальної кількості шкідливих програм / вторгнень, щоб знайти підходящу реакцію на ці загрози.

**Література**

1. F.A. Narudin, A. Feizollah, N.B. Anuar, A. Gani, Evaluation of machine learning classifiers for mobile malware detection, Soft Comput. 20 (1) (2016), pp. 343-357.

2. S.Y. Yerima, S. Sezer, G. McWilliams, I. Muttik, A new Android malware detection approach using bayesian classification, in: 2013 IEEE 27th International Conference on Advanced Information Networking and Applications (AINA), March 2013, pp. 121-128.

3. S.Y. Yerima, S. Sezer, I. Muttik, High accuracy android malware detection using ensemble learning, IET Inf. Security 9 (6) (2015), pp. 313-320.

*УДК 342.52*
**Марущак А. І.**
доктор юридичних наук, професор,
Національна академія СБ України

# ПРОБЛЕМА ЛЕГІТИМІЗАЦІЇ ПРОЦЕСУ ВЗАЄМНОГО ПЕРЕТВОРЕННЯ ПАПЕРОВИХ І ЕЛЕКТРОННИХ ДОКУМЕНТІВ

У сучасний стан розвитку процесів диджіталізації суспільного життя і, насамперед, однієї із найскладніших його систем – державного управління, виникає низка запитань теоретичного і практичного характеру, зокрема щодо легітимності перетворення паперових документів в електронні і навпаки без втрати юридичної сили таких документів.

Не зважаючи на те, що Закон України «Про електронні довірчі послуги» від 5 жовтня 2017 року [1] частково розширив регулювання відповідних відносин, започатковане у Цивільному кодексі України, законах України «Про електронні документи та електронний документообіг», «Про захист інформації в інформаційно-телекомунікаційних системах», наукова і практична проблема взаємного перетворення паперових і електронних документів не вирішена і потребує подальшого дослідження.

Закон України «Про електронні документи та електронний документообіг» передбачає, що електронний документ – це документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа [2, ст. 5]. Зазначеним Законом передбачається можливість створення, передачі, збереження і перетворення електронного документа електронними засобами у візуальну форму.

Крім цього, законодавство про електронні документи та електронний документообіг оперує дискусійним поняттям «оригінал електронного документа» під яким розуміється електронний примірник документа з обов'язковими реквізитами, у тому числі з електронним підписом автора або підписом, прирівняним до власноручного підпису відповідно до Закону України «Про електронні довірчі послуги» [2, ст. 7]. Дискусійність даного терміну обґрунтовується не лише теоретичними пошуками представників науки інформаційного права, а й закладена у самому законі: «у разі надсилання електронного документа кільком адресатам або його зберігання на кількох електронних носіях інформації кожний з електронних примірників вважається оригіналом електронного документа» [2, ст. 7]. Таким чином, фактично будь-який примірник електронного документа є його оригіналом, що фактично нівелює питання розмежування оригінала і копії електронного документа.

Законодавство про електронний документообіг оперує поняттям «копія документа на папері для електронного документа», під яким розуміється візуальне подання електронного документа на папері, яке засвідчене в порядку, встановленому законодавством [2, ст. 7]. Однак порядок засвідчення копії електронного документа на папері чинним законодавством України не визначено. Тобто фактично, легітимна процедура перетворення електронного документа в паперовий на даний час не передбачена. І якщо технологічно такий процес забезпечити можливо, наприклад, використовуючи програмні засоби для перетворення документа, створеного у редакторі Word, в документ формату .pdf, то юридичні наслідки таких дій не визначені чинним законодавством України.

Таким чином, невирішеною на сьогодні частиною проблеми як на законодавчому рівні, так і серед науковців є регламентація переходу електронного документа у паперовий. Зазначений недолік інформаційно-правових відносин може суттєво пригальмувати розвиток процесів виконання державно-владних функцій з використанням електронного документообігу. Наприклад, у процесі запровадження електронного кримінального провадження в Україні [3] особливого значення набуває переведення процесуальних документів з електронного формату у паперовий зі збереженням легітимності, а також навпаки, процедура і юридичні наслідки перетворення паперових документів в електронну форму.

Таким чином, проблема легітимізації процесу взаємного перетворення паперових і електронних документів потребує поглибленого аналізу представників науки інформаційного права, а також фахівців з ІКТ технологій.

**Література**

1. Про електронні довірчі послуги: Закон України від 5 жовтня 2017 року № 2155-VIII. Відомості Верховної Ради України. 2017. № 45. Ст. 400.

2. Про електронні документи та електронний документообіг: Закон України від 22 травня 2003 року № 851-IV. Відомості Верховної Ради України. 2003. № 36. Ст. 275.

3. Склад міжвідомчої робочої групи з питань запровадження електронного кримінального провадження. URL: https://yur-gazeta.com/publications/practice/kriminalne-pravo-ta-proces/pravove-regulyuvannya-elektronnogo-kriminalnogo-provadzhennya.html.

*УДК 34:004*
**Матяш О. І.**
кандидат технічних наук,
старший науковий співробітник,
Національна академія СБ України

# ЦИФРОВІ ТЕХНОЛОГІЇ У ПРОВЕДЕННІ НАУКОВИХ ФОРУМІВ

Наукові форуми відіграють важливе значення у проведенні наукової діяльності, на них представляються результати наукових досліджень, обговорюються проблемні питання, відбувається пошук шляхів подальших наукових розробок.

У проведенні наукових форумів не останнє місце посідає застосування цифрових технологій, починаючі від використання електронної пошти у розсилці інформаційних повідомлень та закінчуючи розміщенням збірників тез доповідей, матеріалів конференцій в електронному вигляді.

Проведення наукових форумів пов'язано з тим, що під час здійснення наукової діяльності завжди існує нагальна потреба створення майданчиків для спілкування наукової спільноти. Закріплено така потреба у пункті 5 статті 5 Закону України «Про наукову і науково-технічну діяльність», відповідно до якої вчений має право публікувати результати своїх досліджень або оприлюднювати їх в інший спосіб у порядку, встановленому законодавством України [1].

На відміну від вченого науковий працівник згідно з підпунктом 2 пункту 4 статті 6 Закону України «Про наукову і науково-технічну діяльність» зобов'язаний представляти результати наукової і науково-технічної діяльності шляхом наукових доповідей, публікацій тощо.

Реалізація вченими та науковими працівниками своїх прав та обов'язків відбувається шляхом участі у наукових форумах. Вибір наукового форуму для авторів важливе питання, у зв'язку з тим, що кожен науковий форум пропонує свої умови участі, відрізняються місця проведення, строки, вартість участі, форма представлення матеріалів наукового форуму. Для авторів також важлива престижність наукового форуму від якого залежить подальша адекватність оцінки наукового результату та можливості його поширення.

Полегшують вибір наукового форуму для авторів сучасні цифрові технології. Розповсюдження інформації про форуми в більшості випадків відбувається в електронній формі, за рахунок розсилки електронних листів, розміщення оголошень на сайтах організаторів, а також в соціальних мережах та месенжерах.

Сприяє розповсюдженню інформації про наукові форуми також Міністерство освіти України та його підпорядковані установи. Так, наприклад, Інститутом модернізації змісту освіти на офіційному сайті представлено розділ «Наукові заходи для ЗВО» в якому щорічно оприлюднюються Перелік міжнародних, всеукраїнських науково-практичних конференцій здобувачів вищої освіти і молодих учених та Перелік наукових конференцій з проблем вищої освіти і науки [2].

Важливими інструментами цифрових технологій є ідентифікатори авторів та наукових результатів – такі як ORCID ID та DOI.

Місія ORCID полягає в тому щоб усі учасники дослідницької, наукової та інноваційної діяльності мали свої унікальні ідентифікатори, які пов'язані з їхніми результатами роботи незалежно від наукового напрямку, місця та часу. Метою ORCID є надання індивідуальним дослідникам ідентифікаторів, який може доданий до імені, під яким вони здійснюють свою діяльність. Надання відкритих інструментів, які дозволяють будувати надійні та прозорі зв'язки між дослідниками, їх внесками та пов'язаними з ними організаціями. А також надання послуг щоб допомогти усім бажаючім знайти потрібну інформацію, спростити звітність та аналіз діяльності [3].

Набуває популярності також DOI (ідентифікатор цифрового об'єкту), який присвоюється електронному документу в глобальній мережі Інтернет. Важливою особливістю DOI є те, що матеріали з ідентифікатором може видалити тільки видавець, тобто організація, яка розмістила його.

Ця особливість дуже важлива в наукових колах. Це обумовлено тим, що джерела інформації це основа наукової діяльності і до них ставляться досить уважно. Достовірність вхідної інформації запорука якісного наукового результату.

Зростання популярності DOI обумовлюється тим, що:

гарантується збереження матеріалів з DOI на відміну від звичайних сайтів або електронних бібліотек;

визнано більшістю видавців зручності і безпеки DOI;

наявність DOI позитивно впливає на репутацію автора або видавця, за рахунок того, що дозволяє розміщувати матеріали у провідних світових наукових бібліографічних каталогах;

цитування стаття з DOI журналом, що входить до наукометричних баз Scopus, WebofScience, заносить цю статтю в зазначені бази, що істотно підвищує її значущість.

Цифрові технології у проведенні наукових форумів на сучасному етапі розвитку науки відіграють ключове значення. Вони сприяють пошуку потрібної інформації, формуванню перевірених джерел, які стають основою подальших досліджень. Для авторів наявність ORCID надає можливість особистої ідентифікації для представлення наукових результатів та

особливо актуальна для українських вчених при розміщенні у англомовних виданнях де виникають помилки при транслітерації.

Сприйняття та застосування науковцями цифрових технології у проведенні наукових форумів це запорука інтеграції у міжнародний науковий простір.

**Література**

1. Закон України від 26.11.2015 № 848»Про наукову і науково-технічну діяльність». – Відомості Верховної Ради України, 2016. – № 3 – Ст. 25

2. Доступ за посиланням: https://imzo.gov.ua/osvita/vyscha-osvita/naukovi-zahodi-dlya-vnz/.

3. Доступ за посиланням: https://orcid.org/.

*УДК 342.1*

**Мельник Д. С.**
кандидат юридичних наук,
Служба безпеки України

## ЩОДО АКТУАЛЬНИХ ПРОБЛЕМ ПРОТИДІЇ ВИКОРИСТАННЮ ЦИФРОВИХ ВАЛЮТ У ПРОТИПРАВНІЙ ДІЯЛЬНОСТІ В УКРАЇНІ

Світові процеси глобалізації та стрімкий розвиток інформаційних технологій зумовили виникнення нових загроз національній безпеці України у фінансовій, інформаційній та інших сферах.

Зокрема, сучасні світові тенденції свідчать про активне використання цифрових валют[1] у протиправній діяльності *(легалізації доходів, одержаних злочинним шляхом, фінансування терористичної й сепаратистської діяльності, посягань на конституційний лад та державну владу, протиправного виведення капіталів за кордон),* внаслідок чого виникають численні загрози та ризики для національної безпеки багатьох держав світу, у т.ч. й України.

Зокрема, Міністерство юстиції США заявило про викриті факти використання РФ цифрових валют (далі – криптовалют) для фінансування ведення підривної діяльності на американській території, у т.ч. хакерські атаки на державні установи протягом 2014 – 2018 років та втручання у вибори Президента США у 2016 році. Також у звіті Мін'юсту США про боротьбу з торгівлею наркотиками за 2017 рік зазначено про використання

[1] Цифрова валюта (криптовалюта) – вираження вартості, що представлений у цифровому форматі і виступає в якості засобу обміну, або розрахункової грошової одиниці, або засобу зберігання вартості і при цьому не підпадає під поняття законного платіжного засобу.

операцій з криптовалютами для відмивання коштів, отриманих злочинним шляхом. У грудні 2017 року Федеральною прокуратурою США спільно з Об'єднаним АТЦ ФБР (м. Нью-Йорк) було викрито факт використання криптовалюти для відмивання злочинних активів, та подальшого фінансування терористичної організації ІДІЛ.

Не є винятком і Україна. Так, у лютому 2019 року саме розрахунки у криптовалюті офіційно визнано СБУ одним із головних механізмів фінансування т.зв. «ДНР/ЛНР». Попередньо 01.02.2018 прес-центром СБУ офіційно повідомлено про викритий механізм фінансування НЗВФ т.зв. «ДНР/ЛНР» та діяльності антиукраїнських Інтернет-ресурсів з використанням криптовалют[1].

Також протягом 2016-2018 років невстановленими особами здійснювалося блокування сайтів низки державних установ та ураження їх інформаційних ресурсів шкідливим програмним забезпеченням з вимогами винагороди у криптовалюті за їх розблокування.

Згідно з оцінками Інтерполу та Європолу, популярність криптовалют як засобу розрахунків серед злочинців стрімко зростає і вже через кілька років їх можна буде визнати основним платіжним інструментом у злочинному світі.

На сьогодні на міжнародному рівні відсутні єдині стандарти регулювання діяльності у сфері створення і обігу криптовалют, їх контролю і моніторингу.

Наразі лише окремі держави світу *(Бразилія, Білорусь, Сінгапур, США, Японія)* визначилися у правовому статусі криптовалюти та вжили заходів щодо законодавчого врегулювання їх обігу. Зокрема, Президент Республіки Білорусь у 2017 році видав указ про «майнінг» криптовалют та порядок їх використання, а також розпорядження щодо створення в країні Парку високих технологій. Однак поняття «криптовалюта» та порядок її створення й операцій з нею залишаються неврегульованими нормами законодавства України.

Водночас Директива ЄС 2015/849 по боротьбі з відмиванням грошей передбачає можливість використання криптовалют з цією метою та визначає повноваження підрозділів Фінансової розвідки (FIU) щодо отримання доступу до інформації про криптовалютні гаманці та біржі.

FATF підготувала за дорученням лідерів країн G-20 та оприлюднила 21.06.2019 оновлену «Настанову по ризик-орієнтованому підходу до цифрових активів та постачальників цифрових послуг» з рекомендаціями для країн-учасниць щодо протидії відмиванню грошей та фінансуванню тероризму з використанням криптовалют[2]. Рекомендації передбачають запровадження до червня 2020 року низку змін до існуючого порядку фінансо-

[1] https://ssu.gov.ua/ua/news/1/category/21/view/4344#.HME5oKQx.dpbs.

[2] https://www.kommersant.ru/doc/4011572.

вого моніторингу, у т.ч. необхідність отримання ліцензії національного регулятора операторами криптовалютних сервісів, проходження ними процедури «знай свого клієнта», обов'язкову ідентифікацію транзакцій на суму від 1 тис. дол. США, обов'язок таких операторів відстежувати і забороняти транзакції для осіб і організацій, які знаходяться під міжнародними санкціями, передавати один одному інформацію про клієнтів при здійсненні ними розрахунків на суму від 1 тис. дол. США незалежно від виду валюти. Також рекомендаціями пропонується запровадити особливі вимоги до фізичних осіб, які часто проводять криптовалютні операції, а також заборонити приховування криптовалютними сервісами реальних учасників транзакцій, передбачити можливість припинення діяльності порушників за рішенням національних регуляторів.

Вказані рекомендації вже впроваджуються країнами-учасницями G-20 у національне законодавство. Також на початку 2020 року набула чинності нова Директива ЄС по боротьбі з відмиванням грошей (5AMLD), яка вимагає реєстрації крипто валютних бірж в місцевих регулятивних органах та дотримання ними місцевого законодавства.

Участь України у глобальних світових процесах останнім часом зумовлює активне впровадження в обіг криптовалют та їх використання в якості засобу розрахунків. Високій популярності криптовалют в Україні сприяють їх невизначений правовий статус та анонімність, децентралізованість створення («майнінгу»[1]) та безконтрольність обігу криптовалют, які нівелюють можливості органів фінмоніторингу та сприяють їх активному використанню організаціями, групами і особами як у цілком легальній, так і у протиправній діяльності.

НБУ, НКЦПФР і Нацфінпослуг України у спільній заяві від 30.11.2017 визнали, що складна правова природа криптовалют не дозволяє визнати їх ані грошовими коштами, ані валютою і платіжним засобом іншої країни чи валютною цінністю, ані електронними грошима, ані цінними паперами чи грошовими сурогатами. Разом з тим фінансові регулятори заявили про триваюче опрацювання питання щодо правового статусу криптовалют та законодавчого врегулювання операцій з ними з урахуванням позицій регуляторів інших країн та останніх тенденцій в розвитку цифрових технологій.

Донедавна у Верховній Раді України на опрацюванні були три законопроекти щодо унормування обігу криптовалют в Україні: № 7183 від

[1] «Майнінг» (створення, генерація) цифрової валюти – обчислювальні операції, які здійснюються за допомогою спеціалізованого обладнання з метою забезпечення працездатності та безпеки системи блокчейн – децентралізованого електронного реєстру усіх проведених легальних (перевірених та підтверджених) транзакцій, зокрема криптовалютних операцій, за проведення яких особа («майнер») отримує винагороду системи блокчейн залежно від умов її функціонування.

06.10.2017 «Про обіг криптовалюти в Україні»; № 7183-1 від 10.10.2017 «Про стимулювання ринку криптовалют та їх похідних в Україні» та № 7246 від 30.10.2017 «Про внесення змін до Податкового кодексу України (щодо стимулювання ринку криптовалют та їх похідних в Україні)». Однак у зв'язку з перезавантаженням системи органів державної влади після виборів Президента та ВР України у 2019 році вказані законопроекти були зняті з розгляду 29.08.2019 та повернуті ініціаторам для повторного внесення.

Тому експертне співтовариство, яке вже висловлювало переконання у необхідності прийняття принципово нового законодавства у цій сфері, отримало шанс бути почутими українським законодавцем. При цьому першочерговим завданням уповноважених державних органів має стати невідкладна підготовка спільно представниками експертного середовища і громадськістю та внесення на розгляд ВР України законопроекту «Про обіг криптовалют в Україні», яким буде визначено засади загальнодержавної стратегії контролю обігу віртуальних валют.

Також актуальним є впровадження рекомендацій з протидії відмиванню грошей та фінансуванню тероризму з використанням криптовалют шляхом внесення необхідних змін у вітчизняне законодавство та практику правозастосування. Певні кроки вже були зроблені з прийняттям 06.12.2019 нової редакції Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення», де передбачено низку ключових положено щодо моніторингу використання віртуальних (цифрових) активів як засобу розрахунку.

*УДК:343.14*

**Метелев О. П.**
Інститут підготовки юридичних
кадрів для Служби безпеки України
Національного юридичного
університету імені Ярослава Мудрого

## ОКРЕМІ АСПЕКТИ ПРАВОВОГО РЕГУЛЮВАННЯ ВИКОРИСТАННЯ ТРАНСПОРТНИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ ЯК ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА ДЛЯ ОТРИМАННЯ ВІДОМОСТЕЙ, ЗНАЧУЩИХ ДЛЯ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ

Інформаційні системи, такі як всесвітня інформаційна система загального доступу Інтернет, є складовими кіберпростору. В свою чергу, транспортна телекомунікаційна мережа (далі – ТТМ) – це невід'ємна частина

глобального інформаційного простору, яка являє собою інформаційне середовище, що забезпечує передачу цифрової інформації (даних) в глобальному інформаційному (кібернетичному) просторі.

Екстериторіальний характер ТТМ, разом із глобальною мережею Інтернет в значній мірі ускладнює їх правове регулювання, оскільки іноді досить складно визначити до юрисдикції якої держави відноситься те чи інше кримінальне правопорушення. Отже, при проведенні слідчих (розшукових) дій виникає закономірне питання, щодо правомірності роботи в інформаційному середовищі ТТМ для отримання цифрових (електронних) доказів в інтересах кримінального провадження.

Проведений аналіз наукової літератури свідчить, що наукові дослідження ТТМ як особливого інформаційного середовища для отримання відомостей значущих для кримінального провадження у юридичній літературі практично відсутні.

В ТТМ циркулюють цифрові відомості, які можуть бути значущими для кримінального провадження, тому під час проведення слідчих (розшукових) дій виникає необхідність використання ТТМ для належного отримання цифрових (електронних) доказів, для їх подальшого використання в кримінальному процесі.

У вітчизняному законодавстві забезпечення гарантії прав і свобод щодо таємниці спілкування законодавець передбачив в новелах Кримінального процесуального кодексу України (далі – КПК) [1]. Так, у відповідності до п. 7 ч. 1 ст. 7 КПК таємниця спілкування є однією із загальних засад кримінального провадження. Також, в ст. 14 КПК наголошується, що під час кримінального провадження кожному гарантується таємниця приватного листування, телефонних розмов, телеграфної та іншої кореспонденції, інших форм спілкування. Єдиною умовою втручання у таємницю спілкування є лише судове рішення, яке прийняте у випадках, передбачених КПК, з метою виявлення та запобігання тяжкому чи особливо тяжкому злочину, встановлення його обставин, особи, яка вчинила злочин, якщо в інший спосіб неможливо досягти цієї мети.

Багаторічний досвід провідних країн в боротьбі зі злочинністю та тероризмом, однозначно свідчить про високу ефективність впровадження систем перехоплення в інформаційному просторі ТТМ для збору превентивної інформації щодо терористичних актів та інші протиправні дії, що плануються. В «Конвенції про кіберзлочинність» від 23.11.2001 р. (або Будапештській конвенції), яка ратифікована Верховною Радою України 07.09.2005 р. зазначається, що здійснення перехоплення інформації у міжнародних ТТМ є необхідною умовою боротьби проти найбільш небезпечних злочинних угрупувань та міжнародних терористів. Згодом був прийнятий «Додатковий протокол про криміналізацію дій расистського й ксе-

нофобського характеру, вчинених через комп'ютерні системи» від 28.01.2003 р., який був ратифікований Верховною Радою України 21.07.2006 р. [2, 3].

На сьогодні, Конвенція про кіберзлочинність залишається найбільш актуальним міжнародним документом відносно кіберзлочинності і електронних (цифрових) доказів. При цьому вона постійно оновлюється в протоколах та керівних вказівках. Також, активно ведуться перемовини стосовно Другого Додаткового протоколу щодо розширення міжнародного співробітництва і доступу до доказів в «хмарних сховищах», що, в перспективі, значно збільшить кількість інструментів та засобів для забезпечення верховенства права в кіберпросторі.

Небезпека злочинів в кіберпросторі багаторазово зростає, коли вони здійснюються стосовно функціонування об'єктів життєзабезпечення, транспортних і оборонних систем, атомної енергетики. А отже, інформаційне середовище ТТМ та законність роботи в ньому стають вагомим чинником при здійсненні діяльності уповноваженими органами отримання відомостей, які мають доказове значення для кримінального провадження. Крім того, необхідне чітке законодавче регулювання процесуальної діяльності в ТТМ, враховуючи їх екстериторіальний характер, для забезпечення в цій сфері суспільних відносин безпеки особистості, суспільства і держави в цілому.

**Література**

1. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI. Режим доступу: http://zakon5.rada.gov.ua/laws/show/4651-17. Дата звернення: 29.02.2020.

2. Конвенція про кіберзлочинність від 23.11.2001 р. Ратифікована із застереженнями і заявами Законом від 07.09.2005 № 2824-IV (2824-15). Режим доступу: https://zakon.rada.gov.ua/laws/show/994_575. Дата звернення: 29.02.2020.

3. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи від 28.01.2003 р., Протокол ратифіковано із застереженням Законом № 23-V (23-16) від 21.07.2006. Режим доступу: https://zakon.rada.gov.ua/laws/show/994_687. Дата звернення: 28.02.2020.

*УДК 621.39 (043.2)*
**Одарченко Р. С.**
доктор технічних наук, доцент,
Державний науково-дослідний інститут
технологій кібербезпеки та захисту інформації
**Бурмак Ю. А.**
ДЗ «Київський коледж зв'язку»
**Усік П. С.**
Центральний український
національний технічний університет

# ОЦІНКА СИСТЕМ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ СТІЛЬНИКОВИХ МЕРЕЖ 5G

Стільниковий зв'язок (мобільний зв'язок) – один з видів мобільного радіозв'язку, в основі якого лежить стільникова мережа [1]. Нові покоління мобільного зв'язку починали розроблятися практично через кожні десять років з моменту переходу від розробок першого покоління аналогових стільникових мереж в 1970-х роках (1G) до мереж з цифровою передачею (2G) в 1980-х роках. Останнім стандартизованим поколінням являються мережі 5G.

На відміну від мереж попередніх поколінь, спектр послуг яких був жорстко обмежений і дещо розширений в 4G [2], послуги платформи 5G носять синергетичний і масштабований характер, і не обмежені одного разу заданим функціоналом. В цілому, можна сказати, що мережа 5G вбирає в себе не тільки мобільні, але також і фіксовані послуги зв'язку, а також високошвидкісний доступ в інтернет з малою затримкою, і, крім того, спеціалізовані та корпоративні мережі.

Концепція безпеки мобільних мереж зв'язку п'ятого покоління ґрунтується на перевикористанні відповідних технологій, прийнятих в стандарті 4G-LTE. На рис. 1 наведена загальна архітектура побудови ядра мережі 5G [3].

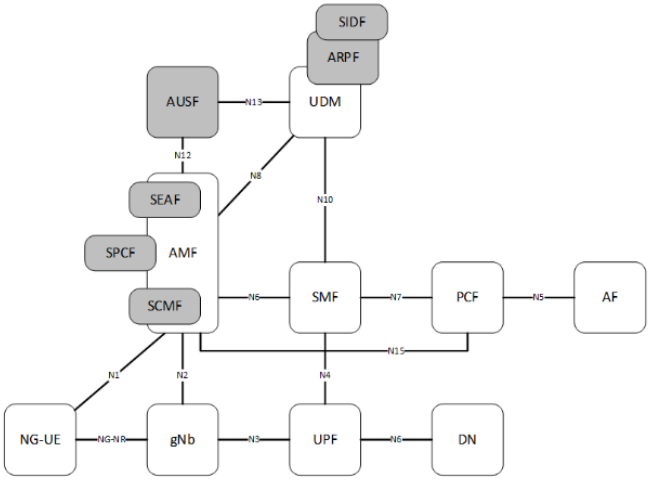


Рис. 1. Архітектура побудови опорної мережі 5G

Темним кольором на ній виділені функціональні об'єкти, що реалізують механізми забезпечення безпеки:

1. Security Anchor Function (SEAF) – якірна функція безпеки.

2. Authentication Server Function (AUSF) – функція сервера аутентифікації.

3. Authentication Credential Repository and Processing Function (ARPF) – функція сховища та обробки облікових даних аутентифікації.

4. Security Context Management Function (SCMF) – функція управління контекстом безпеки.

5. Security Policy Control Function (SPCF) – функція управління політикою безпеки.

6. Subscription Identifier De-concealing Function (SIDF) – функція виокремлення ідентифікатора користувача.

В цілому концепція безпеки мереж 5G включає в себе: аутентифікацію користувача з боку мережі; аутентифікацію мережі з боку користувача; узгодження криптографічних ключів між мережею і призначеним для користувача терміналом; шифрування і контроль цілісності сигнального трафіку на рівні RRC (між UE і gNb); шифрування і контроль цілісності сигнального трафіку на рівні NAS (між UE і AMF); шифрування і контроль цілісності призначеного для користувача трафіку (між UE і gNb); захист ідентифікатора користувача; захист інтерфейсів між різними елементами мережі відповідно до концепції мережевого домену безпеки, описаного в рекомендації 3GPP TS 33.310, в т.ч. захист інтерфейсів N2, N3 і Xn; ізоляцію різних верств архітектури Network slicing і визначення для кожного шару власних рівнів безпеки; захист сигнального та призначеного для користувача трафіку між eNb мережі 4G-LTE і gNb мережі 5G в рамках «Option 3» сценарію міграції 4G до 5G, включаючи узгодження криптографічних ключів, шифрування і контроль цілісності; аутентифікацію користувача і захист трафіку на рівні кінцевих сервісів (IMS, V2X – Vehicle to Everything, IoT тощо).

В результаті проведених досліджень стало зрозумілим, що мережі 5G відіграватимуть в майбутньому поки що найбільш значущу роль в формуванні електронного суспільства, критичної інфраструктури тощо. Тому дуже актуальними і важливими є питання, пов'язані із забезпеченням інформаційної безпеки в майбутніх мережах 5G. Основні рушійні сили розвитку 5G, згруповані в чотири основні характеристики (нові моделі довіри, нові моделі служби доставки, розширений перелік загроз, і збільшення рівня конфіденційності) створюють визначальний вплив на підходи щодо формування вимог до систем безпеки та конфіденційності в мережах 5G.

**Література**

1. Бойко М. П. Системи стільникового зв'язку: конспект лекцій / М. П. Бойко. – Одеса: ОНАЗ, 2004. – 76 с.

2. Тихвинский В.О., Терентьев С.В., Юрчук А.Б. Сети мобильной святи LTE: технологии и архитектура. – М.: Эко-Трендз, 2010. – 284 с.: ил.

3. 5G Network Architecture 5G Network Architecture A High-Level Perspective.

*УДК 342.52*

**Петров С. Г.**
кандидат юридичних наук,
Служба безпеки України

## ДО СПІВВІДНОШЕННЯ ПОНЯТЬ ДЕРЖАВНІ І НАЦІОНАЛЬНІ ЕЛЕКТРОННІ ІНФОРМАЦІЙНІ РЕСУРСИ

У законодавстві України про кібербезпеку у 2017 році вперше було закріплено поняття «національні електронні інформаційні ресурси» як систематизовані електронні інформаційні ресурси, які містять інформацію незалежно від виду, змісту, форми, часу і місця її створення (включаючи публічну інформацію, державні інформаційні ресурси та іншу інформацію), призначену для задоволення життєво важливих суспільних потреб громадянина, особи, суспільства і держави [1; ст. 1]. При цьому, під електронними інформаційними ресурсами розуміється будь-яка інформація, що створена, записана, оброблена або збережена у цифровій чи іншій нематеріальній формі за допомогою електронних, магнітних, електромагнітних, оптичних, технічних, програмних або інших засобів [1; ст. 1].

Попереднє визначення, яке було закріплено у підзаконному нормативно-правовому акті, містило поняття «національні електронні інформаційні ресурси» як ресурси незалежно від їх змісту, форми, часу та місця створення, форми власності, призначені для задоволення потреб громадянина, суспільства, держави. Національні ресурси включають державні, комунальні та приватні ресурси [2].

Таким чином, до визначення поняття на рівні закону включено такі ознаки як «систематизованість» відповідних інформаційних ресурсів та включення усіх без винятку форма власності на такі ресурси. Крім того, акцентовано увагу на видовому різноманітті національних електронних інформаційних ресурсів, зокрема державні електронні інформаційні ресурси визначено одним із видів національних електронних інформаційних ресурсів.

Для органів державної влади України діє конституційний принцип «дозволено лише те, що передбачено законом». Тому розмежування двох понять «національні електронні інформаційні ресурси» та «державні електронні інформаційні ресурси» має не тільки науково-теоретичне, а й прак-

тичне значення. Наприклад, якщо повноваження СБ України визначаються законом по відношенню до державних електронних інформаційних ресурсів, то цілком зрозуміло, що вони не поширюються на приватні електронні інформаційні ресурси. Хоча останні і входять до обсягу поняття «національні електронні інформаційні ресурси».

Питання співвідношення двох понять актуалізується з розвитком національної системи кібербезпеки, оскільки впливають на формулювання повноважень державних органів. Так, поняття «об'єкти критичної інформаційної інфраструктури» не завжди потраплятиме до обсягу поняття «державні електронні інформаційні ресурси», але завжди – до обсягу поняття «національні електронні інформаційні ресурси». Відповідно, для цілей забезпечення кібербезпеки держави поняття «об'єкти критичної інформаційної інфраструктури» вважаємо інтеграційним для визначення повноважень державних органів, зокрема і СБ України, у сфері забезпечення кібербезпеки особи, суспільства, держави.

**Література**

1. Закон України від 05.10.2017 «Про основні засади забезпечення кібербезпеки України». Відомості Верховної Ради України, 10.11.2017, № 45, ст. 403.

2. Розпорядження Кабінету Міністрів України від 05.05.2003 р. № 259-р «Про затвердження Концепції формування системи національних електронних інформаційних ресурсів» // Офіційний вісник України. 2003, № 18, ст. 864.

*УДК 004.056.53*

**Плєц О. О.**
Національний технічний
університет «Дніпровська політехніка»
**Кручінін О. В.**
Національний технічний
університет «Дніпровська політехніка»

## АНАЛІЗ РЕАЛІЗАЦІЇ ОПТИКО-ЕЛЕКТРОННОГО КАНАЛУ ВИТОКУ ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ БЕЗПІЛОТНИХ ЛІТАЮЧИХ АПАРАТІВ

У зв'язку зі здешевленням та розвитком електронної компонентної бази та відносно вільного доступу для придбання безпілотних літальних апаратів (БПЛА) особливого значення набуває питання щодо нових варіантів реалізації за їх допомогою технічних каналів витоку інформації (ТКВІ). Одним із таких ТКВІ є оптико-електронний (ОЕ).

Як відомо, у загальному випадку технічний засіб розвідки (ТЗР) в ОЕ ТКВІ має у своєму складі передавальну та приймальну частини. Передавальна частина опромінює лазерним променем вібруючу поверхню (ВП), та може мати у своєму складі: блок формування сигналу, блок модулятора, блок випромінювача , оптичний модуль для фокусування променю та інші [2-5].

Існуючі ТЗР в ОЕ ТКВІ конструктивно можуть містити приймальну та передавальну частини в одному корпусі (моноблок) або в різних корпусах (багатокорпусні). Крім того, траєкторії падаючого та віддзеркаленого променю лазеру можуть співпадати або не співпадати [2-5]. Залежно від конструкції, для ефективної роботи існуючих ТЗР повинні виконуватись умови щодо розташування їх відносно ВП, а також взаємного розташування передавальної та приймальної частин для багатокорпусного типу. Загальною вимогою для ефективної реалізації ОЕ ТКВІ є встановлення ТЗР на приблизно однаковій висоті з ВП, тобто з об'єктом інформаційної діяльності (ОІД).

Слід зазначити, що сучасні технічні рішення, які використовують для створення ТЗР, дають змогу за сприятливих погодних умов вести розвідку з достатньо великої відстані (сотні метрів-кілометри).

Вище зазначені фактори враховуються при розробці моделі загроз для інформації від її витоку ОЕ ТКВІ на ОІД. Таким чином, для ОІД, які розташовані на великій висоті відносно оточуючих будівель та споруд, реалізацію ОЕ ТКВІ можна було вважати малоймовірною.

З появою БПЛА, таких як квадрокоптери, є змога розміщувати їх майже у будь-якій точці вільного простору. Інвестування у ринок БПЛА з кожним роком зростає. Враховуючи це, а також відсутність ефективних механізмів контролю за БПЛА, існує ймовірність використання їх для створення засобів розвідки.

БПЛА можуть підіймати у повітря не тільки себе, але і корисний вантаж, яким може бути ТЗР або його елементи. Таким чином, з'являється можливість реалізації нових варіантів схем ОЕ ТКВІ [1].

Варіант 1. Одна з частин ТЗР знаходиться у повітрі: передавальна частина може бути в повітрі, приймальна – на стаціонарній позиції або навпаки. При цьому висота розміщення стаціонарної позиції може бути значно нижче, ніж висота розміщення ОІД.

Варіант 2. Приймальна та передавальна частини обидві знаходяться у повітрі: на одному БПЛА при моноблочній конструкції ТЗР або на декількох БПЛА для багатокорпусних ТЗР.

Безумовно, для реалізації вказаних варіантів схем ОЕ ТКВІ необхідно забезпечити достатньо високу точність позиціонування та орієнтації БПЛА у просторі. Сучасні БПЛА обладнані цілим комплексом датчиків та технічних рішень для виконання зазначених умов: барометр, компас, дат-

чик вітру, гіроскоп, системи супутникової навігації, акселерометри, відеокамери та інше.

Крім того, гіроскопи можуть бути використані для стабілізації позиціонування та орієнтації самого ТЗР при застосуванні спеціалізованої системи його кріплення до корпусу БПЛА.

Слід зазначити, що ще одним фактором, який негативно впливає на ефективність ТЗР в ОЕ ТКВІ, є власні вібрації БПЛА від працюючих двигунів. Але можна припустити, що ці вібрації мають періодичну характеристику, і їх вплив може бути скомпенсований шляхом подальшої цифрової обробки отриманих сигналів.

Таким чином, на сьогодні можна припустити, що технічна задача використання БПЛА в якості носія ТЗР для ОЕ ТКВІ є цілком реальною для реалізації.

З появою БПЛА виникла можливість реалізації нових схем ОЕ ТКВІ. Для визначення можливості практичної реалізації зазначеного ТКВІ на основі проаналізованих матеріалів та висунутих допущень необхідні подальші теоретичні та експериментальні дослідження. У разі підтвердження можливості ефективної реалізації ОЕ ТКВІ з використанням БПЛА результати цих досліджень повинні бути враховані при розробці моделі загроз для комплексів технічного захисту інформації. Також це може призвести до необхідності перегляду існуючих моделей загроз.

**Література**

1. ardupilot-mega [Електронний ресурс] – Режим доступу: http://ardupilot-mega.ru/index.php/manuals.

2. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. – М.: Гостехкомиссия России, 1998.

3. Хорев А.А. Способы и средства защиты информации. – М.: МО РФ, 2000.

4. Заболотный В.И. Модель отражающей поверхности лазерного канала разведки информации / В.И. Заболотный, Ю.А. Ковальчук // Прикладная радиоэлектроника. – 2007. – Т. 6. № 3. – С. 432-434.

5. Заболотний В.І. «Безшумний» захист від «лазерних мікрофонів» / В.І. Заболотний, Ю.О. Ковальчук // Прикладная радиоэлектроника. – 2009. – Т. 8. № 3. С. 377-381.

*УДК [004.42+005.6]:378.1*
**Придатко О. В.**
кандидат технічних наук, доцент,
Львівський державний університет безпеки життєдіяльності
**Малець І. О.**
кандидат технічних наук, доцент,
Львівський державний університет безпеки життєдіяльності

# РЕАЛІЗАЦІЯ ПРОЄКТУ «РОЗУМНИЙ УНІВЕРСИТЕТ» ЯК СКЛАДОВА ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ОСВІТНЬОГО СЕРЕДОВИЩА

Тенденції цифрової трансформації суспільства набувають широкого розповсюдження та охоплюють більшість галузей економіки та сфер діяльності суспільства. На сьогодні важко уявити своє життя без використання smart-технологій у повсякденному житті. Звичайно, осторонь цифрова трансформація не обійшла і осередок вищої освіти в Україні. Підтвердженням цього є успішна багаторічна ініціатива електронного вступу до закладів вищої освіти (ЗВО) [1], облік студентів, науково-педагогічних працівник та матеріально-технічного оснащення через Єдину державну електронну базу освіти [2] тощо. До загальнодержавних тенденцій, які є обов'язковими для запровадження і використання у ЗВО, додаються і локальні ініціативи. Більшість ЗВО розробляють власні або закуповують інформаційні системи, що дозволяють полегшити процес організації та адміністрування освітнього процесу, покращити умови навчання, підвищити якість забезпечення вищої освіти тощо. Не виключенням став і Львівський державний університет безпеки життєдіяльності, де студенти спеціальностей галузі знань 12 «Інформаційні технології» в рамках вивчення профільних курсів та спільної реалізації проєкту «Розумний університет» розробляють низку інформаційно-пошукових, довідкових та інтегрованих систем, що підвищують комфорт перебування студентів у закладі освіти та інтегрують їх до цифрової глобалізації.

Проєкт «Розумний університет» об'єднує усі ініціативи, що пов'язані з розробкою інтелектуальних, інформаційних, пошукових та довідкових систем націлених на розвиток і підтримку комфортних умов навчання у Львівському державному університеті безпеки життєдіяльності. Проєкт включає в себе багаторічні ініціативи, зокрема розробка та підтримка дистанційної освітньої платформи де здобувачі вищої освіти отримують постійний віддалений доступ до освітнього контенту (теоретична, практична, лабораторна база, література, відеоконтент, консультації, спілкування з викладачем в режимі реального часу, контроль отриманих знань тощо).

До переліку ключових компонент проєкту також можна віднести реалізовану студентами інформаційно-довідкову систему «UniBell». Основне

призначення цієї системи полягає у відображенні розкладу занять на мобільних пристроях за різними критеріями пошуку: для викладача; для навчальної групи; для навчальної аудиторії. Пошукова система надає можливість здійснювати пошук актуального розкладу на день, на визначену дату або ж за вказаним діапазоном дат. Додаток наділений можливістю сканування індивідуального QR-коду аудиторії в режимі реального часу, на підставі чого готує інформацію про заняття (дисципліну), викладача та групу, які знаходяться в аудиторії у даний момент часу.

Науковим товариством студентів та ініціативною групою здобувачів освіти також розробляється низка допоміжних сервісів в сфері забезпечення безпеки людини. Зокрема розроблено демо-версію та проводиться розгортання серверної частини додатку «Find safe place», що дозволятиме здійснювати пошук найближчого об'єкту укриття та будувати маршрут слідування у разі виникнення надзвичайної ситуації. Сповіщення про надзвичайну ситуацію також проводиться через додаток із відображенням зони ураження. Сервіс наділений «соціальною» компонентою, яка дозволяє відслідковувати місце знаходження та маршрут руху близьких людей, а також спілкуватись з ними у вбудованому чаті або сповістити їх про небезпеку.

В рамках навчання за освітньою програмною «Комп'ютерні науки» курсанти та студенти генерують унікальні ідеї та створюють власні робототехнічні системи на базі апаратних обчислювальних платформ Arduino. Зокрема на етапі реалізації знаходяться тепловізор для пошуку постраждалих під завалами зруйнованих будівель та система «Безпечний будинок», що націлена на запобігання накопичення вибухонебезпечної концентрації природнього газу та смертельної концентрації чадного газу у приміщенні в наслідок несправності газових побутових приладів. Остання система окрім виконання запобіжних заходів (зменшення концентрації небезпечного середовища) також спроможна здійснювати інформування визначених абонентів про витік природнього або чадного газу у квартирі.

Цифрова трансформація, що представлена у вигляді проєкту «Розумний університет» торкнулась не лише студентських ініціатив. В рамках означеного проєкту на випускових кафедрах Університету запроваджуються системи електронного адміністрування та менеджменту через систему управління завданнями Trello та спільного доступу і редагування кафедральної документації через хмарні сервіси (Google-диск, Dropbox тощо). Означені сервіси допомагають спростити процеси документообігу, постановки завдань та контролю їх виконання, миттєвого реагування на проблемні питання тощо.

Отже, як випливає з тезисного опису основних освітніх ініціатив у Львівському державному університеті безпеки життєдіяльності цифрова трансформація освітнього середовища націлена на підвищення комфорту

та ефективності самоорганізації освітнього процесу для усіх стекголдерів та адаптує освітнє середовище до світових тенденцій цифрової глобалізації.

**Література**

1. Порядок подання та розгляду заяв в електронній формі на участь у конкурсному відборі до закладів вищої освіти України в 2019 році : Наказ Міністерства освіти і науки України від 11 жовтня 2018 року № 1096.

2. Положення про Єдину державну електронну базу з питань освіти : Наказ Міністерства освіти і науки України від 08 червня 2018 року № 620.

*УДК 342.1*

**Прозоров А. Ю.**
кандидат юридичних наук
Національна академія СБ України

## ПРАВОПОРУШЕННЯ У СФЕРІ ВИКОРИСТАННЯ БАНКІВСЬКИХ ПЛАТІЖНИХ КАРТОК ПРИ ПРОВЕДЕННІ БЕЗКОНТАКТНИХ ТА ІНТЕРНЕТ ПЛАТЕЖІВ

Розвиток інформаційних технологій призвів до істотних змін функціонування у тому числі й банківської сфери, зокрема виникла така нова форма розрахунків за товари та послуги як безготівкові операції, кількість яких з часом лише збільшується. З метою приведення законодавчої бази у відповідність до сучасних вимог безпечного функціонування інформаційних технологій органами державної влади України було внесено зміни до низки нормативних актів. Так, відповідно до постанови правління Національного банку України від 25 листопада 2016 року № 407, якою, власне, вносяться зміни до постанови № 210 «Про встановлення граничної суми розрахунків готівкою» підприємства (підприємці) під час здійснення розрахунків зі споживачами за товари, роботи, послуги на суму понад 50 000 гривень повинні проводити такі операції в безготівковій формі [1]. Водночас, зазначена форма розрахунків не залишилась поза увагою злочинців. На прес-брифінгу, присвяченому безпеці безготівкових операцій, начальник відділу протидії злочинам у сфері платіжних систем Департаменту кіберполіції Національної поліції України М. Вольвак наголосив, що протягом 2017 року кіберполіцейськими задокументовано 3820 кіберзлочинів, з них пов’язаних з платіжними картками, включаючи скіммінг, банкоматні злочини – 1330, і це на 70% більше, ніж у 2016 році. За його словами, найбільш поширене правопорушення у цій сфері – це встановлення скіммінгових пристроїв на банкомати, за допомогою яких кіберзлодії копіюють інформацію, нанесену на платіжну картку, та встановлюють

відеонагляд з метою копіювання пін-коду з подальшим виготовленням дублікатів та списанням грошових коштів. Ще одними з найбільш поширених кіберзлочинів у платіжній сфері є вірусне зараження банкоматів, за допомогою якого кіберзлодій подає команду на видачу готівки з банкомату, а також несанкціоноване списання коштів за допомогою інтернет-банкінгу. При цьому, він зазначив, що в разі своєчасного повідомлення кіберполіції, упродовж доби-двох, поліцейські можуть здійснити блокування даних грошових коштів, звернувшись до представників банку. В разі запізнілого звернення встановити організаторів злочинів і повернути власникам вкрадені гроші буде вкрай важко [2].

На нашу думку, зазначений перелік кіберзлочинів, пов'язаних з банківськими платіжними картами, не є вичерпним. Так, окремої уваги потребують питання запобігання таким новим протиправним діям у кіберпросторі як фішинг, вішинг та фармінг.

Фішинг (англ. phishing, від fishing – «рибалка») – це вид інтернет шахрайства, метою якого є виманювання у довірливих або неуважних користувачів персональних даних клієнтів онлайнових аукціонів, сервісів з переказу або обміну валюти, інтернет магазинів. Особливість фішингу полягає в тому, що злочинці незаконно отримують таку інформацію через створення так званих сайтів клонів провідних бізнес кампаній [3].

Вішинг (англ. vishing, від англ. voice – «голос», fishing – «рибалка») є різновидом інтернет-шахрайства, при якому зловмисники заволодівають по телефону, в більшості випадків під виглядом представників банку, конфіденційною інформацією про дані картки з її подальшим протиправним використанням [4].

Фармінг (англ. pharming) – це вид Інтернет шахрайства, що полягає в організації зловмисниками злочинного механізму прихованого перенаправлення жертви на хибну IP-адресу, з використанням навігаційної структури (файл hosts, система доменних імен (DNS)) [5].

Адекватною реакцією нашої держави на виникнення зазначених кіберзагроз стала створення у складі МВС України нового підрозділу – кіберполіція.

Нарешті в чинному законодавстві, зокрема, у Положенні Національного банку України «Про організацію заходів із забезпечення інформаційної безпеки в банківській системі України» від 28 вересня 2017 року № 95 (надалі – Положення) з'явилась термінологія у сфері кіберзагроз в банківської сфері, що дозволяє ідентифікувати неправомірні дії, які проводяться з використанням інформаційних технологій, та розробити організаційні та правові засади з їх виявлення, попередження та припинення. В Законі України «Про основні засади забезпечення кібербезпеки України» нарешті дано визначення терміну кіберзлочин (комп'ютерний злочин) – суспільно-небезпечне винне діяння у кіберпросторі та/або з його використанням,

відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами [6].

Не зважаючи, на прийняття Закону України «Про основні засади забезпечення кібербезпеки України», Положення та низки інших нових нормативних актів України, спрямованих на протидію кіберзлочинності, її рівень в нашій державі фактично не зменшується. Таке становище потребує адекватного реагування як з боку держави в особі органів законотворчої та виконавчої влади, правоохоронної системи, так й в цілому суспільства та особи. Кожний з перелічених суб'єктів за умов злагодженої взаємодії між собою вживати на своєму рівні вичерпних заходів із запобігання цьому негативному явищу, що фактично створюватиме передумови до його мінімізації. Стрімкий розвиток інформаційних технологій обумовлює регулярне виникнення нових видів кіберзлочинів, у тому числі у банківській сфері, через що спостерігається тенденція постійного відставання та застарілості статей кримінального та адміністративного права, якими передбачено такі протиправні дії. Це фактично викликає потребу в уніфікації та узагальненні правових норм у сфері протидії кіберзлочинності. В цьому контексті, на нашу думку, доцільно б було запропонувати внести зміни до Кримінального кодексу України шляхом заміни назви розділу XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» Кримінального кодексу України на «Кіберзлочини».

**Література**

1. Покупки не дороже 50 тысяч: НБУ ограничивает сумму расчетов наличными для физлиц [Електронний ресурс]. – Режим доступу: http://www.segodnya.ua/economics/enews/pokupki-ne-dorozhe-50-tysyach-nbu-ogranichivaetsummu-raschetov-nalichnymi-dlya-fizlic-785316.html.

2. Укрінформ [Електронний ресурс]. – Режим доступу: https://www.ukrinform.ua/rubric-society/2392710-top5-zlociniv-iz-platiznimi-kartkami-eksperti-skazali-ak-zapobigti.html.

3. Вікіпедія «Фішинг» [Електронний ресурс] / Фішинг. – Режим доступу: http://www.uk.wikipedia.org/wiki/Фішинг/.

4. Вікіпедія «Вішинг» [Електронний ресурс] / Вішинг. – Режим доступу: http://www.uk.wikipedia.org/wiki/Вішинг/.

5. Вікіпедія «Фармінг» [Електронний ресурс] / Фармінг. – Режим доступу: http://www.uk.wikipedia.org/wiki/ Фармінг/.

6. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. № 2163-VIII [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2163-19.

*УДК 342+32.019.5:659.4*
**Радзієвська О. Г.**
кандидат юридичних наук,
НДІ інформатики і права НАПрН України

# ІНФОРМАЦІЙНІ ТА ПСИХОЛОГІЧНІ ОПЕРАЦІЇ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ СУСПІЛЬСТВА ТА ДЕРЖАВИ

Широке залучення інформаційно-комунікаційних технологій до усіх суспільних процесів у сучасному світі призводить до трансформації суспільства та держави. Домінування інформаційної складової у забезпеченні функціонування усіх сфер життя та діяльності сучасної людини і суспільства потребує додаткових зусиль у забезпеченні інформаційної безпеки. Сама інформаційна безпека стає вагомою складовою забезпечення національної та міжнародної безпеки.

Інформаційні та психологічні операції, які ще недавно розглядалися як допоміжні складові у військовому протистоянні, нині займають одне з основних місць у системі стратегічних комунікацій держави, а протидія їм є значимим елементом у забезпеченні інформаційної та національної безпеки.

З розвитком технологій інформаційні та психологічні операції стають дедалі складнішими, багаторівневими, їх сфера застосування урізноманітнилась, а інструментарій – значно розширився. Інтенсивність застосування інформаційних і психологічних операцій в суспільно-політичній, економічній, військовій та інших сферах нині набуває таких масштабів, що становить загрозу існування самої держави та її інститутів.

Очевидно, що система протидії подібним загрозам повинна виходити із наявних викликів, застосовувати відповідний інструментарій та трансформувати методи та засоби своїх дій у відповідності до рівня та сутності небезпеки. Однак на сьогодні жодна держава світу не є повністю убезпечена в інформаційній сфері. Проблеми організаційно-правого та технікотехнологічного забезпечення інформаційної безпеки пов’язані перш за все з надзвичайно інтенсивними трансформаціями суспільних відносин та інформаційно-комунікаційних технологій. Проте існує низки системних проблем у формуванні ефективної системи інформаційної безпеки.

Перше, про що слід було б говорити, – це відсутність системного моніторингу та аналізу застосування багаторівневих інформаційних та психологічних операцій довготермінової дії. Наприклад, використання багаторівневих довготермінових емоційно забарвлених інформаційних впливів направлених на масову свідомість з «розмитим» закінченням вважалися характерними рисами пропаганди. Інформаційні та психологічні операції визначалися діаметрально протилежними характеристиками. Однак,

трансформація цілей, засобів та методів ведення операцій в інформаційній сфері надала їм інших характеристичних властивостей, тим самим замаскувавши їх під пропаганду. Це ускладнило процес виявлення, аналізу та нейтралізації довготривалих, суспільно небезпечних інформаційних загроз.

По-друге, відсутність системи моніторингу загроз на нових інформаційних платформах, зокрема, у соціальних мережах. Надзвичайно небезпечними є інформаційні операції щодо формування політичних вподобань та нових наративів. Серед основних чинників, які створюють можливість для ефективного проведення інформаційних та психологічних операцій слід відзначити недосконаліть системи формування запиту на інформацію, а також широке використання систем з елементами штучного інтелекту, зокрема інтернет-ботів, під час комунікації користувачів.

Наприклад, одним із чинників, які створюють умови для проведення спеціальних інформаційних та психологічних операцій проти суспільства та держави, є притаманна мережі Інтернет система «запит-відповідь». Технологічно система «запит-відповідь» у мережі налаштована так, що на запит інформації отримується найбільш популярна відповідь, яка може бути згенерована штучно, а відповіді не верифікуються і не модеруються.

Значна частина інформації у мережі продукується інтернет-ботами, тобто створена автономними програмами, здатними виконувати прості одноманітні завдання. До такого висновку прийшли фахівці з Оксфордського інституту інтернету (Oxford Internet Institute) проаналізувавши політичний контент мереж Facebook і Twitter. Інтернет-боти стають сьогодні суттєвим інструментом впливу на формування політичної думки, культури, цінностей та основою для трансформацій у політико-правовій системі держави, однак все ще залишаються поза її нормативно-правовою базою та системним моніторингом.

Надзвичайна популярність сучасних інформаційних платформ здатна формувати нові суспільні наративи. Наративність є системотворчим елементом самого суспільства, людини та впорядкованості навколишнього світу. Привнесення наративу допомагає узгодити та стабілізувати будь-яку соціальну систему, а його відсутність, або невизначеність створює хаос в індивідуальному і суспільному світосприйнятті та дезорієнтацію у суспільстві. Дестабілізація у суспільстві становить загрозу національним інтересам, національним цінностям та існуванню самої держави.

Підсумовуючи, слід зазначити, що система забезпечення протидії інформаційним і психологічним операціям на разі є недостатньо сформованою через відсутність системного бачення у забезпеченні інформаційної безпеки та у виявленні й нейтралізації існуючих загроз у коротко- та довготривалій перспективі. Швидкість впровадження нових технологій при інтенсифікації інформаційного протистояння на всіх рівнях і в усіх сферах

суспільного життя не дозволяє нині ефективно протистояти інформаційно-психологічним операціям, інформаційній експансії та інформаційній агресії загалом. Правові механізми протидії інформаційним і психологічним операціям у сучасній державі повинні будуватися, трансформуватися і оновлюватись у відповідності до реальних загроз в інформаційній сфері, працювати на випередження та основуватись на принципах верховенства права, дотримання прав, свобод та безпеки людини і громадянина, суспільства і держави.

*УДК 519.7*

**Радов Д. Г.**
кандидат економічних наук,
Воєнно-дипломатична академія
імені Євгенія Березняка

## ІНТЕЛЕКТУАЛЬНА ЗБРОЯ: МАЙБУТНЄ ШТУЧНОГО ІНТЕЛЕКТУ У ВІЙСЬКОВІЙ СФЕРІ

Сучасний світ практично пронизаний поняттям штучного інтелекту (ШІ), яке використовується в повсякденному лексиконі, засобах масової інформації, в економіці, промисловості, науковій сфері.

Не оминула ця тенденція стороною і військову сферу – звичними стали терміни «інтелектуальні боєприпаси», «роботизована військова система з елементами штучного інтелекту» тощо.

Динамічні зміни основ військової стратегії й тактики, які ми спостерігаємо сьогодні, свідчать про якісні зміни сучасного поля бою. Стрімке скорочення часу на прийняття критичних рішень поряд зі створенням більш досконалих засобів доставки винесли на порядок денний питання щодо першочергового розвитку систем бойового управління. Останні конче потрібні війську, щоб контролювати зазначені процеси та перебіг бойових дій загалом.

Найперше відзначається критичне зростання просторово-часового чинника в сучасному бою, а отже, на всіх рівнях військового ланцюжка стає актуальним питання максимального скорочення часу реакції на загрози.

Нове дослідження Дослідницької лабораторії ЗС США (Army Research Lab) спрямоване на поліпшення взаємодії між військовим та тим озброєнням чи технікою, яке потребує контролю людини. Зокрема, йдеться про створення нових систем штучного інтелекту, що будуть здатні зчитувати думки військового. «Наше бачення технології полягає в тому, щоб закрити петлю між системою та військовим. Система має розуміти, що відбувається з її оператором та робить висновки, засновані на фізіологіч-

ному стані бійця, а також застосувавши вже відпрацьовані на тренуваннях знання», – описує технологію представник Дослідницької лабораторії Майк Лафіандра [1].

Ключові принципи та можливості штучного інтелекту у військовому секторі [2]:

комплексний і всебічний аналіз ситуації на певних ділянках місцевості, де проводиться військова операція;

повномасштабна координація польових штабів і військових підрозділів між собою;

можливість шифрованої передачі даних;

автоматизація бойової техніки, що може діяти автономно в рамках запланованих операцій;

посилення боєздатності солдат за рахунок використання розумних натільних пристроїв;

ефективний аналіз дій супротивника і прогнозування відповідної атаки ворога;

контроль місцевості, пошук боєприпасів і виявлення потенційно небезпечних зон.

На сьогоднішній день експерти виокремлюють і акцентують увагу на наступних видах кібератак, що можуть завдати шкоди плануванню і проведенню будь-якої військової операції, коли мова йде про мережеві методи оперування стратегічною інформацією [3]:

атаки, що спрямовані на відмову в обслуговуванні користувачів мережі (DDoS);

атаки, що спрямовані на отримання доступу до захищеної інформації через вразливості мережі.

Наразі, шляхом проведення багатьох тестувань, доведено, що системи тактичного штучного інтелекту можуть суттєво мінімізувати наслідки вище зазначених атак завдяки алгоритмам машинного навчання. ШІ може не лише розпізнавати потенційну загрозу, але й завчасно блокувати доступ до ресурсу саме тим пристроям, які його атакують. Притому, варто враховувати, що розумні системи здатні вчитися та аналізувати, тож, кожного наступного разу вони вже не просто включаються в автономну боротьбу із загрозою, а заздалегідь попереджають про неї. Таким чином, у перспективі подібні ризики можуть бути фактично повністю виключені.

Крім того, ШІ здатен проводити аналіз вразливості програмного забезпечення, використовуючи технологію фазингу (Fuzzing), що дає можливість досить швидко знаходити та нейтралізувати критичні вразливості будь-якої системи і координувати атаки на ворожу інфраструктуру. Це дозволяє використовувати інтелектуальні машини не тільки для захисту, а й для нападу.

**Література**

1. У США розробляють штучний інтелект для взаємодії військового та озброєння. URL: http://opk.com.ua/ (дата звернення: 27.02.2020).

2. Переваги цифровізації оборонного комплексу і стратегічний вплив розумних технологій на військовий сектор. URL: https://www.everest.ua/ai-platform/analytics/perevahy-tsyfrovizatsiyi-oboronnoho-kompleksu-ta-stratehichnyy-vplyv-rozumnykh-tekhnolohiy-na-viyskovyy-sektor/ (дата звернення: 27.02.2020).

3. Борохвостов І. В., Білокур М. О. Визначення критеріїв та методів оцінювання шляхів забезпечення військових формувань озброєнням та військовою технікою. *Озброєння та військова техніка.* Київ. 2018. № 3(19). С. 3-8.

*УДК 681.5(042.3)*

**Семко В.В.**
доктор технічних наук,
Національна академія СБ України
**Гулак Г. М.**
кандидат технічних наук,
Національна академія СБ України
**Семко О. В.**
кандидат технічних наук,
Інститут телекомунікацій та глобального
інформаційного простору НАН України,

## ВІРТУАЛІЗАЦІЯ ПРОСТОРУ ФУНКЦІОНУВАННЯ КОНФЛІКТУЮЧИХ СЕНСОРНИХ МЕРЕЖ

Доцільність застосування методів інтелектуального управління маршрутизацією потоків даних (ПД) в сенсорних мережах (СМ) ВТ за умов забезпечення вимог гарантоздатності визначається при вирішенні проблем, які виникають при створенні відповідних систем управління (СУ) вузлами мережі. При цьому СУ кожного вузла є складовою частиною розподіленою динамічної СУ маршрутизацією ПД в СМ.

Сутність вирішення задачі синтезу і вибору рішення щодо інтелектуального управління маршрутизацією ПД в децентралізованих СУ мережами при забезпеченні інформаційної взаємодії вузла-відправника і вузла-отримувача даних полягає вирішенні задачі динамічної дискретної оптимізації.

Синтез управління маршрутизацією ПД в СМ здійснюється в віртуальному параметричному просторі функціонування мережі, що враховує щільністю навантаження каналів ПД, властивості взаємного переміщення, невизначеності, завади, навантаження на обчислювальне середовище вузлів мережі, тощо. Зазначені параметри віртуального простору функціону-

вання СМ дозволяють формально визначити додатню функцією ціни при синтезі і виборі рішень щодо управління маршрутизацією ПД.

Математичну модель функціонування СМ можна представити у вигляді зв'язного графу

$$G = (V, E), \quad (1)$$

де $V$ – множина вузлів графа, що представляє СМ, $E$ – множина ребер графа,що з'єднує вузли і відображає можливий маршрут ПД.

Кожному ребру $e_{ij} \in E \forall \{i, j\} \in V$ графа $G$ поставлено у відповідність невід'ємне число $c_{ij} \geq 0$, що визначає пропускну здатність ребра, як функція ціни при передачі ПД. Введемо таке поняття ПД $f$ між вершинами $s$ і $t$, яка є додатньою функцією на ребрах графа $G$ $f_{ij} \geq 0$ за умови того, що ПД не накопичується в проміжних вузлах мережі між вузлами $s$ і $t$, тобто

$$\sum_k f_{ki} = \sum_j f_{ij}, \forall i \in V, i \neq \{s, t\} \quad (2)$$

і не перевищує пропускної спроможності каналу ПД , а саме $f_{ij} \leq c_{ij}$ і $e_{ij} \in E$. Залишкова пропускна здатність ребра $e_{ij}$ визначається як різниця пропускноїздатності ребра і ПД по ньому, тобто $c_{ij}^f = c_{ij} - f_{ij}$.В такому разі з графу мережі $G$ отримуємо залишкову мережу $G' = (V, E^f)$,в якій залишаються ребра з додатною залишковою пропускною спроможністю.

Виникненні ПД в СМ визначається як поява заявки в мережі між парою вершин з множини $\{\{s_1, t_1\}, \ldots \{s_n, t_n\}\}$ полюсів. Час життя заявок обмежений обслуговуванням заявок за умови встановленого маршруту ПД між вузлами СМ. Тим самим забезпечується вивільнення пропускної спроможності ребер СМ у випадку обслуговування заявки на обслуговування(маршрут між вузлами мережі був прокладений).Множина ПД між кожною парою вузлів через проміжний $m$-й вузол можна визначити як продукт $\{s_m, t_m\}$ ы назвати продуктом $v_m$.

В якості обмеженого ресурсу СМ, що визначає функцію ціни, обрано пропускну спроможність каналів зв'язку, які визначають ребра (дуги) моделі мережі $G$ (1).

Множина ребер, видалення яких розриває мережу на кілька незв'язних між собою частин таким чином, що полюса знаходяться в різних частинах мережі, визначає множину $\Re_m$ – множину мінімальних розрізів кожного продукту $v_m$ та пропускну спроможність цих розрізів – $R_m$. В такому разі вирішення задачі мережі дискретної динамічної оптимізації при взаємодії конфліктуючих вузлів СМ ПД з використанням евристичного алгоритму інтегрального усікання варіантів зводиться до пошуку маршруту ПД найменшої вартості, причому значення вартості присвоюються ребрам мережі в залежності від кількості мінімальних розрізів продукту і пропускної спроможності мережі, а також кількості елементів (*hops*) синтезованого маршруту.

Залежно від способу визначення вартості дуг моделі мережі, для визначення функції ціни застосовується субоптимальний мінімально-розрізний алгоритм, що орієнтований на синтез і вибір маршруту ПД з застосуванням ребер

граф-моделі СМ, які мають найбільший резерв пропускної спроможності каналів і мінімальну кількість елементів синтезованого маршруту. Такий алгоритм забезпечує обслуговування найбільшої кількості заявок.

Відповідно моделі (1) при синтезі і виборі стратегії управління маршрутизацією визначається додатня функція ціни (2).

Найбільш значущими параметрами, що характеризують функціонування каналу ПД при взаємодії вузлів СМ є залишкова пропускна здатність каналу передачі даних між вузлами мережі, який відображає ребро графа мережі (1), і враховує значенням корегуючої віртуальної відстані до *j-го* вузла СМ $\Delta d_{ij}$.

Тим самим, рішення задачі синтезу і вибору оптимального маршруту ПД буде здійснюватись у віртуальному просторі $Q$.

В загальному вигляді при взаємодії*i*-говузла з *j*-м вузлом мережі значення $d^{ij}$ може бути визначено як

$$d^{ij} = C^{ij}_{зад} d^{ij}_{зад} + C^{ij}_{□} \Delta d^{ij} + C^{ij}_{звірт} d^{ij}_{звірт}, \qquad (3)$$

де $d^{ij}_{зад}$ – відстань взаємодії *i-го*вузла при інформаційній взаємодії з *j*-м вузлом СМ під час визначення маршруту ПД; $\Delta d^{ij}$ – невизначеність, яка враховує динамічність *i-го* вузла і параметрів каналів ПД; $d^{ij}_{звірт}$ – віртуальна відстань, що враховує прогноз і невизначеність взаємного переміщення вузлів СМ.

Віртуальна відстань при синтезі і виборі оптимального маршруту ПД в СМ є адитивним критерієм відбору, для якого згідно (3) має виконуватись умова $C^{ij}_{зад} + C^{ij}_{□} + C^{ij}_{звірт} = 1$.

В загальному вигляді значення $\Delta d^{ij}$ для $k$ – мірного простору $Q$ визначається співвідношенням

$$\begin{cases} \Delta d^{ij} = \sqrt{\sum_{j=1}^{k} \left( \left| \Delta x^i_j \big|_{t=t0} - \Delta x^i_j \big|_{t=0+□t} \right| - \left| \Delta x^i_j \big|_{t=0-□t} - \Delta x^i_j \big|_{t=t0} \right| \right)^2 \frac{\Delta t^2}{2}} + d^k_{ij} + \Delta d^k_{ij} \\ □x^i_j = \left| \left( x^i - x^j \right) \big|_{t=t0} - \left( x^i - x^j \right) \big|_{t=0+□t} \right| \end{cases}, \qquad (4)$$

де $x^i$ – координати вузла-відправника *i*в $k$ – мірному просторі $Q$, $x^j$ координати вузла-отримувача *j*в $k$ – мірному просторі $Q$, $\Delta t$ – інтервал часу вимірювання, $d^k_{ij}$ – корегуюча відстань за методом уточнення місцезнаходження вузла *RSSI*до *j-го* вузла СМ (*RSSI*); $\Delta d^k_{ij}$ – корегуюча віртуальна відстань до *j-го* вузла СМ, що враховує властивості каналу ПД та завантаженість обчислювальних ресурсів *j-го*вузла мережі.

В загальному випадкукорегуюча віртуальна відстань $\Delta d^k_{ij}$ визначається функцією

$$\Delta d^k_{ij} = z(n, s), \qquad (4)$$

де $n$ – кількість запитів до вузла СМ, $s$– швидкість передачі даних.

Визначивши величину додаткового затухання, в СУ вузла СМ обчислюється значення корегвуючої відстані від *i*-го вузла до інших *j-тих* вузлів мережі

$$d_{\text{ij}}^{k} = \left( d_{ij}^{l} \right)^{\frac{k-\square}{k}} \left( \frac{4\pi\eta}{c} \right)^{\frac{\square}{k}}, \qquad (5)$$

де $d_{\text{ij}}^{k}$ – корегвуючої відстані від *i*-го вузла до інших *j*-тих вузлів мережі, що визначена за метолом уточнення місцезнаходження по індикації рівня отримуємого сигналу *RSSI*; $d_{ij}^{l}$ – локальна відстань до *j*-тих вузлів мережі; $k$ – коефіцієнт послаблення; $\square$ – додаткове затухання; $\eta$ – частота сигналу; $c$ – швидкість світла.

Тим самим за наявністю залишкової пропускної здатності каналу зв'язку можна в якості додаткового критерія відбору визначити сумарну затримку сигналу в маршруті ПД, що визначається значенням $\Delta d_{ij}^{k}$ в співвідношенні (3).

Обчислення значення $d_{звірт}^{ij}$ в $k$ - мірномувіртуальному просторі $Q$ здійснюється за співвідношенням

$$\begin{cases} d_{вірт}^{ij} = x_j^i + v_j^i \square t + \square v_j^i \dfrac{\Delta t^2}{2} \\ v_j^i = \dfrac{\sqrt{\sum\limits_{m-1}^{k} \left( x_m^i - x_m^j \right)^2}}{\square t} \\ x_j^i = \sqrt{\sum\limits_{m-1}^{k} \left( x_m^i - x_m^j \right)^2} \\ \square v_j^i = \dfrac{v_j^i \big|_{t=t0} - v_j^i \big|_{t=t0+\square t}}{\square t} \end{cases}, \qquad (6)$$

де $x_m^i$ – $m$-та координата вузла $i$, $x_m^j$ – $m$-та координата вузла $j$, $v_j^i$ – швидкість зближення/віддалення вузлів $i$ і $j$, $\Delta v_j^i$ – прискорення зближення/віддалення вузлів $i$ і $j$.

Виходячи з формального опису математичних моделей взаємодії вузлів СМі синтезу та прийняття рішень щодо стратегій управління маршрутизацією ПД, визначимо мінімально-перебірну процедуру синтезу і вибору рішення на основі методу інтегрального усікання варіантів у відповідності до критерію оптимальності $\Phi$, який фактично є адитивним критерієм вибору, що визначається співвідношенням

$$\Phi = \sum_{i=1}^{k} C_i \lambda_i, \forall \lambda_i = \frac{\Delta u_i}{\sup \left| u_i \right|}, \forall \lambda_i \in \lambda, \sum_{i=1}^{k} C_i = 1. \qquad (7)$$

Значення коефіцієнтів $C_i$ в співвідношенні (7) визначається для кожного виду конфліктів окремо. $\lambda_i$ визначає «витрати на управління» параметрами функціонування СМ згідно стратегії (2) на множині ребер граф-

моделі СМ $G$ за рахунок управління $u_i$ для $i$-го елемента маршруту ПД в просторі $Q$.

В такому разі задачу синтезу управління можна сформулювати як конфлікт взаємодії об'єктів (вузлів СМ) графу мережі $G$ в просторі $Q$

$$K = \left\langle M, A, \Gamma_{пр}, G, \mu \right\rangle, \tag{8}$$

а процедуру синтезу стратегій рішення конфлікту $\mu$ згідно принципу оптимальності $\chi$, який реалізовує вимоги критерію $\Phi$, можна представити у вигляді

$$\begin{cases} K = \left\langle M, A, \Gamma_{пр}, G, \mu \right\rangle \\ \chi K = \mu \end{cases}. \tag{9}$$

Вибір оптимальної стратегії рішення конфлікту $\mu^*$ з врахуванням правила зупинки $\Gamma_{зуп}$ формулюється в вигляді $\mu^* = \inf_{\chi, \Gamma_{зуп}} K$, що є постановкою задачі опису конфлікту взаємодії об'єктів та синтезу оптимального рішення в просторі $Q$.

# УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА ЗАХИСТІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

*УДК 316.77*
**Аблазов І. В.**
кандидат психологічних наук, доцент
**Рубель К. В.**
кандидат історичних наук, доцент,
Воєнно-дипломатична академія
імені Євгенія Березняка

## ТЕНДЕНЦІЇ РИНКУ PR-ПОСЛУГ ТА ЇХ ВПЛИВ НА СТАН ДЕРЖАВНО-ПРИВАТНОГО ПАРТНЕРСТВА У СФЕРІ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ

Міжнародний та вітчизняний досвід використання державно-приватного партнерства (public-private partnership, ДПП) є свідченням того, що ДПП є інструментом партнерської, рівноправної та взаємовигідної співпраці між державою, територіальними громадами, органами державної влади чи місцевого самоврядування та бізнесом. Розвиток державно-приватного партнерства є одним з ключових трендів у вирішенні більшості нагальних проблем сучасності. ДПП являє собою тип взаємовідносин між державним та приватним секторами, який на цей момент визнано найбільш оптимальним для сфери захисту безпекових об'єктів, в тому числі навіть об'єктів критичної інфраструктури у країнах з розвинутою ринковою економікою та високою правовою культурою, до кола яких прагне долучитися і Україна. На цьому принципово наголошено у резонансній аналітичній доповіді Національного інституту стратегічних досліджень «Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України» (2018 рік) [1]. Відповідно концепт ДПП закладено у нормативну базу кібербезпеки України. Проте інформаційна безпека країни не вичерпується кібернетичною безпекою, а контентне насичення стратегічних комунікацій як проактивної форми протидії інформаційним загрозам залишається нагальною проблемою кожного міністерства та відомства України. Специфікою стратегічних комунікацій є необхідність реалізації державних програм через залучення креативних творчих колективів виконавців.

Сьогодні міжсекторальна взаємодія у стратегічних комунікаціях в основному спирається не на приватні компанії, а на співпрацю з недержавними громадськими організаціями, які скоріше мали б складати фундамент системи демократичної підзвітності у системі стратегічних комуні-

кацій. Волонтерські проекти та недержавні громадські організації (НГО) обмежені обсягами міжнародних грантів і не можуть інвестувати у розвиток інфраструктури стратегічних комунікацій. Разом з тим практика стратkому в Україні показала, що суттєва частка таких НГО була створена спеціалістами комерційних PR-фірм. Отже, управлінська проблема полягає у виявленні причин унеможливлення або небажання приватного рекламного та PR – сектору брати участь у комунікативних проектах держави в сфері інформаційної безпеки на засадах ДПП.

Серед тенденцій розвитку вітчизняного PR-ринку, які можуть впливати на стан ДПП, варто відзначити такі: збільшення частки вітчизняних кампаній, які ведуть супроводження ТНК не лише в Україні, але й за кордоном; участь міжнародних PR-фірм у глобальних інформаційних проектах протидії гібридним загрозам та у забезпеченні відповідних глобальних політичних та соціальних інфопроектів; залучення українських фірм на аутсорсінгу до проведення вищезазначених проектів; переважання послуг у сегменті b2b; конкуренція між PR-агенціями за просування популярних програм b2c та g2c (зокрема, у сфері фактчекінгу та медіаосвіти) [2].

Дослідження тенденцій ринку PR дозволяє виокремити такі основні проблеми у ДПП. По-перше, це традиційне небажання українського бізнесу робити інвестиції у гуманітарні проекти, які вважаються апріорі збитковими (за невеликим виключенням туристичних, спортивних та освітянських програм). По-друге, більшість операторів PR – ринку відзначають проблемність проведення тендерів. Серед позитивних тенденцій можна відзначити те, що молоді фірми участь у проектах страткому розглядають як можливість виходу на зарубіжні ринки. Також збільшилась кількість фірм, що пропонують послуги стратегічного піару.

У передових країнах світу розбудова ДПП стала унормованим явищем і безпековим трендом. Для його розвитку використовують різноманітні інструменти, серед яких важливе місце займають координаційні ради, форуми і платформи, які забезпечують контакти, обмін інформацією, узгодження позицій між партнерами на постійній основі. Для започаткування ДПП в Україні з використанням апробованих у США, НАТО та ЄС підходів, слід виділити ряд ключових вимог до процесу реалізації концепції партнерства. ДПП не можливе за відсутності: взаємної довіри та встановлених обмежень, спрямованих на недопущення зловживань; чітких, недвозначних цілей та стратегій, зафіксованих у документах; чіткого розподілу ризиків, відповідальності та повноважень [3].

З боку державних органів, які несуть загальну відповідальність за інформаційну безпеку, інтерес до ДПП, ймовірно, буде полягати у такому: у намаганні залучити кошти приватного сектору до фінансування заходів, надання приміщень для їх проведення; у залученні креативних кадрів; у

отриманні доступу до кулуарної інформації щодо підготовки інформаційних атак як у політичному протиборстві, так і у комерційній конкуренції.

Для приватного сектору ДПП буде виглядати найбільш привабливим у такому: в отриманні податкових пільг в разі інвестування у заходи з інформаційної безпеки, у можливості використання побудованих інформаційних центрів (агентств, корпунктів, медійних та презентаційних центрів тощо) на засадах концесії; в можливості участі у формуванні інформаційної політики через своїх представників у безпекових проектах; у своєчасному отриманні від компетентних державних органів надійної інформації про комерційні ризики; у методологічній підтримці з боку держави щодо забезпечення готовності адекватно реагувати на них, включаючи відповідне навчання та тренування.

**Література**

1. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України (2018 рік). Аналітична доповідь НІСД України. URL: https://niss.gov.ua/publikacii/analitichni-dopovidi/derzhavno-privatne-partnerstvo-u-sferi-kiberbezpeki-mizhnarodniy-0 (дата звернення: 03.03.2020).

2. Тенденції і прогнози-2020 на українському ринку PR. Матеріали Інтернет-конференції за результатами дослідження Publicity Creating. Укрінформ (10.02.20). URL: https://www.ukrinform.ua/rubric-presshall/2870643-tendencii-i-prognozi2020-na-ukrainskomu-rinku-pr.html (дата звернення: 10.02.2020).

3. Державно-приватне партнерство як механізм реалізації нової регіональної політики. Експертне дослідження за підтримки ЄС. URL: http://rdpa.regionet.org.ua/images/129/PPP_report_U-LEAD_30_10_2017.pdf (дата звернення: 20.02.2020).

*УДК: 340.1*

**Беланюк М. В.**
кандидат юридичних наук,
НДІ інформатики і права НАПрН України

## КІБЕРБЕЗПЕКА В СИСТЕМІ ЗАХИСТУ ДЕРЖАВИ

З розвитком інформаційного суспільства розвиваються й інформаційні технології, які поширюються на всі сфери життєдіяльності людини і суспільства. Крім позитивного, що привносять інформаційні технології в наше життя, є й інша сторона – небезпека застосування кібератак проти військових, політичних, фінансово-економічних та промислових інфраструктур держави.

Основними міжнародними документами, що регулюють сферу кібербезпеки в Україні є Будапештська Конвенція про кіберзлочинність (2001 р., ратифікована у 2005 р.) [1], Статут Міжнародного союзу електрозв'язку 1992 року, доповнений Доповіддю ООН про кібербезпеку у 2015 р. [2] та Директива Європейського парламенту і Ради Європи «Про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу» від 6 липня 2016 р. 2016/1148 [3]. Основними національними нормативно-правовими актами у цій сфері є Національна стратегія кібербезпеки України [4] та Закон України "Про основні засади забезпечення кібербезпеки України" [5].

Відповідно до зазначених нормативно-правових актів до пріоритетів забезпечення кібербезпеки України віднесено: розробку безпечного, стійкого та надійного кіберпростору; забезпечення безпеки урядових інформаційних ресурсів та критичної інфраструктури; розбудову кібербезпекових спроможностей в оборонному секторі; боротьбу з кіберзлочинами тощо.

Аналіз нормативно-правових актів з питань кібербезпеки України надає можливість висловити певні зауваження та пропозиції.

Закон України "Про основні засади забезпечення кібербезпеки України", містить визначення важливих термінів, розмежовує повноваження між агенціями з кібербезпеки та визначає принципи подальшого регулювання захисту критичної інфраструктури і державно-приватного партнерства. Поряд з цим в законі досить розмиті розмежування повноважень між суб'єктами кібербезпеки. Слід зазначити, що це рамковий набір правил та вимог, подальша деталізація яких має бути визначена у постановах уряду, в інакшому випадку, на наш погляд, вимоги положень Закону залишаться декларативними.

В нормативно-правових актах у сфері кібербезпеки не узгоджена термінологія, відсутні ряд термінів, зокрема таких як "користувач послуг", "дані про рух інформації", "електронні докази". Не врегульовані терміни "термінове збереження комп'ютерних даних, які зберігаються", "термінове збереження та часткове розкриття даних про рух інформації", що унеможливлює в повній мірі виконання положень Будапештської конвенції.

Постанова Кабінету Міністрів України «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави» [6] суперечить Закону "Про основні засади забезпечення кібербезпеки України", оскільки постанова була прийнята раніше (2016 р.) і після прийняття Закону до неї не було внесено жодних змін. Не затверджено положення про критичну інфраструктуру, а регуляторні правила щодо захисту критичної інфраструктури недостатні та непослідовні, не визначені критерії та методологія віднесення об'єктів до критичної інфраструктури, а також процедура її атестації та категори-

зації. Через зазначене ряд положень Закону "Про основні засади забезпечення кібербезпеки України" залишаються декларативними.

Відомствами, на які покладено контроль кібербезпеки в Україні визначено МО України, ДССЗЗІ, СБУ, Національну поліцію України, Національний банк України та розвідувальні органи. Існує дублювання функцій цих органів. Відсутні чіткі повноваження, завдання та обов'язки державних агенцій, відповідальних за захист критичної інфраструктури, права та обов'язки керівників об'єктів критичної інфраструктури.

Відповідно до Директиви Європейського парламенту і Ради Європи «Про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу» країни мають встановити певні вимоги до безпеки та інформування операторами істотних послуг і провайдерами цифрових послуг. Законом "Про основні засади забезпечення кібербезпеки України" дійсно встановлена вимога до операторів об'єктів критичної інфраструктури щодо інформування CERT-UA про кіберінциденти, але переліку таких об'єктів немає. Законопроект про критичну інфраструктуру та її захист [7], зареєстрований 27.05.2019 р., донині перебуває на розгляді у ВР України. Внаслідок цього зазначена вимога залишається лише декларативною.

Одним із рішень проблем кібербезпеки, за висновками Круглова В.В. є використання моделей державно-приватного партнерства, які мають вирішити такі завдання: забезпечити надійний доступ до Інтернет-мережі, регулювати технічну безпеку та обробку даних, проводити обмін інформацією щодо загроз і вразливостей, здійснювати допомогу щодо вирішення ситуацій, пов'язаних із загрозами або незаконним контентом в мережі Інтернет [8]. Питання взаємодії державного і приватного партнерства в кібербезпековій сфері, на нашу думку, має бути врегульовано законодавчо. Єрменчук О.П. та Пальчик М. Л. вважають, що до основних пріоритетних напрямів розвитку державно-приватного партнерства (ДПП) у сфері захисту критичної інфраструктури слід віднести: розвиток ДПП у сфері запобігання надзвичайним ситуаціям та реагування на них; ДПП у запобіганні кіберзагрозам, реагуванні на кібератаки та кіберінциденти, усуненні їх наслідків, зокрема, в умовах кризових ситуацій, надзвичайного і воєнного стану та в особливий період; здійснення обміну та захисту інформації між державними органами, приватним сектором і населенням стосовно загроз критичній інфраструктурі та захисту чутливої інформації у цій сфері; сприяння приватними партнерами державним органам у виконанні завдань із забезпечення кібербезпеки та кіберзахисту [9] .

Крім зазначеного, в умовах сьогодення недостатньо покладатися виключно на захист. Для того, щоб мінімізувати збитки від кібератак, важливо фокусуватися не лише на захисті, але й на побудові правильних про-

цесів реагування на інциденти [10]. Все більше фахівців галузі схиляються до думки щодо необхідності навчання реагуванню на кіберзагрози шляхом створення національного порталу кібербезпеки, спрямованого на формування культури кібербезпеки у суспільстві.

З урахуванням зазначеного, до недоліків кібернетичного захисту України можна віднести:

– електронно-комунікаційна інфраструктура, її розвиток і захист не відповідають сучасним вимогам;

– критична інфраструктура недостатньо захищена;

– організаційно-технічні заходи недостатні для забезпечення кібербезпеки та кіберзахисту критичної інфраструктури та державних електронно-інформаційних ресурсів;

– недостатня протидія суб'єктів сектору безпеки і оборони кіберзагрозам;

– недостатність координації, співробітництва та обміну інформацією між суб'єктами забезпечення кібербезпеки;

– неузгодженість між політикою та урядом скоординованих дій, визначених стратегічними пріоритетами України щодо кіберзахисту;

– недостатність бюджетного фінансування для залучення та виплати конкурентоспроможних зарплат фахівцям з кібербезпеки.

**Висновки**

Незважаючи на ряд позитивних кроків для виконання своїх міжнародних зобов'язань та вдосконалення законодавства в Україні правове поле у сфері кібербезпеки потребує доопрацювання. Вбачається необхідним:

1. Прийняти Закон про критичну інфраструктуру.

2. Узгодити норми вітчизняних нормативно-правових актів у сфері кібербезпеки з законодавством ЄС. При цьому слід залучити суб'єктів забезпечення кібербезпеки, вчених та фахівців галузі.

3. Гармонізувати національне законодавство щодо термінології у кібербезпековій сфері.

4. Розробити ефективний механізм розмежування повноважень між правоохоронними органами, відповідальними за кібербезпеку.

5. Розробити стратегію внутрішньої комунікації стосовно кіберінцидентів між суб'єктами критичної інфраструктури.

6. Опрацювати механізм державно-приватного партнерства у сфері кібербезпеки.

7. Вжити заходів щодо формування культури кібербезпеки у суспільстві.

**Література**

1. Конвенція про кіберзлочинність. Рада Європи; Конвенція, Міжнародний документ від 23.11.2001. URL: https://zakon.rada.gov.ua/laws/show/984_013-16 (дата звернення: 19.03.2020).

2. Статут Міжнародного союху електрозв'язку. Міжнародний союз електрозв'язку; Статут; Міжнародний документ від 22.12.1992. URL: https://zakon.rada.gov.ua/laws/show/995_099 (дата звернення: 15.03.2020).

3. Директива Європейського Парламенту і Ради (ЄС) 2016/1148 від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на […]. Європейський Союз; Директива, Міжнародний документ від 06.07.2016 № 2016/1148 URL: https://zakon.rada.gov.ua/laws/show/984_013-16 (дата звернення: 19.03.2020).

4. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» Указ Президента України; Стратегія від 15.03.2016 № 96/2016. URL: https://zakon5.rada.gov.ua/laws/show/96/2016 (дата звернення: 05.04.2020).

5. Про основні засади забезпечення кібербезпеки України. Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 19.03.2020).

6. Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави. Постанова Кабінету Міністрів України; Порядок, Пропозиції, Форма типового документа від 23.08.2016 № 563. URL: https://zakon.rada.gov.ua/laws/show/563-2016-%D0%BF (дата звернення: 05.04.2020).

7. Проект Закону про критичну інфраструктуру та її захист. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=65996 (дата звернення: 05.04.2020).

8. Круглов В.В. Державно-приватне партнерство у сфері кібербезпеки. Вчені записки ТНУ імені В.І. Вернадського. Серія: Державне управління. С. 57-61. URL: http://www.pubadm.vernadskyjournals.in.ua/journals/2018/3_2018/13.pdf (дата звернення: 20.03.2020).

9. Єрменчук О.П., Пальчик М.Л. Проблемні аспекти правового регулювання державно-приватного партнерства у сфері захисту критичної інфраструктури. Сайт НА СБ України. URL: http://academy.ssu.gov.ua/ua/page/page_1581342397.htm (дата звернення: 20.03.2020).

10. Янковський О. Україні потрібна нова кіберстратегія. Газета Українська правда. URL: https://www.pravda.com.ua/columns/2019/09/14/7226291/ (дата звернення: 16.03.2020).

*УДК 342.95:351.74(477)*
**Благодарний А. М.**
доктор юридичних наук,
старший науковий співробітник,
Національна академія СБ України

# ШЛЯХИ УДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ УКРАЇНИ

Науково-технічна революція, нові інформаційні технології, глобальні інтеграційні процеси призвели до формування інформаційного середовища, в якому інформація є головним чинником управління сучасним світом й основним елементом влади [1, с. 152], тому інформаційне забезпечення сфери охорони правопорядку потребує постійного вдосконалення.

Починаючи розгляд зазначеної проблематики зауважимо, що наразі є нагальна необхідність створення принципово нової інформаційної системи, яка могла б об'єднати всі оперативно-пошукові бази даних в єдину інформаційну мережу правоохоронної системи України [2, с. 347]. Розглядаючи міжнародний досвід правозастосовної діяльності, варто зазначити, що поліцейські структури та спеціальні служби різних країн дедалі частіше взаємодіють між собою у протидії міжнародній злочинності, тероризму тощо. Також зазначені структури співпрацюють із миротворчими місіями ООН, двосторонні угоди між країнами та багатосторонні договори, укладені міжнародними організаціями, дозволяють обмінюватися інформацією та накопиченим досвідом, завдяки чому збільшується ефективність правоохоронної діяльності [3].

Дедалі більшу роль у процесах державотворення відіграє такий важливий прояв демократичного розвитку країни як наявність ефективної комунікації між владними інститутами та громадянським суспільством. В сучасних умовах стратегічна комунікація в системі державного управління стає особливо результативною, оскільки передбачає реалізацію трьох основних цілей: передачу інформації, трансформацію позиції громадськості у ставленні до державно-управлінських інституцій та зміну поведінки громадянина. Це відкриває нові можливості для участі громадськості в процесах формування та реалізації державної політики, що дає змогу зробити її більш відкритою, прозорою та демократичною [4, с. 5–6]. Особливо актуальним питання стратегічних комунікацій органів державної влади взагалі та правоохоронних органів зокрема постає в умовах гібридної війни проти України. Вважаємо, що у сучасних умовах вітчизняні правоохоронні органи повинні використовувати інформацію, перш за все, для підвищення патріотичної налаштованості громадян; посилення авторитету

державної влади, Збройних Сил України серед населення; активізації антипропаганди; вивчення громадської думки і формування її в позитивному напрямку; забезпечення громадського контролю; встановлення соціального партнерства; посилення зворотнього зв'язку із суспільством; профілактики та усунення можливих непорозумінь з громадськістю.

Як засвідчують матеріали судової практики, іноді має місце протиправне використання інформації, що міститься у базах даних правоохоронних органів України [4], тому особлива увага має зосереджуватися на захисті зазначеної інформації від несанкціонованого використання та протиправного знищення.

Розглядаючи проблеми інформаційного забезпечення діяльності правоохоронних органів, варто зазначити, що інформація на письмові запити посадових осіб правоохоронних органів не завжди надається належним чином. Однією з основних причин такої ситуації є недоліки вітчизняного інформаційного законодавства [5, с. 73]. Вважаємо, що порядок надання інформації правоохоронним органам має бути більш уніфікованим.

Отже, вирішення завдань сучасного інформаційного забезпечення діяльності правоохоронних органів України має бути досягнуто за рахунок упровадження єдиної політики інформаційного забезпечення системи державного управління; створення зазначеними органами спільних багатоцільових інформаційних систем, забезпечення їх повноти, актуальності та безпеки; покращення взаємодії з громадськістю.

**Література**

1. Протидія інформаційному тероризму та його фінансуванню в сучасних умовах : моногр. / В. В. Крутов, М. П. Стрельбицький, О. А. Шевченко ; за заг. ред. В. В. Крутова. – К. : Вид-во НАПрНУ; Ужгород : ТОВ "ІВА", 2014. – 309 с.

2. Гусаров С. М. Адміністративно-юрисдикційна діяльність органів внутрішніх справ : дис. ... д-ра юрид. наук : 12.00.07. / С. М. Гусаров. – К. : Ін-т законодавства Верховної Ради України, 2009. – 462 с.

3. Нефедова Н. А. Інформаційне забезпечення спеціальної поліцейської діяльності // Адміністративне право і процес. – № 2(8). – 2014. [Електронний ресурс]. – Режим доступу : http://applaw.knu.ua.

4. Вирок Шевченківського районного суду м. Києва від 28 вересня 2017 року по справі № 761/28897/17, провадження №1-кп/761/1555/2017 [Електронний ресурс] // Офіційний веб-портал судової влади України // Режим доступу : http://www.reyestr.court.gov.ua.

5. Благодарний А. М. Проблемні питання надання інформації посадовим особам правоохоронних органів / А. М. Благодарний // Бюлетень Міністерства юстиції України. – 2010. – № 10. – С. 72–78.

*УДК 351.863*
**Богуш В. М.**
кандидат технічних наук, доцент,
**Бровко В. Д.**
кандидат технічних наук,
**Настрадін В. П.**
кандидат технічних наук, професор,
Національна академія СБ України

# ЩОДО ВИРІШЕННЯ ЗАВДАННЯ СТВОРЕННЯ СИСТЕМ УПРАВЛІННЯ СТІЙКІСТЮ ТА БЕЗПЕКОЮ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ

Проблеми безпеки об'єктів критичної інфраструктури визначені Законом України «Про національну безпеку України». Основу щодо створення державної системи захисту об'єктів критичної інфраструктури закладає Концепція [1], схвалена розпорядженням КМУ від 6 грудня 2017 р., та Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури, затверджені постановою КМУ від 19 червня 2019 р. № 518 [2]. На черзі прийняття Верховною Радою України Закону України «Про критичну інфраструктуру та її захист».

Аналіз стану стосовно захисту об'єктів критичної інфраструктури держави на сьогодні не задовольняє вимогам національної безпеки і вимагає ретельного вивчання досвіду розвинених країн та сприйняття новітніх технологій у цій галузі національної безпеки.

Основні акценти політики США у сфері безпеки критичної інфраструктури полягають у зміцненні безпеки і стабільності критичної інфраструктури, насамперед, проти фізичних і кіберзагроз. Уряд держави працює з власниками і операторами критичної інфраструктури, щоб зміцнити її безпеку і стійкість.

Директива про політику президента 21 (PPD-21): Безпека та стійкість критично важливої інфраструктури [4] визначає безпеку як зменшення ризику для критичної інфраструктури за допомогою фізичних засобів або засобів кіберзахисту від вторгнень, нападів або наслідків стихійних чи техногенних катастроф, а стійкість як здатність готуватися та адаптуватися до змінних умов, швидко протистояти і швидко відновлюватися з післядії перешкод. Також стійкість включає в себе здатність протистояти і відновлюватися від навмисних нападів, аварій або природних загроз чи інцидентів.

Виконання цих вимог здійснюється на основі використання технологій управління стійкістю та безпекою. Управління організаційною стійкістю [organizational resilience management] – це систематичні і скоординова-

ні дії і практики, через які організація управляє операційним ризиком, і пов'язаними з ним потенційними загрозами і наслідками їх реалізації.

Для створення системи управління можна використати запропонований у стандарті ASIS SPC.1-2009 [3] і розвинений в інших стандартах цієї серії комплексний підхід щодо упровадження системи управління для забезпечення безпеки, готовності, реагування, пом'якшення наслідків, неперервності бізнесу і відновлення після руйнівних інцидентів, у результаті надзвичайної ситуації, кризи або катастрофи. Цей підхід адаптується до моделі неперервного покращення процесів Демінга-Шухарта [Plan-Do-Check-Act (PDCA)] наступним чином:

Плануй [plan]. Створення системи управління відповідно до політики, цілей, процесів і процедур, що мають відношення до управління ризиками та підвищення безпеки, готовності, реагування на інциденти, безперервності та відновлення і для досягнення результатів відповідно до загальної політики і цілей організації.

Виконуй [do]. Реалізація політики та експлуатації системи управління, контроль процесів і процедур.

Перевіряй [check]. Оцінка і вимірювання продуктивності процесу системи управління відповідно до політики, цілей і практичного досвіду та представлення результатів керівництву для аналізу.

Дій [act]. Реалізація коригувальних та запобіжних дій, заснованих на результатах внутрішнього аудиту системи управління та вказівок керівництва, для досягнення постійного поліпшення системи управління.

Дотримання вимог щодо створення системи управління стійкістю та безпекою об'єкту критичної інфраструктури може бути перевірено за допомогою процесу аудиту, який сумісний і узгоджується з методологією ДСТУ ISO 9001, ДСТУ ISO 14001 та/або ДСТУ ISO/IEC 27001 стосовно PDCA моделі.

Результати роботи, у першу чергу призначені для використання при створенні робочих навчальних програм дисципліни «Методи та засоби захисту об'єктів» для спеціальностей 256 Національна безпека, 125 Кібербезпека, а також спеціалізації «Контррозвідувальний захист об'єктів критичної інфраструктури».

**Література**

1. Концепція створення державної системи захисту критичної інфраструктури. Схвалена розпорядженням Кабінету Міністрів України від 6 грудня 2017 р. № 1009-р.

2. Порядок формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави. Затверджено постановою Кабінету Міністрів України від 23 серпня 2016 р. № 563.

3. ASIS SPC.1-2009 – Organizational Resilience: Security, Preparedness, and Continuity Management Systems – Requirements with Guidance for Use, Approved March 5, 2009.

4. Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (PPD-21), released on February 12, 2013.

*УДК 341.824:338.47(043.2)*

**Браницький О. А.**
Служба безпеки України

## ДЕРЖАВНИЙ ЗАХИСТ ОСІБ, ОБІЗНАНИХ З ДЕРЖАВНОЮ ТАЄМНИЦЕЮ

Чинним законодавством визначено, що інформація з обмеженим доступом, зокрема державна таємниця, підлягають охороні державою.

При цьому, організація та забезпечення режиму секретності здебільшого будується навколо охорони матеріального носія секретної інформації, під яким розуміються матеріальні об'єкти, в тому числі фізичні поля, в яких відомості, що становлять державну таємницю, відображені у вигляді текстів, знаків, символів, образів, сигналів, технічних рішень, процесів тощо.

Проте, як вбачається, з аналізу норм законодавства про державну таємницю, нормативне регулювання захисту громадянина чи іншої особи, що обізнана з державною таємницею, є суцільною прогалиною та має лише фрагментарні *(безсистемні)* риси.

Так, у вітчизняному законодавстві захист секретоносіїв обмежується лише декількома соціальними гарантіями, закріпленими у «Положенні про види, розміри і порядок надання компенсації громадянам у зв'язку з роботою, яка передбачає доступ до державної таємниці», затвердженому постановою Кабінету Міністрів України № 414 від 15.06.1994 *(а саме, у частині виплати такої компенсації і наявності переважного права у секретоносія залишатися на роботі у разі вивільнення працівників у зв'язку із змінами в організації виробництва і праці)* та декларативним завданням розвідувальних органів України щодо безпеки відряджених за кордон громадян України, які обізнані у відомостях, що становлять державну таємницю *(ст. 4 Закону України «Про розвідувальні органи України» та ст. 3 Закону України «Про Службу зовнішньої розвідки України»)*, механізм реалізації якого на практиці відсутній.

Тож такий захист в сучасних умовах, включаючи збройну агресію проти України, наявність тимчасово окупованих територій тощо, є вкрай

недостатнім і підвищення рівня правового захисту секретоносіїв варто визнати нагальною потребою.

З урахуванням викладеного є цілком виправданим кроком передбачити у новому проекті закону, який має замінити чинний Закон України «Про державну таємницю», що для забезпечення захисту осіб, обізнаних з державною таємницею, з урахуванням конкретних обставин, можуть застосовуватися такі заходи:

а) особиста охорона, охорона житла і майна;

б) видача спеціальних засобів індивідуального захисту і сповіщення про небезпеку;

в) використання технічних засобів контролю і прослуховування телефонних та інших переговорів, візуальне спостереження;

г) заміна документів, місця роботи або навчання;

д) тимчасове розміщення у місцях, що забезпечують безпеку;

е) забезпечення конфіденційності даних про об'єкти захисту.

Підставою для вжиття заходів забезпечення захисту осіб, обізнаних з державною таємницею, є дані, що свідчать про наявність реальної загрози їх життю, здоров'ю або майну.

Приводом для вжиття заходів забезпечення захисту осіб, обізнаних з державною таємницею може бути заява такої особи або отримання оперативної чи іншої інформації про наявність загрози життю, здоров'ю, житлу та майну вказаних осіб.

З урахуванням характеру і ступеня небезпеки для життя, здоров'я, житла та майна осіб, обізнаних з державною таємницею, можуть здійснюватися й інші заходи державного захисту відповідно до чинного законодавства.

Органом, який прийматиме рішення про вжиття заходів забезпечення захисту осіб, обізнаних з державною таємницею, та здійснюватиме такі заходи – має стати Служба безпеки України.

Підсумовуючи викладене, враховуючи, що безпека персоналу, який працює з державною таємницю є одним з ключових сучасних факторів забезпечення режиму секретності та нейтралізації каналів її витоку, окреслена модернізація Закону України «Про державну таємницю», прийнятого ще у 1994 році на радянській світоглядній базі, де правові норми були спрямовані, перш за все, на захист «системи», а не людини, сприятиме закладенню у нове законодавства саме людиноцентристських підходів, що полягають у вирішенні проблем держави через пріоритет захисту прав людини.

**Література**

1. Закон України «Про інформацію» від 02 жовтня 1992 року № 2657-XII. [Електрон. ресурс]: – Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12.

2. Закон України «Про доступ до публічної інформації» від 13 січня 2011 року № 2939-VI. [Електрон. ресурс]: – Режим доступу: https://zakon.rada.gov.ua/laws/show/2939-17.

3. Закон України «Про державну таємницю» від 21 січня 1994 року № 3855-XII. [Електрон. ресурс]: – Режим доступу: https://zakon.rada.gov.ua/laws/show/3855-12.

4. Закону України «Про розвідувальні органи України» від 22 березня 2001 року № 2331-III. [Електрон. ресурс]: – Режим доступу: https://zakon.rada.gov.ua/laws/show/2331-14;

5. Закону України «Про Службу зовнішньої розвідки України» від 01 грудня 2005 року № 3160-IV. [Електрон. ресурс]: – Режим доступу: https://zakon.rada.gov.ua/laws/show/3160-15.

6. Постанова Кабінету Міністрів України від 15 червня 1994 року № 414 «Про види, розміри і порядок надання компенсації громадянам у зв'язку з роботою, яка передбачає доступ до державної таємниці». [Електрон. ресурс]: – Режим доступу: https://zakon.rada.gov.ua/laws/show/414-94-п.

*УДК 004.056:5:378.1(045)*

**Бровко В. Д.**
кандидат технічних наук,
Національна академія СБ України
**Архипов О. Є.**
доктор технічних наук,
Національний технічний університет України
«КПІ імені Ігоря Сікорського»
**Скубак О. М.**
кандидат технічних наук,
Національна академія СБ України

## ВИЗНАЧЕННЯ МОМЕНТУ РОЗЛАДКИ ІНФОРМАЦІЙНОГО ПОТОКУ

Прогнозування виникнення інформаційних загроз є невід'ємною частиною системи захисту інформації. При правильному виявленні загрози, а також правильному її опрацюванню, вжиття запобіжних заходів знижується ризик виникнення атаки. Одним із джерел можливої інформації для виявлення загроз є інформаційний потік. Інформаційний потік являє собою сукупність усіх форм інформації, представленої у вигляді друкованих, електронних, усних носіїв, та яка має повний зміст розкриття об'єкту інформації. При аналізі інформаційного потоку важливим являється виявлення можливого інформаційного викиду інформації, яка сама по собі

може бути загрозою або провокувати виникнення інформаційних загроз. Ця проблема може бути вирішена шляхом виявлення моментів розладки часового ряду, сформованого з інформаційного потоку. Масова комунікація у мережі Інтернет набирає дедалі більших обертів. Зокрема, ринок онлайнової реклами був єдиним рекламним ринком, який не лише не скоротився в роки фінансової кризи 2008–2009 рр., а навіть трохи зріс. Абсолютну меншість серед найвідвідуваніших інтернет-ресурсів становлять сайти зі сталим змістом або рідко поновлювані джерела, такі, як електронні бібліотеки, енциклопедії або деякі корпоративні сторінки. Усі інші мережеві ресурси є, по суті, інформаційними потоками. Тому доцільно сформувати визначення: ***Інформаційний потік*** – це система продукування й поширення повідомлень, які характеризуються певними спільними ознаками.

Для дослідження доцільно було використовувати таке поняття як часовий ряд – особливий тип даних, який містить інформацію про плинність значень станів або характеристик ОД у часі. При дослідженні часових рядів в їх структурі намагаються окремо виділити детерміновану $y_t$ та стохастичну $e_t$ складові, процедури моделювання та прогнозування яких принципово відмінні. Найчастіше при цьому спираються на адитивну модель представлення часового ряду:

$$z_t = y_t + e_t \ , \ t = \overline{1,n} \qquad (1.1)$$

В свою чергу в детермінованій складовій традиційно виділяють три адитивних компонента: *тренд* – базовий (основний) детермінований компонент часового ряду, який характеризує вплив довгострокових постійно діючих факторів, повільний та інерційний; *циклічний компонент* описує нерегулярні, відносно довгі за часом періоди зростання та спаду рівнів часового ряду; с*езонний компонент* відображає достатньо поширену як серед природних, так і штучних процесів регулярну повторюваність явищ: метеорологічних, кліматичних, соціально-економічних, демографічних і т.п., які не мають точної періодичності та сталості амплітуд.

Наступним кроком є *модель авторегресії* – це модель стаціонарної послідовності, що відображає значення показника $y_t$ у вигляді лінійної комбінації скінченого числа попередніх значень цього показника та адитивної випадкової складової [1]:

$$y_t = a_1 y_{t-1} + a_2 y_{t-2} + ... + a_p y_{t-p} + e_t . \qquad (1.2)$$

Одним із важливих етапів побудови авторегресивної моделі є визначення її порядку $p$ та обчислення її параметрів. Якщо порядок моделі вибрано не вдало, то процедуру обчислення оцінок можна повторити для моделі авторегресії іншого порядку чи структури. Необґрунтоване підвищення порядку моделі та ускладнення її структури знижує точність оцінок параметрів та якість прогнозу. Водночас недостатня кількість коефіцієнтів моделі й занадто малий порядок авторегресії не дадуть можливість адекватно оцінити динаміку процесу та спрогнозувати його подальші зміни.

Тому задача полягає в тому, щоб вибрати модель авторегресії найменшого порядку за умови забезпечення достатньої точності опису даних та прогнозування. Для визначення порядку авторегресії використовують автокореляційну функцію.

Беручи до уваги вище сказане, з'являється такі процеси як момент розладки та згладжування часового ряду. Виявлення зміни властивостей – одна з основних складових аналізу сигналів та динамічних систем, основа алгоритмів розпізнавання образів, контролю та технічної діагностики інформаційно-керуючих систем, а також додаткові адаптивні процедури ідентифікації стану систем зі складною динамікою.

При формальній постановці задачі виявлення істотних змін властивостей випадкових процесів під розладкою процесу можна розуміти стрибкоподібну зміну параметрів, які описують даний процес, в невідомий момент процесу по тій чи іншій координаті, частіше – по часу [2]. Задача виявлення моменту розладки – встановлення факту розладки, і, якщо розладка відбулась, – то оцінка моменту розладки. Вихідними даними для вирішення задачі виявлення моменту розладки при аналізі процесу є дані поведінки процесу до і після можливої розладки.

Випадкові процеси, розладку в яких потрібно виявити, можуть мати неперервний та дискретний час. При побудові алгоритму виявлення та їх дослідження різниця між цими двома типами задач не є суттєвою. При описі алгоритмів вважатиметься, що час – дискретний.

Мета згладжування часового ряду – виділення його детермінованої складової $y_t$, $t=\overline{1,n}$. Одним з найбільш поширених способів згладжування часового ряду є його обробка із застосуванням процедури зваженого ковзкого середнього. В загальному вигляді процедуру обчислення згладженої оцінки $\widetilde{y}_t$ для *t*-ого рівня ряду $z_t$ описує вираз:

$$\widetilde{y}_t = \sum_{j=-m}^{m} v_j z_{t+j}, \qquad (1.3)$$

При попередньому аналізі вихідних даних іноді можна спостерігати окремі значення, які суттєво відрізняються від значень, що знаходяться поруч. Це так звані аномальні дані, що виникли, наприклад, через випадкові збої у вимірювальній або обчислювальній техніці. Аномальні дані (АД) можуть зустрічатися у будь-яких експериментальних даних: як у вибіркових сукупностях, так і у часових рядах, причому у кожному з цих випадків не вилучені АД стають причиною появи серйозних помилок у результатах, отриманих з використанням цих даних.

Застосовування методу медіанного згладжування для виявлення та усунення АД реалізується шляхом аналізу даних в межах ковзкого інтервалу, що по кроково переміщується вздовж часового ряду в заданому напрямі, звичайно за наростанням індексів членів ряду. Довільному положенню ковзкого інтервалу відповідає фрагмент вихідного часового ряду з

$2m+1$ елементів: $y_{i-m},\ldots,y_i,\ldots,y_{i+m}$. Згладжена оцінка $\tilde{y}_i$ визначається для середнього елемента інтервалу шляхом побудови варіаційного ряду з його елементів $y_{(1)},\ldots,y_{(m+1)},\ldots y_{(2m+1)}$ та виділення його медіани:

$$\tilde{y}_i = Med\{y_{i-m},\ldots,y_i,\ldots,y_{i+m}\} = y_{(m+1)}. \quad (1.4)$$

Після цього зі складу ковзкого інтервалу виключається крайній лівий елемент та дописується справа черговий елемент часового ряду. При цьому середина інтервалу зміщується на один елемент вправо. Для нового положення ковзкого інтервалу повторюється процедура обчислення згладженої оцінки середнього елемента. У такий спосіб ковзкий інтервал проходить повздовж усього часового ряду, починаючи з його лівого краю. Після згладжування вихідного ряду можна оцінити трендову складову часового ряду і далі, аналізуючи послідовність нев'язок, виявити АД. Хотілося б відзначити, що для аналізу поведінки інформаційного потоку ми використали поняття часового ряду, а також поняття моделі авторегресії, моменту розладки процесу і розглянуті методи згладжування часових рядів.

**Література**


1. Аналіз данних та статистична обробка сигналів: навч. посіб. / О.Є. Архіпов, С.А. Архіпова . – 2012 р.
2. *Інформаційна технологія аналізу самоподібних інформаційних потоків: нав. посіб. / О.М. Барановський. – 2015 р.*
3. Феномены современных информационных потоков : навч. посібник / Д.В. Ландэ, А.Б. Литвин // Сети и бизнес. – 2001р.
4. Політика і мас-медіа (переклад з нім.): навч. посіб. / Г. Штромайєр – К.: Вид. дім «Києво-могилянська академія». – 2008 р.
5. Обнаружение раз ладки случайных процессов: навч. посіб. /А.А. Жиглявський, А.Є. Красовський. – 1988 р.
6. Алгоритм обнаружения моментов изменения параметров уравнения случайного процесса//Автоматика и телемеханіка: навч. посіб. / Л.І. Бородкін, В.В. Моттль. – 1976. – № 6.
7. Непараметрический метод обнаружения моментов переключения двух случайных последовательностей// Автоматика и телемеханіка: навч.посіб./ Б.Е. Бродський, Б.С. Дарховський. – 1989 р.
8. Вікіпедія. Інтернет. – [Електроний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/%D0%A1%D1%82%D0%BE%D1%85%D0%B0%D1%81%D1%82%D0%B8%D1%87%D0%BD%D0%BE%D1%81%D1%82%D1%8C .
9. Последовательные оценки параметров стохастических динамических систем: навч.посіб. / В.В. Конєв. – Томск: изд-во Томского ун-та. – 1985 р.
10. Обнаружение изменения свойств сигналов и динамических систем:навч.посіб. / М. Бассвиль, А. Банвениста. – М.: Мир. – 1989 р.

*УДК355/359*
**Войтко О. В.**
кандидат військових наук
**Петренко К. М.**
Національний університет оборони України
імені ІванаЧерняховського

# ЧИННИКИ, ЯКІ ВПЛИВАЮТЬ НА ФУНКЦІОНУВАННЯ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ МІНІСТЕРСТВА ОБОРОНИ ТА ЗБРОЙНИХ СИЛ УКРАЇНИ

Збройна агресія Російської Федерації проти України, яка здійснюється з лютого 2014 року, має складний комплексний характер. Впливи здійснюються як одночасно, так і послідовно, фактично на всі сфери життєдіяльності нашої держави, причому отримані результати в одній сфері відразу використовуються для посилення інших напрямів.

Міністерство оборони України є 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 [1, с. 4].

Система забезпечення інформаційної безпеки Міністерства оборони України та Збройних Сил України є невід'ємною складовою системи забезпечення інформаційної безпеки держави.

Нові виклики національній безпеці обумовлюють нагальну необхідність створення дієвої та ефективної системи забезпечення інформаційної безпеки Міністерства оборони та Збройних України до стандартів НАТО. Ця система на сьогоднішній день перебуває в стадії становлення, при чому цей процес, на відміну від провідних країн світу, відбувається в реальних бойових умовах [2, с. 59].

Отже, важливим моментом має стати те, що Міністерство оборони України повинно сформувати таку систему забезпечення інформаційної безпеки, яка дозволить гарантовано забезпечити національні інтереси за будь-яких умов.

Разом з тим існує багато чинників, які безпосередньо впливають на функціонування системи забезпечення інформаційної безпеки Міністерства оборони України та Збройних Сил України:

нескоординована діяльність різних структур, які реалізують інформаційну політику держави, через відсутність: чіткого розподілу функцій між різними суб'єктами стратегічних комунікацій (це можливо тільки в єдиній системі);

відсутність спільного планування та узгодження дій різних суб'єктів стратегічних комунікацій;

єдиної системи моніторингу інформаційного простору;

низька медіаграмотність населення України (зокрема особового складу Збройних Сил України) і, як наслідок, недостатнє розуміння і підтримка державної інформаційної політики, довіра до фейків та матеріалів дезінформуючого характеру, в тому числі – матеріалів дискредитації та компрометації керівного складу;

недостатня мотивація громадян України до проходження військової служби в Збройних Силах;

низький інтерес більшості населення України до стримування російської збройної агресії, дій Збройних Сил України на Донбасі, їх розвитку та реформування;

загроза федералізації України через сепаратистські настрої серед частини населення та зовнішній вплив Росії, Угорщини, Румунії та на територіях Донецької, Луганської, Харківської, Херсонської, Миколаївської, Одеської, Закарпатської, Чернівецької областей.

Таким чином, для ефективного функціонування та досягнення мети при створенні системи забезпечення інформаційної безпеки Міністерства оборони України та Збройних Сил України необхідно врахувати вищенаведені чинники.

**Література**

1. Про затвердження Концепції стратегічних комунікацій Міністерства оборони України та Збройних Сил України : Наказ Міністра оборони України від 22.11.2017 р. №612/2017. URL:http://www.mil.gov.ua.

2. Основи забезпечення інформаційної безпеки держави у воєнній сфері: навч. посіб. / М.М. Биченок – К.: НУОУ ім. І. Черняховського, 2019. − 125 с.

*УДК: 378.016:004.056.5*

**Воскобойніков С. О.**
кандидат педагогічних наук,
**Решетніков О. В.**
Національна академія СБ України

## ВИКОРИСТАННЯ ПЛАТФОРМ ВІРТУАЛІЗАЦІЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ В ПРОЦЕСІ ПІДГОТОВКИ ФАХІВЦІВ З КІБЕРБЕЗПЕКИ

В умовах розвитку національної інформаційної інфраструктури та впровадження сучасних інформаційних технологій в критичну інфраструктуру України за останні шість років модернізаційні зміни обумовлені низкою викликів для фахівців кібернетичної безпеки.

Більша частина комерційних організацій в Україні поступово переходять до розгортання хмарних технологій, використання електронних продуктів та переходу до електронного документообороту, накопичуючи власні інформаційні активи [1].

Міжнародні ІТ-компанії займаються розробкою продуктів із поєднанням різних технологічних інформаційних платформ, що дає поштовх міграції робочих потоків на різні хмарні сервіси, тим саме ускладнює організацію системи кібербезпеки та реалізацію єдиної політики інформаційної безпеки, викликає інтерес до вивчення досвіду подолання міжнародної кіберзлочинності. Аналіз останніх загроз, яким були підтверджені об'єкти критичної інфраструктури показав що існує тенденція збільшення проявів кіберзлочинності у мовах виникаючих криз та інтенсивності масового розповсюдження ними шкідливого програмного забезпечення, використання вразливостей операційних систем та прикладного програмного забезпечення для здійснення таргетованих атак. В цих умовах існує потреба в якісній підготовці нової генерація компетентних фахівців, здатних реагувати на сучасні загрози для захисту критично важливих інформаційних ресурсів, що є власністю держави [3].

Світова практика показала важливість використання платформ віртуалізації у процесі фахової підготовки, підвищення кваліфікації фахівців кібербезпеки і набуття ними нових компетенцій з оперативного виявлення та реагування на комп'ютерні інциденти, про це свідчить позитивні відгуки зарубіжних фахівців естонських компаній з кібербезпеки – CYBExer Technologies, Bytelife Solutions Oz, BHC Laboratory Oz (Андруса Ківіаса, 2019), які працюють над впровадженням подібних систем у комерційній сфері та активно впроваджують власні методики в навчальний процес провідних закладів вищої освіти Європи таких як: Університет Порту (Португалія), Тартуський університет (Естонія) [2].

Сприяння міжнародними організаціями використанню програмного забезпечення для створення гнучких систем віртуального інформаційно-телекомунікаційного середовища на основі визначених параметрів дає змогу організувати відпрацювання окремих сценаріїв атак та технік реагування на них під час проведення масштабних навчальних заходів кібертренувань, до яких залучаються фахівці організацій різних форм власності. Це дає змогу фахівціям з кібербезпеки, бізнесу, органів державного управління, правоохоронним органам та науковцям якісно обмінюватись передовим досвідом, якісно та оперативно взаємодіяти в процесі розробки нових систем кібернетичної безпеки, впроваджувати їх в національні системи кібербезпеки та здійснювати якісну підготовку нових фахівців які відповідають новим викликам [2].

Заклади вищої освіти, які здійснюють підготовку фахівців галузі 125 Кібербезпека досліджують сучасні тенденції розвитку інформаційної безпеки у світі та розробляють алгоритми ефективних дій і відповідь на виклики кіберзагроз. Вітчизняні науковці використовують віртуальне середовище як потребу в процесі підготовки сучасних фахівців.

**Література**

1. Федоренко Р.М. Віртуалізація як варіант побудови іт-інфраструктури для проведення навчань з кібербезпеки / Р.М. Федоренко, М.В. Ткаченко, Ю.В. Кондратенко, М.В. Петрушен. // Системи управління, навігації та зв'язку, 2014,. – 2014. – С. 141–145.

2. CybExer Technologies. Лига киберзащиты Эстонии принимает участие в учениях по кибербезопасности, организованных CybExer и EY [Електронний ресурс] / CybExer Technologies // Блог компании Positive Technologies. – 2019. – Режим доступу до ресурсу: https://cybexer.com/estonian-cyber-defence-league-takes-part-in-cyber-security-exercise-hosted-by-cybexer-and-ey/.

3. Positive Technologiesберугрозы. I квартал 2019анія. Актуальные киберугрозы. I квартал 2019 [Електронний ресурс] / Positive Technologiesберугрозы. I квартал 2019анія // Блог компании Positive Technologies. – 2019. – Режим доступу до ресурсу: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-q1-2019/.

*УДК 32.019.5*

**Галєєв В. А.**
кандидат соціологічних наук, доцент
**Омельченко О. А.**
кандидат політичних наук,
Академія зовнішньої розвідки України

## ЗАХИСТ ІНФОРМАЦІЙНОГО ПРОСТОРУ В КОНТЕКСТІ БЕЗПЕКОВОЇ ПОЛІТИКИ УКРАЇНИ

У сучасному світі інтернет-простір перетворився на поле битви на всіх рівнях: інтелектуальному, цифровому, інституціональному.

Захист інформаційного простору є серйозним завдання не лише для будь-якої розвиненої держави та її соціально-культурного середовища, а й для різних сфер і груп впливу. Інтернет-ресурси стають ключовим компонентом забезпечення національної безпеки, зокрема у системі захисту кіберпростору держави.

Національна безпека, національні інтереси та інформаційний вплив – взаємопов'язані складові суспільно-державних відносин, які мають важ-

ливе значення для будь-якої нації з огляду на необхідність попередження та ліквідації загроз суверенітету, територіальній цілісності та прогресивному розвитку країни. Важливим для України є визначення сутності національних інтересів в нових геополітичних умовах, з'ясування особливостей національної безпеки в ракурсі агресивної політики Російської Федерації, грамотне ведення інформаційної боротьби та вигідне позиціонування нашої держави на міжнародному рівні.

Характерною ознакою сучасного протистояння між державами є геополітичний інформаційний вплив. Це – один із сучасних засобів міждержавної боротьби, що здійснюється з метою порушення інформаційної безпеки супротивника, при одночасному захисті від аналогічних дій з його боку. Агресивний воєнний сценарій часто тісно переплетений із інформаційними операціями: маніпуляціями, дезінформацією, інсинуаціями та відкритим обманом. А іноді силові маневри спрямовуються виключно на нав'язування політичної волі та ґрунтуються на інформаційних атаках для дестабілізації внутрішнього суспільно-політичного життя.

Саме тому головним нормативно-правовим актом з питань інформаційної безпеки має стати концепція інформаційної боротьби, захисту інформаційного простору, протиборства з кібертероризмом і проектування мережевої системи захисту.

Сучасна боротьба української нації за власний суверенітет і незалежність є інформаційним протистоянням, яке має здійснюватися за наступними напрямками:

– інформаційна розвідка (пошук, збір, обробка й аналіз відомостей про інформаційні ризики та загрози);

– планування інформаційних заходів тактичного (локального), оперативного (що торкається сусідніх держав) та стратегічного (разом із світовою спільнотою) рівнів;

– проведення активних дій інформаційного характеру з метою реалізації завдань внутрішньої та зовнішньої політики;

– оцінка ефективності інформаційних заходів і визначення рівня досягнення успіху.

Сьогодні в Україні за умов недосконалої інформатизації суспільства, за відсутності вивчення досвіду розв'язання питань щодо створення сучасного інформаційного простору та системи його захисту посилюються загрози національній безпеці, поширюється зовнішній інформаційно-психологічний вплив, що призводить до величезних політичних, воєнних, моральних і суспільних збитків.

У нашій державі за роки незалежності вийшла значна кількість наукових праць щодо проблем національної безпеки, зокрема захисту інформаційного простору. Питання інформаційної безпеки найчастіше пов'язувалося з технічним і криптографічним захистом інформації. Проте

в умовах гібридних війн (як економічних, так і політичних) пріоритетом є захист громадян і суспільства від негативних інформаційних впливів, поширення неправдивої інформації тощо.

Забезпечення інформаційної безпеки ґрунтується на детальному аналізі структури та змісту управління, а також інформаційних процесів і використання при управлінні відповідних технологій. При цьому визначальними факторами при розробці засобів інформаційної зброї мають стати саме індивідуальні особливості людини, соціальних груп і соціуму. Для того, щоб змоделювати поведінку суспільства в разі інформаційної атаки, необхідно знати саме його індивідуальні особливості та переваги. Наразі інформаційна боротьба стає тим фактором, що впливає на саму гібридну війну, її початок, хід і результат.

Актуальною проблемою безпеки України є аналіз факторів інформаційних впливів та протидії інформаційній зброї, за яким має слідувати розробка концепції захисту системи інформаційно-аналітичного забезпечення завдань інформаційної боротьби. Саме такий підхід, на нашу думку, дозволить протидіяти зовнішній інформаційній ескалації в Україні.

**Література**

1. Петрик В., Кузьменко А., Остроухов В., Соціально-правові основи інформаційної безпеки: навч посіб., К.: Росава, 2017. – 496 с.

2. Хорошко В., Хохлачова Ю., Прокофьєв М., «Концепція застосування інформаційних впливів та протидії інформаційній зброї», Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. Вип. 1 (31), 2016. – С. 9-24.

3. Libicki M., Conquest in cyberspace. National security and information warfare, Cambridge, 2019. – 207 p.

*УДК 351.004*

**Горовий В. М.**
доктор історичних наук, професор,
заслужений діяч науки і техніки,
Національна академія СБ України

## ПРОБЛЕМА ДОСТОВІРНОСТІ ІНФОРМАЦІЇ В СУЧАСНИХ СОЦМЕРЕЖАХ

Здобутки науково-технічного прогресу останніх десятиліть обумовили якісно новий етап у розвитку суспільства на основі нових інформаційних технологій, створили умови для загальної інформатизації. Насамперед цей процес обумовив забезпечення масового доступу до наявних у суспі-

льстві інформаційних ресурсів практично всім членам суспільства. Реалізація цих можливостей, поряд із розвитком доступних для користування всієї соціально активної частини населення соціальних комунікацій, можливостей нового інфотворення, сприяє організації активних інформаційних обмінів.

Характерною ознакою цих обмінів в умовах інформаційного суспільства є зниження вертикальної регламентації і стрімке збільшення контактів горизонтального спілкування, активне використання при цьому технологій соціальних мереж.

Розвиток соцмереж став переконливим свідченням успішного впровадження глобальної інформатизації на території нашої країни. Згідно з інформацією про останні рейтинги визначення популярності соціальних мереж в 2019 році серед 2000 респондентів по всій Україні, за винятком окупованих Росією територій, найпопулярнішою серед них в Україні є Facebook – нею користуються 50% респондентів. Про це свідчать дані опитування компанії Research & Branding Group[1]. Як зазначають соціологи, за період з травня 2018 року в Україні помітно збільшилося число таких користувачів соцмереж, як Facebook (до 50%), YouTube (30%), Instagram (27%) і суттєво зменшилася кількість таких користувачів соцмереж, як Одноклассники (6%) до і ВКонтакте (10%).

Найчастіше українські користувачі соцмереж користуються ними для спілкування з друзями (60%). Новини та події в країні і в світі цікавлять 36% респондентів. Характерним при цьому є те, що платні послуги в користувачів становлять лише (2%) відвідувань мереж, а питання ведення бізнесу – лише (1%). Не дивлячись на масове користування громадян України соціальними мережами, низькі проценти їх використання в діловій сфері свідчать про початковий етап входження цих технологій спілкування в соціальну практику обміну інформацією в Україні.

Технології інформаційних обмінів у соцмережах сприяють розвитку громадянського суспільства, його консолідації на якісно новому рівні розвитку. Винахідник Всесвітньої мережі «Інтернет» Тімоті Бернерс-Лі у книзі «Заснування Павутини» зазначає: «Мережа – це більше соціальне, ніж технічне явище». Задумував я її для досягнення результату – допомогти людям працювати разом, – а не як технічну іграшку. Найзагальніша мета Мережі – підтримка і поліпшення нашого існування у світі, яке саме багато в чому є мережевим»[2]. У той же час на нинішньому етапі свого розвитку соціальні мережі можуть створювати і певні небезпеки націона-

[1] https://www.rbc.ua/ukr/news/sostavlen-reyting-populyarnosti-sotsialnyh-1555070035.html.

[2] Бернерс-Лі Т. Заснування Павутини: З чого починалася і до чого прийде Всесвітня мережа / Т.бернерс-Лі, М. Фічетті; Пер. з англ. А.Іщенка. – К.: Вид. дім «Києво-Могилянська академія», 2007. – С.107.

льному інформаційному простору України у зв'язку із недостатнім розвитком технологій нейтралізації негативних, в умовах інформаційної війни, і відкрито ворожих, впливів на процеси інформаційних обмінів у суспільстві.

Зважаючи на вільний, практично неконтрольований доступ до участі в спілкуванні у соцмережах для кожного дієздатного члена суспільства, як досвідченого в такого роду спілкуванні, так і недосвідченого, як компетентного в порушуваній тематиці, так і некомпетентного, як відповідального за створюваний контент, так і безвідповідального, в соціальних мережах насьогодні ще не вробились надійні механізми забезпечення достовірності інформації, присутні зумисно чи ненавмисно поширювані плітки та неточна, викривлена інформація.

При всьому цьому соціальні мережі стають все більш ефективним джерелом взаємного інформування в сучасному суспільстві. Адже джерело дружнього спілкування, як свідчить соціологія, стало дуже вагомим і значимим у суспільному взаємоінформуванні, у формуванні поглядів на навколишню дійсність. І довіра до такого спілкування в обмінах думками з друзями, знайомими, людьми, авторитетними для учасників спілкування камуфлює його недоліки і часто використовується зловмисниками і некомпетентними людьми для дезінформування, створення хибних точок зору на суспільнозначимі процеси. У той же час «за результатами багатьох досліджень, соціальні мережі роблять молодь, і особливо представників покоління міленіалів (люди, які народилися у період з 1981 по 1994-2000 роки) та покоління Z (люди, які народилися в період між 1995 та 2000 роками) більш політично активними»[1].

Боротьба з пліткарством у соцмережах має дуже велике значення в умовах сучасної інформаційної війни. Але при цьому вона також має і довготривале, перспективне значення, оскільки підвищення достовірності інформаційних обмінів в соцмережах має підняти ефективність цієї нової, але перспективної в розвитку інформаційного суспільства технології спілкування в суспільнозначимих вимірах: в розвитку інформаційних послуг в бізнесі, освіті і т.п. Оскільки даний процес є суспільно значимим, державні інформаційні, інформаційно-аналітичні та аналітичні структури мають виробити і реалізовувати централізовану політику стосовно соцмереж, спільні підходи стосовно підвищення реальної дієвості цих інструментів сучасних інформаційних обмінів.

Насамперед, в обоймі засобів боротьби з пліткарством в соцмережах мають бути чіткі уявлення про перспективи суспільного розвитку власного суспільства, організація популяризації орієнтирів розвитку, визначених Президентом, урядовою програмою, іншими документами, що відображають тренди розвитку суспільства, його соціальних структур. Дієвість

[1] Соціальні мережі та демократія: тисячі ботів і тролів поширюють «фейкові новини» // https://www.radiosvoboda.org/a/29166101.html.

ції популяризації буде залежати від того, наскільки владні структури зможуть показати вплив запланованих змін на життя первинних соціальних структур суспільства, конкретних його членів. При належній організації популяризації орієнтирів вони будуть відігравати не лише стержневу роль у створенні певних інформаційних систем орієнтації для учасників спілкування в мережах у насиченому інформаційному просторі, але й матимуть певне упереджувальне значення в боротьбі з дезінформацією.

Важливою умовою боротьби з пліткарством в соцмережах є обов'язкова постійна присутність держави, її інформаційно-аналітичних структур, в тому числі бібліотечних, в соцмережах. Успішна боротьба з цими явищами обумовлює також необхідність постійного вивчення інформаційного противника, розвитку форм його діяльності, прогнозування перспектив його диверсійної діяльності в національному інформаційному просторі України, добору аргументації і т.д. Інформування учасників соцмереж про очікувані вкиди в національний інформаційний простір неправдивої інформації значно знижує її ефективність.

У боротьбі з пліткарством слід мати на увазі і міжнародні напрацювання. Так, «*Google* вже працює над індексом надійності, що визначає та демонструє градус достовірності змісту певного повідомлення. «Такі заходи працюватимуть на алгоритмах, а це породжує побоювання, що вони обмежать вільне поширення інформації в Інтернеті», – пояснює Мішела дель Вікаріо *(Michela Del Vicario)* з лабораторії комп'ютерної соціології в Люуці (Італія), Мовляв, у такому разі відбуватиметься щось на кшталт цензури»[1]. У той же час Facebook намагається знайти інші форми боротьби з недостовірною інформацією в мережах. Ставка при цьому робиться на зростання свідомості користувача, який у стрічці новин зможе позначити повідомлення, яке він вважатиме несерйозними чи фейковими[2].

У наших публікаціях вже не раз піднімалося питання про вдосконалення правового забезпечення розвитку електронного спілкування, що постійно відстає від розвитку нових інформаційних технологій. Серед гострих проблем у цій сфері фахівці виділяють безпеку і захист персональних даних, відсутність уніфікованих принципів правового регулювання відносин у соціальних мережах, захист та критерії відповідальності за порушення прав інтелектуальної власності, проблеми правового регулювання реклами, електронної комерції і використання товарних знаків у соціальних мережах та ін.

Таким чином, можемо приєднатися до думки американського політичного науковця та економіста Франсіса Фукуями у виданні The Atlantic[3] про те, що більше інформації завжди краще. Однак, сучасна практика сві-

[1] https://zbruc.eu/node/45985.

[2] https://zbruc.eu/node/45985.

[3] https://www.radiosvoboda.org/a/29166101.html.

дчить, що в епоху інтернету, коли тисячі ботів і тролів можуть посилювати розповсюдження дезінформації, «надання хорошої інформації, яка зрештою протидіятиме поганій» є безсумнівно важливим, але не єдиним напрямом підвищення достовірності інформаційних обмінів в мережах. Паралельно суспільство має вдосконалювати також і відповідні регулятивні механізми, які забезпечать використання самої по собі нейтральної платформи нового способу спілкування в інтересах суспільного прогресу.

*УДК 342.571*

**Губський В. М.**
помічник-консультант народного депутата України

## ВПЛИВ ГРОМАДСЬКИХ ОРГАНІЗАЦІЙ НА ФОРМУВАННЯ ТА РЕАЛІЗАЦІЮ ДЕРЖАВНОЇ ПОЛІТИКИ УКРАЇНИ

Проблеми нашої держави все більше і більше виходить за рамки кабінетів високих політиків та стають турботою простих українців. Слід визнати, що на сьогодні існує велика недовіра українського суспільства до влади, суду та в цілому правової системи України, а громадські організації та їх представники мають великий авторитет, до їх думок населення прислухається.

В сучасному демократичному суспільстві є нормою зростаюча соціально-політична активність громадян та їх безпосередня участь в житті держави.

Так, статтею 36 Конституції України проголошено, що Громадяни України мають право на свободу об'єднання у політичні партії та громадські організації для здійснення і захисту своїх прав і свобод та задоволення політичних, економічних, соціальних, культурних та інших інтересів [1].

Постанова Кабінету Міністрів України «Про забезпечення участі громадськості у формуванні та реалізації державної політики» від 3 листопада 2010 р. № 996 передбачає утворення тимчасових консультативно-дорадчих органів – Громадських рад при міністерствах, інших центральних органах виконавчої влади та місцевих державних адміністраціях [2].

До складу таких громадських рад можуть бути обрані представники громадських об'єднань, релігійних, благодійних організацій, творчих спілок, професійних спілок та їх об'єднань, асоціацій, організацій роботодавців та їх об'єднань, недержавних засобів масової інформації, які зареєстровані в установленому порядку і провадять діяльність на території України. Строк повноважень громадської ради становить 2 роки [2].

До складу громадських рад не можуть бути обрані лише ті особи, які є депутатами всіх рівнів, посадовими особами органів державної влади, ор-

ганів влади Автономної Республіки Крим та органів місцевого самоврядування [2].

Попри те, що відповідно до законодавства рішення громадських рад мають рекомендаційний характер, вони є обов'язковими для розгляду органом при якому створені. А рішення органу, прийняте за результатами розгляду пропозицій громадської ради, не пізніше ніж у десятиденний строк після його прийняття в обов'язковому порядку доводиться до відома членів громадської ради та громадськості шляхом його оприлюднення на офіційному веб-сайті органу та в інший прийнятний спосіб. Інформація про прийняте рішення має містити відомості про врахування пропозицій громадської ради або причини їх відхилення.

Із переваг участі у консультативно-дорадчих органах хочу відмітити наступні:

– можливість брати участь у формуванні та реалізації державної політики;

– оперативно отримувати інформацію щодо можливих змін в законодавстві з того чи іншого питання, надавати свої пропозиції та рекомендації;

– законним шляхом лобіювати прийняття чи неприйняття певних рішень державним органом;

– законним та етичними методами позбутися конкурентів у певному сегменті ринку, на який має вплив державний орган;

– отримання нових, корисних зв'язків, як серед членів громадської ради, так і серед представників державного органу, від простих спеціалістів до керівництва.

На мою думку, досить гарним прикладом діяльності громадської ради є Громадська рада при Міністерстві екології та природних ресурсів України, яка діяла з грудня 2016 р. по грудень 2018р.

«Громадська рада при Мінприроди за два роки своєї роботи провела ряд громадських експертиз, підготувала близько 200 рекомендацій та опрацювала понад 30 нормативно-правових актів. Переважна кількість рекомендацій, наданих Громадською радою, були враховані Мінприроди», – зазначав тодішній Міністр екології та природних ресурсів України Остап Семерак [3].

Отже, хочу підкреслити, що не тільки олігархи за допомогою «ручних» депутатів можуть лобіювати прийняття вигідних для себе законів. А і звичайні громадяни, цілком законно, можуть просувати ту чи іншу позицію завдяки членству у громадських радах при органах державної влади.

Повертаючись до теми національної безпеки, хочу зазначити, що агенти спецслужб іноземних держав, на мою думку, без особливих зусиль можуть ставати членами таких громадських рад, як від «легендованих» професійних об'єднань та асоціацій, так і від зовсім нейтральних громадських організацій.

Слід згадати про так звану «агентуру впливу» – агентуру з числа осіб, що належать до державних і громадських діячів, лідерів громадської думки, що завдяки своєму суспільному становищу можуть здійснювати вигідний для супротивнка вплив на вирішення питань державної політики, позицію громадянського суспільства, масові настрої тощо[4].

Пріоритетом функціональної спеціалізації агентури впливу є не підривна діяльність та збір розвідувальної інформації, а окремі дії, що сприяють комплексному та довгостроковому просуванню інтересів іноземної держави та розкладанню суверенітету української держави [4].

Із недавніх прикладів, не дивлячись на презумпцію невинуватості, хочу навести наступну інформацію. Засновник ветеранської організації, будучи з 2019 р. членом громадської ради при Комітеті Верховної Ради України з питань соціальної політики та захисту прав ветеранів став помічником-консультантом народного депутата України (голови Комітету). А навесні 2014 року він активно підтримував анексію Криму державою-агресором, в результаті чого отримав Російське громадянство (за інформацією Харківської міської громадської організації «Союз Чорнобиль»). Висновки приходять самі собою.

Підсумовуючи вищезазначене, можна стверджувати, що потрібно законодавчо закріпити більш суворі вимоги для членства в громадських радах та запровадити проходження спеціальної перевірки для кандидатів в їх члени.

**Література**

1. Конституція України від 28.06.1996 № 254к/96-ВР. Поточна редакція від 01.01.2020, [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/254к/96-вр.

2. Постанова Кабінету Міністрів України «Про забезпечення участі громадськості у формуванні та реалізації державної політики» від 3 листопада 2010 р. № 996 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/996-2010-%D0%BF.

3. За два роки Громадська рада при Мінприроди надала близько 200 рекомендацій та опрацювала понад 30 нормативно-правових актів, [Електронний ресурс]. –- Режим доступу: https://menr.gov.ua/news/32853.html.

4. Як працює українська контррозвідка, [Електронний ресурс]. – Режим доступу https://glavcom.ua/columns/mikhalchishin/yak-pracyuje-ukrajinska-kontrrozvidka-649589.html.

*УДК: 94(477)*
**Гуз А. М.**
доктор історичних наук, професор,
Національна академія СБ України

# ЗАХИСТ ТАЄМНОЇ ІНФОРМАЦІЇ В УКРАЇНСЬКОМУ ВИЗВОЛЬНОМУ РУСІ В 20-50 РОКИ ХХ СТ.

Проблеми захисту інформації з обмеженим доступом були актуальними на різних етапах українського державотворення. Не менш важливими є вони й у сучасних умовах. У 20-50-х роках ХХ ст. представники українського визвольного руху (УВО, ОУН, УПА) виробили чимало специфічних способів захисту інформації, які є актуальними і в наші дні та потребують вивчення.

У нашому дослідженні спробуємо охарактеризувати, яку інформацію у визвольному русі відносили до таємної, які способи захисту та зберігання таємної інформації використовували, які інструктивно-розпорядчі акти регулювали цю діяльність, а також на які підрозділи було покладено функції її захисту.

Спочатку спробуємо визначити ті види інформації, які в українському визвольному русі відносили до таємної. Найбільш важливими даними, які захищалася, на наш погляд, були: персональні дані учасників визвольного руху; військова інформація; коди та методи шифрування; питання конспірації; про «живий» та «мертвий» засоби зв'язку, а також пункти зв'язку; про діяльність структурних підрозділів визвольного руху; про підпільну мережу; про дислокацію й будівництво криївок; про систему оперативного обліку, діловодство та збереження справ в «архівах» тощо.

Український повстанський рух виробив специфічні способи захисту та збереження таємної інформації. Насамперед до таємної інформації обмежували доступ. Окремим документам присвоювався гриф обмеження доступу – «довірочно», «суворо довірочно» та інші. В усіх учасників визвольного руху виховувалися морально-психологічні якості, а саме: мовчазність, холоднокровність, уміння виробляти бездоганне алібі. Конспірація стала одним із способів захисту учасників визвольного руху. Розглядали питання запровадження органів цензури. Для утаємничення важливої інформації про повстанський рух використовували елементи криптографічного захисту, зокрема кодування, шифрування й тайнопис. Для шифрування використовували простий шифрувальний квадрат, складний шифрувальний квадрат, шифрування за допомогою підпільної або іншої літератури, шифрування цифровим ключем, шифрування за допомогою заміни літер [1].

Крім того, з метою захисту таємної інформації у 40-х роках 20 ст. воякам УПА рекомендувалося: завести «скритки» (сейфи, шафи тощо) для

зберігання таємних документів у штабах та помешканнях командного складу; обмежити коло осіб, з якими й у присутності яких обговорюються таємні справи; усі приміщення штабів та командні пункти «строго законспірувати»; вжити заходів до належного зберігання секретної документації, карт, не потрібну документацію спалювати; запровадити шифри та коди для забезпечення секретності у паперових повідомленнях, радіоперемов тощо; засекретити місця дислокації частин і загонів УПА; щоденно виділяти 10-20 хвилин для проведення виховної роботи з особовим складом, роз'яснення значення та способів зберігання військової таємниці; бойові накази віддавати безпосередньо перед початком операції; зберігати у таємниці від населення плани з передислокації військ [2]. Відповідальність за дотримання режиму секретності покладалося особисто на командирів та функціональних начальників. За розголошення військової таємниці учасників визвольного руху притягували до суворої відповідальності – смертна кара.

Визвольний рух виробив також специфічні способи зберігання матеріальних носіїв таємної інформації. Вона розміщувалася, як правило, в таємних схронах, в «архівах», де зберігалися звіти, протоколи, хроніки, «життєписи» або спогади вищого керівництва підпілля, гасла, щоденники, бофони, криптоніми підпільна пошта, списки втрат учасників визвольного руху, звітна документація інші важливі документи. Усі ці таємні документи ховали у молочний бідон, і коли він заповнювався – закопували в лісі. Перед тим його просмолювали і запечатували для кращого зберігання [3]. В учасників повстанського руху це стало одним із основних способів зберігання таємних документів. На сьогодні дослідниками знайдено понад 40 таких бідонів з документи про події повстанського руху 40-50 років 20 ст. Для зберігання таємних документів також використовувалися спеціально відведені місця криївок або спеціальні схрони.

З метою забезпечення охорони таємної інформації в повстанському русі було видано низку «вишкільних матеріалів», інструктивно-розпорядчих актів, наказів, які конкретизували й нормативно забезпечували порядок захисту такої інформації. Зокрема, це брошури з основ конспірації: «Пашні буряки», «Конспірація, Конспірація та секрет; наказ командувача УПА № 10 від 10 вересня 1943 р. «Про зберігання військових таємниць»; Інструкція з конспірації 1944 р.; Положення «Конспіративно-розвідчого вишколу» тощо. Здійснювалися також спроби створення підрозділів, які мали забезпечувати охорону таємниці повстанського руху. Так, окремі функції із захисту таємної інформації підпілля у різні часи покладалися на: референтуру УВО, СБ ОУН, СБ УПА.

Таким чином, вироблені українським визвольним рухом в 20-50-х роках 20 ст. специфічні способи захисту інформації сприяли його боротьбі за незалежну українську державу.

**Література**

1. Іщук О.С., Ніколаєва Н.Б. Методи зашифрування кореспонденції у підпіллі ОУН і УПА та їх розшифрування органами державної безпеки УРСР в 1944-1954 рр. – К.: 2017. – 38 с.

2. Кентій А. В. Українська повстанська армія в 1942-1943 рр. – К.: Інститут історії України НАН України, 1999. – С. 13.

3. Таємниці молочних бідонів: що приховують «капсули пам'яті УПА»?/https://www.bbc.com.

*УДК316.485.6:351.746.1(477)*

**Давиденко М. О.**
кандидат юридичних наук,
Національна академія СБ України

## ПРОТИДІЯ СБ УКРАЇНИ ПОШИРЕННЮ ІДЕОЛОГІЇ ТЕРОРИЗМУ В ІНФОРМАЦІЙНОМУ СЕРЕДОВИЩІ

На сьогодні в АР Крим, окупованих територіях Донецької та Луганської областей з позиції РФ та т.зв «ДНР»/«ЛНР» проводяться інформаційно-психологічні кампанії, які дезінформують суспільство, несуть загрозу територіальній єдності країни, пропагують терористичну та екстремістську діяльність, стоять на заваді проведенню державної політики у сфері європейської та євроатлантичної інтеграції».

Наприклад, технологіїінформаційної блокади, що активно застосовувалась під час анексії Криму, були спрямовані на формування інформаційного вакууму для українських засобів масової інформації в АР Крим з метою безальтернативного подання фактівпро події в Україні та Криму, забезпечуючи єдину інтерпретацію подій. Поряд з цим, низка журналістів піддавалися силовому тиску – відбувалися стеження і профілактичні бесіди з боку спецслужб РФ, прослуховування їх розмов і читання листування, погрози фізичної розправи з подальшим викликом спецслужб, звинувачення в іноземному фінансуванні тощо.

На наш погляд ідеологія тероризму є одним із різновидів ідеології ненависті. Ідеологія ненависті – духова настанова, спосіб мислення, ідеологічна течія, яка обстоює необхідність корінних змін у суспільстві, державі та політиці, шляхом насильницьких дій, спрямованих на розпалювання ворожнечі та ненависті, приниження честі та гідності окремих осіб, включаючи пошкодження майна та вбивства, заперечує право інших на власну позицію та легітимізує використання всіх методів для доведення власної правоти.

Як зазначають науковці, основою ідеології ненависті загалом вважається поширення в суспільстві «чорно-білого» (бінарного) світосприйнят-

тя [1, с. 186]. Так, дослідник Л. Баєва зазначає, що «формування настанови на агресію щодо іншого відбувається в тому випадку, коли людина звикла некритично ставитись до своїх поглядів і вчинків та вважає себе незрівнянно вищою за інших» [2, с. 21].

Дослідники визначають поняття "ідеологія тероризму" як систему ідей, теорій, понять, поглядів, звичаїв, традицій, що існує на рівні теоретичної й повсякденної свідомості суб'єкта історичної дії й обґрунтовує необхідність насильства або погрозу його застосування, спрямованого на соціально-психологічне залякування при досягненні злочинних цілей; звідси "поширення ідеології тероризму" – розповсюдження з метою доведення до населення ідеології тероризму [3, с.110].

Так, на сьогодні через медіа-контент, який отримав символічну назву серед мусульманських країн *«медіа-джихад»,* поширюються професійно зняті відеоролики с публічними стратами, знищенням пам'ятників культури, інтерв'ю з їх польовими командирами і активістами, фото трофеїв і вбитих противників. Схожі відеоматеріали поширюються і бойовиками т.зв. «ДНР»/«ЛНР».

На наш погляд, сучасна протидія СБ України поширенню ідеології тероризму в сучасному інформаційному середовищі має здійснюватися через систему взаємоузгоджених заходів, які застосовуються комплексно. Основними з них є:

1. Організація інформаційно-пропагандистської і ідеологічноїдіяльності органів влади та правоохоронних структур.

2. Розвінчування ідеології тероризму (його антологічних і гносеологічних основ).

3. Здійснення «деромантизації» терористичних лідерів у медійному середовищі.

4. Контроль і протиборство щодо поширення ідеології тероризму у мережі Інтернет (блокування сайтів, публікацій на форумах, соціальних мережах тощо).

5. Організація інформаційного контролю за середовищем молоді.

Таким чином, інформаційна антитерористична пропаганда має стати ключовим елементом антитерористичної стратегії в державі у ході попередження поширення ідеології тероризму в інформаційному середовищі. На сьогодні здійснення контрпропагандистської антитерористичної діяльності є одним із пріоритетних завдань СБ України у ході попередження сепаратизму та терористичних актів на окупованих територіях та низці суміжних областей.

Вважаємо, що протидія поширенню ідеології тероризму має здійснюватися таким чином, щоб попереджати й викривати всі тематичні блоки пропаганди т.зв. «ЛНР/ДНР», опираючись при цьому також на змістовні дані і факти, бажано з іноземних джерел. Основним кроком до успішного її здійснення є проведення першочергових контрпропагандистських захо-

дів у молодіжному середовищі з метою попередження входження молоді до незаконних збройних формувань та вчинення терористичних актів.

**Література**

1. Антонян Ю. М. Терроризм: Криминологическое и уголовно-правовое исследование / Ю. М. Антонян. – М.: Щит-М, 1998. – 306 с.

2. Баева Л.В. Экстремизм: природа и формы проявления / Л. В. Баева // Каспийский регион: политика, экономика, культура. – 2008. – № 3. – С. 21-25.

3. Метелев С.Е. Современный терроризм и методы антитеррористической деятельности : моногр. / С. Е. Метелев. – М. : ЮНИТИ-ДАНА, 2008. – 275 с. – 67.628 / М 541. – ДВГНБ.

*УДК 355. 402*

**Давидюк А. В.**
Інститут проблем моделювання
в енергетиці імені Г.Є Пухова НАН України

## СЕРЕДОВИЩЕ ТА РИЗИКИ ФОРМУВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

З розвитком інформаційних технологій та широкою доступністю глобальної мережі Інтернет обсяги даних безперервно збільшуються і ми все більше починаємо залежати від них. Проте часто вплив інформації на людину є недооціненим.

Не зважаючи на розвиток технічних засобів захисту, людина залишається найуразливішим місцем будь-якої інформаційно-телекомунікаційної системи. Враховуючи це, доцільним є впровадження процесу оцінювання ризиків інформаційної безпеки [1].

Сьогодні оцінювання ризиків може здійснюватися з використанням різних методів та методик [2]. Однак основою у більшості з них є суб'єктивна оцінка експерта та не приділяється належної уваги інформаційному середовищу.

Отже, що є інформаційним середовищем? Під інформаційним середовищем будемо розуміти середовище, що існує у часі та просторі між джерелом інформації та її приймачем. Таке середовище може існувати як з використанням технічних засобів, так і без них.

Щодо захисту інформації з використанням технічних засобів в нашій державі існують нормативні документи та відповідне законодавство в сфері технічного захисту інформації, а щодо захисту інформації у середовищі з відсутністю технічних засобів є більш складною.

Проблема захисту інформації у такому середовищі знаходиться у компромісі між правом на анонімність (приватність) та контролем за по-

ширенням інформації. Як оцінити ризики інформаційної безпеки за умов такого компромісу.

У загальному випадку під ризиком інформаційної безпеки розуміють добуток імовірності настання несприятливої події на величину можливого збитку [3]. У нашому ж випадку необхідно оцінити імовірність вчинку конкретної людини на конкретному місці(посаді). Дана задача потребує вивчення її поведінки на певному проміжку часу, аналізу психологічного стану та потреб. Звісно, на це не завжди є час і ресурси. Тоді постає питання як створити такі умови (середовище) за яких людина не матиме потреби сприяти витоку інформації або матиме страх перед вчиненням таких дій. Вирішення такого роду проблеми полягає в управлінні (маніпулюванні) загальнолюдськими цінностями. Для цього потрібно їх визначити. На професійному шляху до таких цінностей можна віднести довіру та повагу оточуючих (колег, сім'ї), грошове забезпечення, можливість кар'єрного зростання тощо.

Та чи є забезпечення усіх цих благ гарантією безпеки. Звісно, ні, проте підвищує ціну інформації, тим самим зменшуючи існуючі ризики. Однак, не зважаючи на вище вказане, найбільш цінним є для будь-якої людини свобода вибору – де, з ким, за скільки працювати. Найчастіше саме цей фактор визначає вибір співробітника.

Враховуючи це, величина ризику настання яких-небудь обмежень для людини повинна бути не меншою за величину ризику інформаційної безпеки для організації. Саме цей принцип, не залежно від механізму його реалізації, повинен стати невід'ємною частиною договору щодо нерозголошення і бути впровадженим у робочий процес, що пов'язаний з використанням конфіденційної інформації.

**Література**

1. ISO. (2020). ISO/IEC 27005:2018. [online] Available at: https://www.iso.org/ru/standard/75281.html [Accessed 22 Feb. 2020].

2. Sciencedirect.com. (2020). Information Security Risk - an overview | ScienceDirect Topics. [online] Available at: https://www.sciencedirect.com/topics/computer-science/information-security-risk [Accessed 22 Feb. 2020].

3. Enisa.europa.eu. (2020). BS 7799-3. [online] Available at: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/rm-ra-standards/bs-7799-3 [Accessed 22 Feb. 2020].

*УДК 351.746.1 + 004.9*
**Довгань О. Д.**
доктор юридичних наук, професор,
заслужений діяч науки і техніки України,
НДІ інформатики і права НАПрН України

# ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ В УМОВАХ ГЛОБАЛІЗАЦІЇ ТА ГІБРИДНОЇ ВІЙНИ ПРОТИ УКРАЇНИ

Стрімкий розвиток сучасних інформаційних технологій, інформаційних ресурсів, продуктів і послуг визнані керівництвом держави як пріоритетні для розвитку України.

Зазначене та процеси трансформації інформаційного суспільства в суспільство знань надають інформаційній сфері статусу однієї із базових для інноваційного розвитку країни.

Натомість, в умовах інформаційної агресії з боку Росії та виникнення нових глобальних викликів у інформаційній сфері, зміщення центру ваги вирішення спірних та конфліктних питань на всіх рівнях в інформаційний простір створили нові виклики і загрози в інформаційній сфері та спонукали до все більшого розуміння необхідності забезпечення інформаційної та кібернетичної безпеки в усіх сферах життєдіяльності людини, суспільства і держави.

Актуальними постають питання формування цілісної системи забезпечення інформаційного суверенітету, управління ризиками і можливостями новітніх викликів в інформаційній сфері, розбудови власних спроможностей і стратегічних комунікацій тощо.

Це насамперед пов’язано з процесами, що відбуваються в глобальному інформаційному просторі і характеризуються такими основними тенденціями та особливостями:

глобальні зміни і трансформації в інформаційній сфері формують новітні виклики і загрози, які становлять реальну загрозу безпеці людства та міжнародному правопорядку;

в інформаційному просторі спостерігається тенденція до поширення інформаційної агресії і насилля, маніпуляції свідомістю людини та суспільства;

періодично проводяться інформаційно-психологічні операції;

більшість країн світу зіштовхнулася з проблемами кібершпигунства, кібертероризму, кіберзлочинності та кібератаками на об’єкти критичної інфраструктури;

наслідки використання сучасної інформаційної зброї можуть призводити до реальної втрати державного суверенітету і територіальної цілісності країн світу.

Комплексний аналіз особливостей і тенденцій розвитку інформаційного суспільства в умовах євроінтеграції України, а також проблем правого забезпечення життєдіяльності людини, суспільства і держави в інформаційній сфері дає змогу дійти висновків, що системними проблемами, які стримують розвиток інформаційного суспільства в Україні є: недосконалість державної політики з питань формування перспективної інформаційної інфраструктури; недостатність темпів демократичних перетворень в інформаційній сфері; низька ефективність використання інформаційних, інноваційних, фінансових, матеріально-технічних, радіочастотних та інших ресурсів; невідповідність системи підготовки кадрів вимогам майбутнього ринку праці; незадовільні масштаби впровадження сучасних інформаційних технологій у різні сфери життєдіяльності людини, суспільства і держави; невпорядкованість законодавства в інформаційної сфері.

За даними Державної служби спеціального зв'язку та захисту інформації України кількість інцидентів в інформаційно-телекомунікаційних системах протягом останніх років не зменшується, а навпаки в умовах воєнного конфлікту численні атаки на цифрові ресурси України продовжувалися.

Тому питання кібербезпеки були останні роки в порядку денному Всесвітнього економічного форуму в Давосі. Згідно з доповіддю про глобальні ризики, кібератаки – на другому місці серед ризиків, які найбільше викликатимуть занепокоєння у бізнесу в усьому світі протягом наступних 10-ти років. Кібератаки на критичну інфраструктуру, оцінені п'ятим найбільшим ризиком у 2020 році, – стали новим нормальним явищем у таких галузях, як енергетика, охорона здоров'я та транспорт[1].

З урахуванням викладених та інших проблем, до пріоритетних заходів щодо розвитку національної системи кібернетичної безпеки України видається за доцільне віднести:

проведення аудиту інформаційних ресурсів органів державної влади та місцевого самоврядування, встановлення розробників, володільців автоматизованих інформаційних систем (інформаційно-аналітичних систем, систем електронного документообігу, баз даних, реєстрів тощо), балансоутримувачів цих систем, організації їх технічної підтримки, вартості розробки та утримання, наявності та потреб апаратних, програмних, організаційних, технологічних засобів і відповідних фахівців;

проведення аудиту стану забезпечення кібербезпеки та імплементації норм чинного законодавства у цій сфері, визначення потреб розвитку систем кіберзахисту в органах державної влади;

запровадження обов'язкових навчальних курсів з питань забезпечення інформаційної та кібернетичної безпеки у середніх та вищих навчальних закладах, підготовки фахівців за спеціалізаціями «інформаційне право»,

[1] Наталия Микольская. Пять важных выводов с Давоса // «Эксперт-Центр» (http://expert.org.ua/v-mire/2020/pyat-vazhnyh-vyvodov-s-davosa). 29.01.2020.

«інформаційна безпека», «кібернетична безпека», а також відродження національної школи підготовки шифрувальників та криптографів.

Крім того, на законодавчому рівні визначити засади забезпечення інформаційної безпеки України як однієї з основних конституційно визначених функцій держави. Прийняти Закон України «Про засади інформаційної безпеки України», який визначить основні засади державної політики, спрямованої на захист життєво важливих інтересів людини і громадянина, суспільства і держави в інформаційній сфері, систему суб'єктів забезпечення інформаційної безпеки та засади їх функціонування в умовах формування і розвитку інформаційного суспільства в Україні та глобального інформаційного простору, а також нову редакцію Закону України «Про захист персональних даних», в якому передбачити удосконалення системи захисту персональних даних та моніторингу її ефективності з огляду на виникнення нових загроз праву на приватність громадян у зв'язку з можливістю профілювання даних про особу.

Насамкінець, забезпечення інформаційної безпеки людини, суспільства і держави має дійсно стати системою, до якої будуть залучені не тільки силові структури, але й неурядові організації, приватний сектор, бізнес, експертні і наукові кола, незалежні ЗМІ та інші. Тільки комплексний всеохоплюючий підхід дозволить консолідувати суспільство і забезпечити його безпеку.

*УДК 355.40:358.12*

**Доля Ю. Г.**
Національний університету оборони України
імені Івана Черняховського

## ОСОБЛИВОСТІ ВИЯВЛЕННЯ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ

Ефективна протидія негативному зовнішньому інформаційно-психологічного впливу, зокрема на особовий склад військ (сил), може бути лише за умов її реалізації на науковій основі. При цьому щонайважливішим є вибір показника ефективності, яким у подальшому слід управляти шляхом відповідного впливу. Таким очевидним показником ефективності протидії слід вважати рівень морально-психологічного стану ЗС України. Звідси потреба в системі соціального управління, де головним об'єктом управління є рівень морально-психологічного стану ЗС України.

Важливо забезпечити стійкість такого управління, що досягається коли його схема (модель) функціонуватиме за кібернетичним принципом з наявністю, так званих, «прямого» і «зворотного» зв'язку. Функціями зазначеної моделі можуть бути:

виявлення впливу;

оцінка рівня впливу;

формування висновків із оцінки рівня впливу та рішення щодо необхідності протидії;

планування заходів протидії впливу, затвердження плану заходів протидії;

реалізація заходів протидії впливу відповідно до плану;

контроль дієвості реалізованих заходів протидії впливу та їх коригування.

Кібернетична модель протидії негативному інформаційно-психологічному впливу буде діяти ефективно, коли її алгоритм роботи передбачатиме чітку кількісних вимірів, особливо параметрів (характеристик) стану цільової аудиторії, стан якої є об'єктом управління.

На практиці ця модель в МО України та ЗС України частково реалізується в межах формування необхідних тематик (меседжів). При цьому оцінка рівня негативного інформаційно-психологічного впливу здійснюється за його наслідками, тобто "постфактум" і опосередковано – через оцінку рівня морально-психологічного стану особового складу ЗС України, який є індикатором сукупного впливу на певні цільові аудиторії, що вже відбувся. Така оцінка, за діючими у ЗС України методиками, визначається в якісній узагальненій формі за принципом «здатність-нездатність». В той же час, цього недостатньо для здійснення випереджувальних стабілізаційних заходів (це мають бути заходи впливу як на особовий склад ЗС України, так і на шкідливі інформаційні джерела), оскільки такий підхід не передбачає кількісного оцінювання та аналізу динаміки негативного впливу, джерелом якого є інформаційний простір.

Аналіз джерел [1, с. 10; 2, с. 5] показує, що існує чимало високопрофесійних робіт щодо технічних аспектів впливу на соціальні об'єкти з метою стабілізації їх стану. Але дослідження з позицій кібернетичного принципу управління станом таких об'єктів на основі результатів моніторингу інформаційного простору держави в інтересах виявлення та оцінки інформаційного впливу у кількісному вимірі на певну цільову аудиторію, зокрема військову, ще не набули розвитку.

Першочергово визначимо, що інформаційно-психологічний вплив – це регульоване або нерегульоване інформаційне втручання у свідомість (підсвідомість) цільової аудиторії, яке може призвести до корекції її поведінки та (або) світогляду, зміни морально-психологічного стану. Сучасними регульованими інструментами інформаційно-психологічного впливу можуть бути технічні засоби (в першу чергу, радіо, телебачення, соціальні комп'ютерні мережі), друкована продукція, публічна голосова агітація, агентурна діяльність. Нерегульованими інструментами такого впливу є вербальне спілкування між людьми та їх власне спостереження певної реальності. Результа-

том сприйняття інформації може бути виникнення у цільової аудиторії позитивних або негативних емоцій, почуттів та реакцій (дій), які спрямовані на послаблення чи посилення волі, зміну здатності до активного опору, створення відчуття відчаю, страху, невпевненості або хоробрості, сміливості, рішучості тощо, що у підсумку і визначає рівень морально-психологічного стану цільової аудиторії [3, с. 32].

Для методичного оцінювання рівня негативного інформаційно-психологічного впливу на збройні сили необхідно мати певну сукупність показників, а для визначення його значимості, аж до критичного (допустимого) значення, – відповідні критерії. Виходячи із того, що деструктивні інформаційні процеси, які відбуваються в інформаційному просторі держави, доходять до військовослужбовців та залишають певне відображення у їх свідомості, можна стверджувати, що для кількісного оцінювання рівня такого впливу доцільно застосувати показник його інтенсивності як інтегральну характеристику (міру) дії на особовий склад військ усієї сукупності інформаційних процесів за певний період часу.

Таким чином, запропонований підхід щодо виявлення інформаційно-психологічного впливу дозволяє реалізувати методику, яка створює можливість оцінити в кількісному вимірі рівень інформаційно-психологічного впливу на особовий склад збройних сил за певний проміжок часу. Це дозволяє відповідному органу військового управління відносно об’єктивно прогнозувати можливі наслідки та адекватно і на випередження реагувати (протидіяти) негативним процесам.

**Література**

1. Вооруженные силы зарубежных государств: информационно-аналитический сборник / А.Н. Сидорин, Г.М. Мингатин, В.М. Прищепов, В.П. Акуленко. – М.: Воениздат, 2009. – 528 с.

2. Социальные сети: модели информационного влияния, управления и противоборства / Д.А. Губанов, ДА. Новиков, А.Г. Чхартишвили. – М.: ФИЗМАЛИТ, 2010. – 228с.

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.

*УДК 340*
**Євтушенко І. В.**
кандидат юридичних наук,
Інститут підготовки юридичних
кадрів для Служби безпеки України
Національного юридичного
університету імені Ярослава Мудрого

# ПРОБЛЕМИ РОЗВИТКУ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ ТА ЇХ ПОДОЛАННЯ

В повсякденному житті обмін інформацією здійснюється з неймовірною швидкістю та на значні відстані. Всі ми є користувачами інформаційного ресурсу, котрий розуміємо як впорядковані інформаційні масиви в електронному вигляді. Їх накопичення в свою чергу сприяє розповсюдженню інформації, що покращує зв'язок між людьми і сприяє розвитку цивілізації з відповідними покращеннями всіх сфер життєдіяльності. Однак, далеко не всі використовують зазначені масиви інформації на позитивне. Існує маса випадків коли інформаційні ресурси стають як об'єктами посягань кіберзлочинців з корисливих мотивів, або навіть для ведення інформаційних війн чи пригнічення потенціалу держав чи корпорацій. Вказане зумовило необхідність вивести поняття інформаційної безпеки та об'єднати зусилля держав по збереженню та захисту інформації, а також для створення умов, що забезпечують можливість швидкого відновлення реальних даних, якщо такі були спотворені або втрачені.

Конституцією України гарантування інформаційної безпеки визначено як одна з найважливіших функцій держави і справою всього українського народу, що зумовлено особливим її місцем у системі національної безпеки [1]. Національні інтереси реалізуються завдяки своєчасному та оперативному інформуванню; інформаційні системи стають об'єктами безпеки; питання національної безпеки безпосередньо пов'язані з питаннями міжнародної безпеки; завдання національної безпеки вирішуються з використанням різноманітних інформаційних ресурсів та інформаційних підходів як основного науково-практичного методу.

Існує визначення інформаційної безпеки, як стану захищеності систем обробки, та зберігання даних, яке забезпечує конфіденційність. Доступність та цілісність інформації, а також створення перешкод для несанкціонованого доступу інформації з подальшим її використанням, оприлюдненням, знищенням або спотворенням. І така безпека являє собою постійне балансування між інформаційною відкритістю та закритістю, між прагненнями максимально розширити доступ громадян до публічної інформа-

ції і максимально захистити інформацію корпоративного і приватного змісту [2].

Кризові події, що відбуваються в Україні у вигляді гібридної війни та спроможність розв'язати вказаний збройний конфлікт ускладнюється зокрема тим що одним із способів впливу є інформаційна війна за допомогою якої об'єкти критичної інфраструктури зазнають впливу нових технологій та новітніх способів втручання. Всі ми пам'ятаємо кібернетичну атаку за допомогою вірусу «Petya» який заблокував роботу багатьох серверів і на певний час була паралізована робота багатьох підприємств та установ, таких як «Ощадбанк» та інші.

А крім цього ми ще спостерігаємо втручання в медійний (інформаційний) простір України, що в свою чергу свідчить про певні проблеми в сфері захисту національної інформаційної безпеки. Має місце потужний інформаційний вплив країн-сусідів на наших громадян та недостатній інформаційний потік з України на закордонні спільноти. Значна частина ефірного часу теле-радіо-трансляцій заповнена кабельними мережами іноземного походження, в тому числі й з країни-агресора і навіть активні спроби блокування таких ресурсів не завжди завершується тотальним успіхом, оскільки технічні можливості дозволяють оминати певні перепони. Прикладом тому є блокування сервісів «Вконтакте», «Яндекс» та інших, однак ми всі помітили, що ці сервіси не повністю заблоковані, оскільки власники цих мереж задіяли динамічні IP-адреси, що дозволяє їм продовжувати свою діяльність [3].

Ми можемо спостерігати тенденцію того, що законодавство України постійно змінюється та вдосконалюється з урахуванням швидких мутацій та вдосконалень способів впливу на безпеку інформаційного простору та кібернетичної безпеки. Так, наприклад для захисту вітчизняного кіберпростору були прийняті нормативно-правові акти, що серед яких слід зазначити Стратегію кібербезпеки України, Рішення РНБО України «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», Закон України «Про основні засади кібербезпеки України» та інші документи у сфері кібербезпеки. Закон України «Про основи національної безпеки України» [4] яким визначались основні напрямки по забезпеченню інформаційного суверенітету України; вдосконаленню нормативно-правових актів для розвитку національної інформаційної інфраструктури та ресурсів, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну; активне залучення засобів масової інформації до запобігання і протидії корупції, зловживанням службовим становищем. Зазначений закон був замінений на Закон України «Про національну безпеку України», в якому вже визначено цілу довгострокову стратегію кібербезпеки України з визначенням пріоритетів національних інтересів України в цій сфері, визначено наявні та потенційні загрози ін-

тересам людини, громадянина, суспільства та держави в кіберпросторі та зазначені пріоритетні напрями стосовно безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави [5].

Таким чином слід зазначити що тенденції по вдосконаленню нормативно-правових актів в України відбуваються з метою постійного вдосконалення та забезпечення інформаційної безпеки, однак слід також зазначити, що самостійно протистояти проблемам кібербезпеки вкрай важко, а тому необхідна тісна співпраця на міжнародному рівні з європейськими країнами та структурами країн НАТО.

**Література**

1. Конституція України, 1996 року, // База даних «Законодавство України/ ВР України URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80 (дата звернення 02.03.2019).

2. Загальні проблеми інформаційної безпеки, URL: https://pidruchniki.com/10560412/politologiya/zagalni_problemi_informatsiynoyi_bezpeki (дата звернення 28.02.2019).

3. STRANA.UA. Стало известно, почему в Украине снова стали доступны сервисы Яндекса. Валерия Ивашкина 19:45, 2 июня 2017 URL: https://strana.ua/news/74134-stalo-izvestno-pochemu-v-ukraine-snova-dostupny-servisyyandeksa. html#.WTGW4Eelbfs.facebook (дата звернення 28.02.2019);

4. Закон України «Про основи національної безпеки України» 2003 р. // База даних «Законодавство України/ ВР України, URL: https://zakon.rada.gov.ua/laws/show/964-15 (дата звернення 05.03.2019).

5. Закон України «Про національну безпеку України», 2018 р. // База даних «Законодавство України/ ВР України, URL: https://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення 04.03.2019).

*УДК 351.863*

**Заславський В. А.**
доктор технічних наук, професор,
Київський національний університет
імені Тараса Шевченка

## РИЗИК-МЕНЕДЖМЕНТ ТА ІНФОРМАЦІЙНА БЕЗПЕКА СИСТЕМ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Сучасна методологія дослідження безпеки та ризиків базується на системних принципах при формуванні методів управління розвитком підприємств та суспільства і безпосередньо пов’язана з проблемою сталого розвитку і його важливими компонентами – забезпеченням безпеки життє-

діяльності та збереженням навколишнього природного середовища. Глобальна індустріалізація і урбанізація порушують природну рівновагу і здійснюють все більший тиск на природні ресурси та вимагають нових підходів до державного управління та забезпечення безпеки [2]. Це висуває складні політичні, соціально-економічні та екологічні проблеми, від розв'язання яких залежить стабільність розвитку як окремих регіонів, країн, так і людства в цілому [1, 3-5].

Особлива увага ризик-менеджменту приділяється при прийнятті рішень для забезпечення захисту критичної інфраструктури (систем з високою ціною відмови). Методи ризик-менеджменту використовуються аналітиками та експертами при проектуванні та науково-технічному супроводженні критичних інфраструктур [1-5]: складові державного управління, транспортні та енергетичні системи, космічна галузь, фінансові системи, безпека інформаційно-аналітичних систем та комунікаційних технології і т.д.

Складність дослідження ризиків пов'язана з їх різноманітністю, взаємозв'язками із процесами (соціальними, економічними, екологічними) та об'єктами різного рівня та масштабу, при цьому розглядаються: об'єкти державного та регіонального рівня, що визначають стабільність розвитку національної і регіональної економіки, пов'язані з реалізацією цілеспрямованого довгострокового (стратегічного) управління, і мають гарантувати необхідний рівень національної безпеки, умови стабільного та ефективного розвитку суспільства, забезпечення економічної ризик-захищеності. Важливими з позиції безпеки є проблеми міждержавного рівня, такі як: глобальні демографічні проблеми, питання охорони здоров'я та прав людини, проблеми розвитку інноваційних технологій та розміщення виробництв, стратегії розвитку енергетики та транспорту, охорона навколишнього середовища і зміна клімату, запобігання природних і техногенних катастроф та усунення їх наслідків, проблеми міжнародного тероризму та виробництва зброї масового знищення.

Сучасний ризик-менеджмент ґрунтується на ідеї, яка полягає у переході від стратегії реагування на певні події до стратегії передбачення можливих несприятливих подій та оцінки їх наслідків. Складовими такої методології ризику є три наступні взаємопов'язані елементи (рис. 1): джерело; шлях (сценарій розвитку несприятливих подій); наслідки (результат).

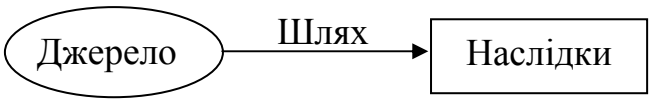


Рис. 1. Складові елементи при дослідженні ризику

Джерело – це об'єкт, який створює небезпеку, що усвідомлюється спеціалістами та характеризується ризиком розповсюдження певними шляхами та з можливими різними наслідками.

З джерелом небезпеки пов’язана ”невизначеність”, яка відображає об’єктивну неможливість отримання абсолютного знання про внутрішню структуру та зовнішні умови функціонування системи, джерела та надійності інформації [5]. Це зумовлює необхідність прийняття рішень в умовах невизначеності при відсутності однозначності та неповноті інформації [1, 3, 5].

Країни і регіони функціонують і розвиваються у взаємозв’язку з прилеглими територіями, прикордонними зонами, кожна з яких має свої внутрішні об’єктивні особливості, стандарти природокористування, етнічні та інші особливості [3].

Це сусідство зумовлює необхідність взаємодії і координації при управлінні територіями з точки зору мінімізації ризиків.

Провідні країни світу, міжнародні організації (UNESCO, The World Bank, МАГАТЕ, МНС, міністерства та відомства різних країн і їх регіональні структури) та науково-дослідні центри (IIASA) проводять дослідження глобальних та катастрофічних процесів, і при ризик-менеджменті розуміють необхідність залучення значних коштів, людських і технічних ресурсів і масштаби втрат (рис. 2).


Рис. 2. Масштаби втрат на різних рівнях адміністративного управління

Чим вище рівень прийняття рішень і відповідальність тим більші можливі збитки.

## Література

1. В.Афанасьев, В.И.Верхотуров, Е.А.Исляев, В.А.Заславский, В.А.Зеленцов и др. Проектирование надежных спутников связи // Под. ред. академика М.Ф.Решетнева, Томск: МГП “РАСКО”, 1993.-221 с.

2. Анісімов. А.В., Заславський В.А., Фаль О.М. Основи інформаційної безпеки та захисту інформації у контексті євроатлантичної інтеграції України. Науково –методологічний посібник//Під загальною редакцією академіка НАН України В.П.Горбуліна, ДП ”НВЦ” Євроатлантикінформ”, 2006.- 104 с.

3. Zaslavskyi V.A. Systems approach for risk management in regional systems Proceedings “The International Conference “Research &Development as the Basis for Innovation in creating the competitive region”12-13 November 2010, Podgorica, Montenegro, Montenegrin Academy of Sciences and Arts, Vol.107, 2011. P. 93-105.

4. Zaslavskiy V., Pasichna M. Optimization Techniques for Modelling Energy Generation Portfolios in Ukraine and the EU: Comparative Analysis//In: Zamojski W., Mazurkiewicz J., Sugier J., Walkowiak T., Kacprzyk J. (eds) Contemporary Complex Systems and Their Dependability. DepCoS-RELCOMEX 2018. Advances in Intelligent Systems and Computing, vol. 761. Springer, Cham, P. 545-555

5. Норкин В.И., Гайворонский А.А., Заславский В.А., Кнопов П.С Модели оптимального распределения ресурсов для защиты критической инфраструктуры, Кибернетика и системный анализ, 2018, том 54, №5, С.13-26.

*УДК 351.746.1*

**Іванов О. Ю.**
кандидат юридичних наук,
Національна академія СБ України

## ВІДРОДЖЕННЯ ІМПЕРСЬКОЇ ВЕЛИЧІ В ІНФОРМАЦІЙНОМУ ДИСКУРСІ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ

У контексті сучасних проблем забезпечення міжнародної безпеки важливе значення має врахування особливостей геополітичного курсу окремих держав. До особливо гострих проблем у цьому контексті належать, зокрема, ті, які пов’язані з тими викликами, що постають у ході зовнішньополітичної діяльності Російської Федерації (далі – РФ). Ця держава схильна до ведення гібридної війни проти міжнародного співтовариства, у ході якої втілює свої прагнення до задоволення стратегічних інтересів у різних регіонах світу. Одним із головних об’єктів ураження засобами російської гібридної війни є і Україна як одна із пострадянських країн. У сучасних умовах основною метою політичного керівництва РФ є відродження її колишньої імперської величі та відновлення в колишніх кордонах Російської імперії.

Актуалізація зазначених питань у російському інформаційному дискурсі пов’язана, зокрема, з тим, що у 2017 р. виповнилося сторіччя від часу ліквідації Російської імперії в ході Лютневої революції. Попри те, що це було закономірним явищем, сучасна російська історіографія характеризує ці події не інакше як «найбільшу трагедію» в історії російського народу. Загалом головною передумовою ліквідації російської монархії став політичний і економічний занепад держави через невдачі у Першій Світовій війні протягом 1916 р. Готуючись вести лише оборонну війну, яка протягом попереднього року була доволі успішною, російське самодержавство перейшло до наступальної манери ведення бою, прагнучи задовольнити свої територіальні інтереси. Проте наявний військовий ресурс не був розрахований на це, що і зумовило глибоку кризу самодержавства. Утім, ро-

сійські історики, а також представники засобів масової інформації, повністю звинувачують у захопленні влади в імперії революційні маси, які створили Тимчасовий уряд на чолі з князем Г. Львовим. Через це на сьогодні в риториці російського політикуму доволі часто звучать заклики до «відновлення історичної справедливості». З огляду на відкритість та доступність різноманітних джерел інформації подібні тези розповсюджуються також і на українське населення, не всі представники якого мають достатній рівень історичної підготовки для критичного осмислення таких фейків російської пропаганди. Саме тому ці та інші подібні фальсифікації широко застосовуються росіянами для ураження свідомості українського населення.

Стратегічна важливість відновлення імперської величі РФ для її вищого політичного керівництва зумовлює вибір широкого арсеналу засобів та способів поширення пропагандистської інформації у середовищі потенційних цілей гібридної війни. Одним із потужних засобів, що застосовуються для таких цілей, виступає телебачення, котре, зокрема, демонструє відповідні тематичні фільми. Зокрема, восени 2017 р. – саме у столітню річницю ліквідації Російської імперії та подальшої Жовтневої революції – на російському телеканалі «Історія» вийшов у прокат 10-серійний фільм «СРСР. Імперія навпаки». Режисером фільму виступив кандидат історичних наук Ю. Стариков. У свою чергу, назва фільму пояснюється тим, що імперська (а потім радянська) Росія, приєднуючи ті чи інші території, нібито мала на меті не колонізувати їх, а сприяти їхньому розвитку, «рятувати» від загибелі.

Істотно, що в 10 серіях охоплені всі 15 колишніх радянських республік, включаючи Росію та Україну. Усі серії побудовані за єдиною системою, котра передбачає спочатку детальний описетнічних та географічних особливостей конкретного регіону, потім короткий виклад його історичного розвитку з особливим акцентом на специфіці процесу входження до складу Російської імперії (а в подальшому – і СРСР) та «прогресивному» значеннійого перебування у складі Росії. Тривалість кожної із серій складає 45 хвилин, із яких історії кожної із колишніх радянських республік до потрапляння під російський вплив присвячено не більше 1–2 хвилин. Причому ця інформація подається після 10–12 хвилин опису сучасного становища тієї або іншої країни з акцентом на «минулі заслуги» Росії в його створенні. Коротка історична довідка формується у такий спосіб, аби підвести до моменту входження до складу Російської імперії крізь призму сприйняття її як «визволителя» і «захисника». Подальший зміст серії побудований не просто на демонстрації «прогресивного» значення періодів імперського і радянського минулого для тієї чи іншої країни, а на яскраво виражених акцентах на нібито неминучості прогресу завдяки такому минулому. Досягнення поставлених цілей авторами циклу фільмів посилю-

ється завдяки залученню відомих діячів культури і науки, котрі є вихідцями із колишніх радянських республік і у своїх інтерв'ю озвучують основні ідеї, провідні для кожної із серій. Більшість опитаних знаменитостей говорять про те, що своє нинішнє становище вони змогли здобути нібито лише завдяки прихильному ставленню радянської влади до тієї чи іншої республіки, зокрема наданим нею широким можливостям для здобуття якісної освіти та культурного зростання. Більш того, за їх словами, саме завдяки імперському та радянському минулому, їхні країни змогли зберегти свою національну ідентичність.

Із зазначеного очевидно, що створення такого багатосерійного фільму підпорядковане цілям пропагандистської політики РФ. Зокрема, історичні довідки складені з грубими викривленнями реального перебігу подій. Так, привертає увагу те, що в кожному випадку момент входження тієї чи іншої країни до складу Російської імперії подається виключно як «прохання» про прийняття до підданства з метою захисту від зовнішніх загроз. Відомості ж про зв'язки із московською державою в більш ранні періоди та їх характер випускаються взагалі. Образ Росії як системоутворюючого центру Радянського Союзу вимальовується за допомогою численних епітетів, що гіперболізують її роль у розвитку інших республік. Доповнюється він курйозним викладом факту того, що відповідно до Декларації про утворення СРСР та Союзного договору 1922 р. Російська республіка була єдиною, котра не мала права виходу зі складу новоутворюваної союзної держави. Сам же факт розпаду СРСР абсолютно в кожній із 10 серій репрезентується не інакше як «трагічна подія», зумовлена волюнтаризмом Б. Єльцина, Л. Кравчука та С. Шушкевича, котрі завізували Біловезькі угоди 1991 р. щодо припинення існування СРСР.

Таким чином, із зазначеного очевидно, що відродження імперської величі відіграє важливу роль у політичному курсі РФ загалом та в її інформаційному дискурсі зокрема. Столітня річниця ліквідації Російської імперії стала доволі сильним поштовхом для розгортання Росією пропагандистської діяльності, спрямованої на відновлення свого колишнього впливу. З огляду на досить значну вагу засобів інформаційного протиборства в арсеналі інструментів, за допомогою яких РФ веде гібридну війну, постає необхідність у веденні контрпропаганди. Задля підвищення рівня дієвості останньої доцільним видається ведення комплексної роботи (можливо, і нарівні загальнодержавної програми) зі зниження рівня вразливості широких мас українського населення щодо дії інструментів російської пропаганди. Зокрема, особливо актуальним видається перегляд на зазначених засадах системи історичної освіти в Україні (як для профільних фахівців, так і в загальноосвітній системі), що і визначає вектор подальших досліджень із заявленої проблематики.

*УДК 351.004*
**Іжутова І. В.**
Національний університет оборони України
імені Івана Черняховського

# ІНФОРМАЦІЙНА БЕЗПЕКА В УМОВАХ СУЧАСНОГО ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА

Теперішній світ, перевантажений інформацією, змінився та примушує змінюватися людину. Інформація впливає на характер ведення сучасних війн. Щоб дістати та забезпечити перевагу в інформаційній складовій, необхідно розуміти глибину концепту сучасного інформаційного середовища (простору) [1, с. 111]. Зокрема, збройна агресія проти України перетворила інформаційну сферу на ключову арену протиборства [2].

Варто зазначити, що, незважаючи на появу Доктрини інформаційної безпеки (далі – Доктрина) ще у 2016 році, досі існує проблема відсутності інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них, а також системи оцінки результатів, так званої роботи над помилками після проведення певних заходів. Сучасне інформаційне середовище стрімко розвивається, даючи простір для появи нескінченної кількості фейкової інформації та дезінформації саме через відсутність належної роботи з громадянами, низького рівня медіаграмотності та обізнаності того, чим загрожує недотримання інформаційної безпеки.

В зазначеній Доктрині одним з пріоритетів визначена, зокрема, побудова дієвої та ефективної системи стратегічних комунікацій. На нашу думку, медіаграмотність, здатність виокремлювати неправдиву інформацію в усьому інформаційному просторі, що дозволить утримуватися від вчинення певних негативних дій та уникнути негативних наслідків, – це основа ефективних стратегічних комунікацій та, відповідно, інформаційної безпеки держави.

Інформація лежить в основі будь-якої діяльності людини, навколо якої відбувається рух чисельних перехресних потоків такої інформації. Тому складність і внутрішня суперечливість глобального інформаційного простору, в якому живе і діє сучасна людина, змушують серйозно рахуватися з умовами інформаційної безпеки [3]. Неправдива, несвоєчасно отримана, неправильно зрозуміла, неповна інформація може нанести серйозної шкоди здоров'ю людини.

Отже, сучасний свідомий громадянин повинен бути медіаграмотним, володіти культурою роботи в інформаційному просторі, тоді держава зможе ефективніше протистояти внутрішнім і зовнішнім загрозам. Задля цього потрібно розвинути на відповідному рівні інформаційну культуру.

**Література**

1. Joint Concept for Operating in the Information Environment (JCOIE). 25 July 2018. URL: https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf?ver=2018-08-01-142119-830.

2. Указ Президента України Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про Доктрину інформаційної безпеки України" від 25 лютого 2017 року №47/2017. URL: https://www.president.gov.ua/documents/472017-21374.

3. Інформаційна безпека в сучасному світі. Горденко С.І. URL: http://molodyvcheny.in.ua/files/journal/2017/9.1/10.pdf.

*УДК 007:304:342.722:355.01:659.3*

**Ірха Ю. Б.**
кандидат юридичних наук, заслужений юрист України,
Державний науково-дослідний інститут МВС України

## ВИСВІТЛЕННЯ ҐЕНДЕРНО-ЗУМОВЛЕНОГО НАСИЛЬСТВА В УМОВАХ ЗБРОЙНОГО КОНФЛІКТУ НА СХОДІ УКРАЇНИ

У багатьох життєвих обставинах людина здатна оперативно діяти та приймати ефективні управлінські рішення за умови володіння достовірною, неупередженою, повною та своєчасною інформацією. Одним із джерел такої інформації є медіа, які завдяки сучасним технологіям можуть миттєво інформувати громадян про найважливіші події та явища, а також впливати на формування у них мислення та поведінки залежно від способу та якості подачі певних відомостей.

Внаслідок агресії Російської Федерації на Сході України відбувається збройний конфлікт низької інтенсивності, який українська і російська сторони висвітлюють з діаметрально протилежних позицій. В умовах інформаційної війни українські засоби масової інформації відіграють важливу роль в інформуванні національної та міжнародної громадськості про реальний стан справ в зоні проведення Операції об'єднаних сил, на тимчасово окупованих територіях, а також про проблеми місцевого населення, військовослужбовців, цивільний персонал, учасників бойових дій, тимчасово переміщених осіб.

Сьогодні серед журналістів є одностайне розуміння важливості теми цього конфлікту, однак більшість спостерігає зниження інтересу аудиторії до нього у зв'язку з накопиченою втомою та відносно спокійною ситуацією на фронті. Українські військові отримують найбільше висвітлення порівняно з іншими соціальними групами, що потерпають від конфлікту, оскільки, на думку журналістів, історії про військових є найбільш цікавими для ау-

диторії, важливими для суспільства та яскравими. Також спрацьовує чинні симпатії журналістів, які підтримують тісний контакт із військовими та вболівають за них [1, с. 19].

Однією з важливих соціальних тем, яка пов'язана із збройним конфліктом у Донецькій та Луганській областях, є проблема ґендерно-зумовленого насильства. Дана проблема не знайшла свого повного та об'єктивного висвітлення у національних засобах масової інформації. Під ґендерно-зумовленим насильством розуміють будь-які небезпечні дії, які вчиняються проти волі людини і які базуються на соціально визначених ґендерних відмінностях між жінками та чоловіками [2, с. 4]. Як правило таке насильство здійснюється у формі фізичного, сексуального, психологічного, економічного насильства При цьому в умовах збройного конфлікту його основними потерпілими стають жінки і дівчати.

На переконання фахівців, під час збройних конфліктів соціальні ролі чоловіків і жінок проявляються досить чітко, посилюється гендерна поляризація. В результаті жінки особливо гостро відчувають наслідки конфлікту в силу гендерно обумовлених ролей. Збройний конфлікт надає ще більш виражений характер нерівності між жінками та чоловіками, а також дискримінації щодо жінок і дівчат. Конфлікти викликають значні зміни у звичній поведінці людей, підривають та змінюють соціальні норми, призводять до соціальних змін [3].

За твердженнями експертів ООН репортажі щодо збройних конфліктів є надзвичайно ґендерно-однобічними, у них здебільшого переважають чоловіки: учасники військових дій, воєначальники, експерти і політики. Водночас, думками жінок цікавляться доволі нечасто, а якщо таки запитують їх про щось, то, зазвичай, це точка зору «жертв» конфлікту. Застосування ґендерно-чутливого підходу щодо висвітлення конфлікту – це досить складний процес. Він передбачає дотримання журналістами ключових стандартів професіоналізму, коли вони неупереджено представляють перевірену інформацію в справедливому та збалансованому контексті, дають можливість висловитися людям, думку яких не було враховано, та уникають ґендерних стереотипів. У конфліктних та після конфліктних фазах ґендерно-чутлива журналістика може спонукати суспільство застосовувати більш доречні ґендерно-трансформаційні процеси, за яких поважаються права жінок у контексті прав людини та закріплюється ґендерна рівність [4, с. 10-11].

Засоби масової інформації можуть руйнувати міфи та стереотипи щодо ґендерно-зумовленого насильства. Проте ігнорування базових принципів етики при висвітленні таких чутливих проблем, може призвести до суспільного осуду тих, хто пережили насильство, посилити травму та поглибити стереотипи та нерозуміння цієї форми насильства. Медіа можуть відігравати впливову роль у підвищенні обізнаності щодо ґендерно-зумовленого насильства, агітуючи за необхідні зміни в законодавстві, ви-

магаючи звітності від держави щодо захисту жінок і чоловіків від насильства і руйнуючи соціальні табу та осуд [2, с. 6].

Ми вважаємо, що українські медіа мають не тільки висвітлювати резонансні події на Сході України, але й посилено інформувати громадськість про факти ґендерно-зумовленого насильства в регіоні. При цьому дуже важливо, щоб журналісти у своїх матеріалах надмірно не драматизували випадки та наслідки насильства, уникали відтворення існуючих стереотипів, не захищали кривдників, не віктимізовували потерпілих. Звертаємо увагу на те, що замовчування зазначеної проблеми не сприятиме її вирішенню, а в окремих випадках, може бути використано противниками для дискредитації держави на міжнародній арені.

**Література**

1. Орлова Д. Висвітлення конфлікту на сході в українських медіа. Спеціальний звіт. К. : ГО «Детектор медіа», 2016.19 с.

2. Рекомендації для медіа щодо висвітлення ґендерно зумовленого насильства в Україні. URL : http://www.un.org.ua/images/documents/4690/Media%20Guide%20for%20GBV%20reporting_UKR.pdf. (дата звернення: 06.02.2020).

3. Артеменко Д., Потарська Н. Жіночий досвід у конфлікті на Сході. URL : https://genderindetail.org.ua/library/ukraina/zhinochiy-dosvid-u-konflikti-na-shodi-134910.html. (дата звернення: 06.02.2020).

4. Рекомендації для медіа щодо висвітлення ґендерних питань і конфлікту. URL : https://www2.unwomen.org/-/media/field%20office%20eca/attachments/publications/2019/07/guidelines%20for%20media%20and%20gender%20ukraine/guidelines_ukr_prew_40719_compressed.pdf?la=en&vs=2940.(дата звернення: 06.02.2020).

*УДК 342:65.012.8(477)*

**Касперський І. П.**
кандидат юридичних наук,
старший науковий співробітник, доцент,
Національна академія СБ України

## ПРОБЛЕМА ВІДПОВІДНОСТІ ЧИННОМУ ЗАКОНОДАВСТВУ ОКРЕМИХ РІШЕНЬ ДЕРЖАВНИХ ЕКСПЕРТІВ З ПИТАНЬ ТАЄМНИЦЬ ЩОДО ВІДНЕСЕННЯ ІНФОРМАЦІЇ ДО ДЕРЖАВНОЇ ТАЄМНИЦІ

Стан функціонування системи охорони державної таємниці суттєво залежить від належного визначення предмета охорони – тих відомостей, які становлять державну таємницю. Відповідно до Закону України «Про

державну таємницю» віднесення інформації до державної таємниці - процедура прийняття (державним експертом з питань таємниць) рішення про віднесення категорії відомостей або окремих відомостей до державної таємниці з установленням ступеня їх секретності шляхом обґрунтування та визначення можливої шкоди національній безпеці України у разі розголошення цих відомостей, включенням цієї інформації до Зводу відомостей, що становлять державну таємницю, та з опублікуванням цього Зводу, змін до нього [1].

Звід відомостей, що становлять державну таємницю (далі – ЗВДТ) [2] є єдиним актом, в якому зведено переліки відомостей, що згідно з рішеннями державних експертів з питань таємниць (далі – держексперти) становлять державну таємницю із наведенням встановлених держекеспертами ступеней секретності конкретних даних. Зміст ЗВДТ неодноразово критикувався правозахисниками [3], проте їх позицію не завжди можна спростувати складністю застосування ними при оцінці обґрунтованості віднесення запровадженого Законом України «Про доступ до публічної інформації» [4] «трискладового тесту», оскільки оцінка можливості та обсягу нанесення шкоди національній безпеці розголошення конкретної інформації дійсно потребує наявності спеціальних знань [5]. Зміст ЗВДТ зазнає критики і з боку науковців із фахового середовища [6, 7], що можливо пояснити відсутністю єдиної методики оцінки інформації на предмет віднесення до державної таємниці.

На жаль, навіть поверхневий аналіз низки статей ЗВДТ (1.9.3, 1.9.7, 1.10.4 та ще 16 статей) дозволяє зробити висновки, що своїми окремими рішеннями держексперти намагаються фактично делегувати свої функції щодо визначення ступеня секретності іншим суб’єктам режимно-секретної діяльності, зазначаючи у рішеннях наступне формулювання «при засекречуванні ступінь секретності встановлюється і змінюється в залежності від обсягу і важливості відповідних відомостей за рішенням посадової особи, уповноваженої на встановлення грифа секретності» або «ступінь секретності встановлюється і змінюється в залежності від ступеня необхідності її зашифрування за рішенням керівника органу СБ». Така диспозитивність у встановленні ступеня секретності є прямим порушенням вимог ст. 9 Закону України «Про державну таємницю» [1], яким єдиним суб’єктом, який має право встановлювати ступінь секретності окремої категорії відомостей є виключно держексперт.

Наведене сумнівне формулювання містить ще одну невідповідність – обсяг даних не може бути підставою зміни ступеня секретності, бо відповідно до вимог ст. 1 Закону України «Про державну таємницю» [1] ступінь секретності – це категорія, яка характеризує виключно важливість секретної інформації. І подібні невідповідності чинному законодавству є непоодинокими, бо у змісті статей 1.9.3, 1.9.5, 2.1.21 та ще 37 статей ЗВДТ

як умова віднесення інформації до державної таємниці вказана можливість нанесення «шкоди національним інтересам і безпеці», що суперечить вимогам ст. 34 Конституції України [8], ч. 2 ст. 6 Закону України «Про доступ до публічної інформації» [4] та ч. 2 ст. 8 і ст. 1 Закону України «Про державну таємницю» [1] де відсутня така підстава обмеження права на доступ до інформації як можливість нанесення шкоди національним інтересам, а фігурує лише можливість нанесення шкоди національній безпеці.

У статті 4.7.2 ЗВДТ держексперт пішов ще далі, стверджуючи, що рішення про засекречування інформації про сили та засоби охорони, що залучаються до забезпечення безпеки пересування посадової особи, щодо якої здійснюється державна охорона, приймається посадовою особою, уповноваженою на встановлення грифа секретності в залежності від обсягу і важливості відповідних відомостей. Таким чином своїм рішенням держексперт делегував іншим суб'єктам уже саме право віднесення інформації до державної таємниці.

Варто зазначити, що ці невідповідності окремих статей ЗВДТ чинному законодавству є не просто приводом для критики з боку громадянського суспільства, вони прямо впливають на ефективність захисту державної таємниці, особливо при делегуванні функцій держексперта окремим посадовим особам, бо так система охорони державної таємниці позбавляється твердої основи у визначенні предмета та рівня захисту, інваріантність рішень за таких умов неминуче призведе до витоку інформації та неможливості застосування юридичної відповідальності до причетних до цього осіб. Сподіваємось, що ці невідповідності буде якнайшвидше усунуто в ході формування нового ЗВДТ.

**Література**

1. Закон України «Про державну таємницю» // Відомості Верховної Ради, 1999, № 49.

2. Звід відомостей, що становлять державну таємницю, затверджений Наказом Служби безпеки України від 12 серпня 2005 р. № 440, зареєстровано в Міністерстві юстиції України 17 серпня 2005 р. за № 902/11182 // Офіційний вісник України. – 2005. – № 5. – Ст. 107.

3. Захаров Є., Рапп І., Які відомості становлять державну таємницю в Україні? // Свобода висловлювань і приватність, 2005, 04.

4. Закон України «Про доступ до публічної інформації» // Голос України від 09.02.2011. – № 24.

5. Пастернак М. Правова регламентація змісту інформації, яка становить державну таємницю, в Україні: сучасний стан та перспективи розвитку // Правова інформатика, 2010, № 4. – С. 86-93.

6. Семенюк О. Порядок віднесення інформації до державної таємниці: порівняльний аналіз вітчизняного та зарубіжного законодавства, шляхи удосконалення цієї процедури // Юридична Україна, 2016, № 3-4. – С. 58-64.

7. Корченко О. Г., Дрейс Ю. О. Про необхідність категоризації та приведення змісту статей ЗВДТ до вимог чинного законодавства // Актуальні проблеми управління інформаційною безпекою держави : зб. матер. наук.-практ. конф. (Київ, 19 березня 2015 року). – К. Центр навч., наук, та період, видань НА СБ України, 2015. – С. 270-273.

8. Конституція України // Відомості Верховної Ради України, 1996 р., № 30, ст. 141.

*УДК 355.40:358.12*

**Кацалап В. О.**
кандидат військових наук,
Національний університету оборони України
імені Івана Черняховського

## ОЦІНЮВАННЯ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ

Спираючись на характеристику інформаційних викликів та загроз національній безпеці України, визначені пріоритети державної політики з питань національної безпеки і оборони, у ході розробки Державних програм різного типу, в яких проаналізовано широкий спектр імовірних ситуацій застосовуватимуться Збройні Сили України, як на довгострокову так і середньострокову перспективу. Ці ситуації об’єднані сценаріями. Сценарії стали базовими для визначення можливого інформаційно-психологічного впливу противника на Збройні Сил України.

Визначення наслідків від інформаційно-психологічного впливу противника пов’язана з урахування ряду умов та чинників: імовірний розвиток обстановки, вірогідні масштаби та наслідки; завдання своїх військ (сил), що повинні бути досягнуті; можливі етапи розвитку ситуації; загальний порядок застосування військ (сил); розрахунки потреб у силах і засобах для протидії. Запорукою адекватної протидії для ефективного застосування військ (сил) є прогнозування впливу зазначених чинників в можливих ситуація та сценаріях.

Розгляд джерел [1, с. 7] свідчить, що сценарії можуть містити можливі причини (умови) виникнення кризи, цілі, які можуть ставитися протилежною стороною. Для прогнозу цілей протилежної сторони (противника) у кожному сценарії визначають напрямок зосередження основних зусиль, кількість сил і засобів, які залучаються до ведення бойових дій, а також можливі способи інформаційно-психологічного впливу противника [2, с. 11]. Враховуючи, що зазначені складові мають свою послідовність моделювання яка не скоординована за місцем і часом в силу того, що застосовуються різні підходи до моделювання. Це дає можливість стверджува-

ти те, що за таких умов визначити можливі наслідки від інформаційно-психологічного впливу противника сьогодні досить складно.

Метою тез є визначення набору параметрів можливих показників які необхідні для оцінювання інформаційно-психологічного впливу в інтересах забезпечення інформаційної безпеки.

Для оцінювання інформаційно-психологічного впливу можемо застосувати метод визначення віддаленої ваги оцінок. Сутність методу полягає в поєднанні експертного методу шкальних оцінок та методу визначення медіани та квартілей [3, с. 47].

На першому етапі в методі визначення медіани та квартілей проводиться експертне опитування результати якого є розрахунок коефіцієнтів відносної важливості способів інформаційно-психологічного впливу.

Другим етапом є формування варіантів інформаційних дій, необхідних при виробленні рекомендацій щодо способів інформаційно-психологічного впливу якими буде досягається поставлена мета.

Наступним кроком буде розрахунок коефіцієнтів відносної важливості необхідних для обґрунтування важливості того або іншого способу інформаційно-психологічного впливу залежно від поставлених цілей і завдань.

Під час проведення експертного опиту складається матриця, в яку вписуються основні способи інформаційно-психологічного впливу, цілі і завдання. Клітки матриці заповнюються значеннями коефіцієнтів відносної важливості вказаних способів, виражених в долях одиниць, але так, щоб сума коефіцієнтів в стовпцях дорівнювала одиниці.

Привласнення коефіцієнтів відносній важливості проводиться в декілька турів. Після здобуття перших результатів група розробників підраховує середнє значення коефіцієнтів і вибирає дані тих фахівців, в яких коефіцієнти значно відрізняються в ту або іншу сторону від середніх. Потім проводиться другий тур привласнення коефіцієнту його значення.

Після визначення коефіцієнтів знов підраховується середнє значення отриманих результатів. Кількість таких турів у великій мірі залежить від кваліфікації фахівців і їх досвіду. Вважається, що в середньому достатнє трьох турів голосування для груп, що складаються з 10-12 експертів.

Такий підхід мав ряд позитивних сторін, але йому були властиві і істотні недоліки. Як і при уявному моделюванні, тут різко виявлявся суб’єктивізм, бо адекватність цих значень повністю залежала від досвіду експерта. Крім того, експерт не завжди може врахувати всі фактори та чинники, які впливатимуть на ситуацію.

Таким чином, запропонований підхід дозволяє оцінити інформаційно-психологічний вплив противника в інтересах бойових дій військ (сил). Зазначене оцінювання характеризує зміст способів інформаційно-психологічного впливу противника та являється основою для прогнозу

поведінки особового складу під час виконання ним бойових завдань. Визначено послідовність моделювання складових способів інформаційно-психологічного впливу противника.

**Література**

1. Указ Президента України «Про затвердження Державної програми реформування Збройних Сил України на 2011 – 2015 роки».

2. «Про оборону України» від 6.12.91 р. № 1932-XII.

3. Тараканов К.В. Математика и вооруженная борьба. – М.: Воениздат, 1974. – 240 с.

*УДК 355.02: 621.396*

**Клочко О. М.**
Національний університет оборони України
імені Івана Черняховського

## ОСОБЛИВОСТІ ВЗАЄМОДІЇ МІЖ СУБ'ЄКТАМИ ОЦІНЮВАННЯ СУСПІЛЬНО-ПОЛІТИЧНОЇ ОБСТАНОВКИ

Суспільно-політична обстановка є складною сукупністю чинників та умов, які стосуються тільки конкретного регіону для певного періоду часу. Її оцінювання та прогнозування здійснюються для вироблення, прийняття та реалізації управлінських рішень застосування Збройних Сил України, а також для організації та здійснення забезпечення інформаційної безпеки держави у воєнній сфері. Рівень складності суспільно-політичної обстановки або критерії, за якими її можливо віднести до певного рівня складності, мають чітку градацію в існуючих нормативно-правових документах [1, с. 3]. У той же час рівень взаємодії суб'єктів оцінювання суспільно-політичної обстановки значною мірою залежить від наявності чітких алгоритмів надання інформації, тому чи іншому, органу державного або військового управління. Враховуючи те, що в Інструкції з оцінювання суспільно-політичної обстановки в районах дислокації військ (сил) під час виконання ними завдань за призначенням чітко визначені суб'єкти оцінювання суспільно-політичної обстановки, то для удосконалення питань взаємодії необхідно кожному з них визначити чіткий порядок надання інформації відповідно до зміни умов та сценаріїв розвитку ситуації.

Прогнозування розвитку суспільно-політичної обстановки повинно передбачати розробку варіантів сценаріїв можливих дій. Кількість варіантів розвитку ситуації в кожному сценарії, що розробляються, залежить від конкретних умов обстановки, ними можуть бути:

найгірший або несприятливий варіант розвитку суспільно-політичної обстановки;

сприятливий варіант розвитку суспільно-політичної обстановки;

інші можливі варіанти розвитку суспільно-політичної обстановки.

Усі розроблені варіанти розвитку суспільно-політичної обстановки потрібно розглянути за ступенем реалістичності або імовірності, в результаті чого визначаються найбільш та найменш імовірні прогнози. Кожен прогноз має певну кількість викликів та інформаційних загроз. Тому базуючись на аналізі викликів та інформаційних загроз, які наведені в Стратегічному оборонному бюлетні до 2025 року [2, с. 8], розглянемо спектр імовірних сценаріїв, у яких можуть застосовуватися війська (сили) (табл. 1). Ці сценарії об'єднані ситуацією і можуть бути базовими для організації взаємодії суб'єктів оцінювання суспільно-політичної обстановки.

*Таблиця 1*

Перелік імовірних сценаріїв під час організації взаємодії між суб'єктами оцінювання суспільно-політичної обстановки

| Найменування сценаріїв | |
|---|---|
| 1. | Здійснення стримування та відбиття збройної агресії проти України |
| 2. | Терористичні акти проти України |
| 3. | Втручання у внутрішні справи України з боку інших держав |
| 4. | Внутрішня нестабільність |
| 5. | Порушення цілісності кордонів України |
| 6. | Надзвичайні ситуації природного, техногенного, соціального та воєнного характеру |
| 7. | Протидія (участь у припиненні дій) організованої злочинності за участю Збройних Сил України |
| 8. | Ведення миротворчих операцій ЗС України |
| 9. | Захист життя громадян України і державної власності за кордоном |
| 10. | Надання військової допомоги Україною іншим державам в рамках багатосторонніх угод |

За своїм змістом сценарій є загальним описом низки кризових ситуацій в яких питання взаємодії між суб'єктами оцінювання суспільно-політичної обстановки будуть формувати перелік та зміст заходів, що має запровадити держава, цілі, які планується при цьому досягти, та базових даних для проведення подальшого застосування військ (сил). Так, одному сценарію (табл. 1) відповідає 4-8 ситуацій. Загальна кількість ситуацій може бути близько 64. Кожний сценарій містить можливі причини (умови) виникнення кризи; сфери зіткнення інтересів (предмет суперечок); цілі, які можуть ставитися протилежною стороною; імовірний розвиток кризи (обстановки); імовірні масштаби та наслідки; цілі, що мають бути досяг-

нуті; функції та завдання військ (сил); загальний порядок застосування військ (сил); розрахунки потреб у силах і засобах для протидії (нейтралізації) загрози (кризової ситуації).

Враховуючи наведену класифікацію інформації, необхідно встановити залежності між кількісними характеристиками протидіючих сторін і можливими результатами їх зіткнення. Це надасть можливість спрогнозувати переваги тієї або іншої системи озброєння, способу ведення бойових дій та спланувати необхідні інформаційні заходи.

Таким чином, наведений алгоритм надання інформації під час оцінювання суспільно-політичної обстановки дозволяє удосконалити ступінь взаємодії та сформувати порядок на зміст потрібної інформації між суб'єктами оцінювання суспільно-політичної обстановки. Порядок здійснення якісного аналізу інформації дозволить удосконалити планування інформаційних заходів, зокрема спрогнозувати порядок блокування противником інформаційного простору та зміст негативної інформації про діяльність органів державного та військового управління.

**Література**

1. Інструкція з оцінювання суспільно-політичної обстановки в районах дислокації військ (сил) під час виконання ними завдань за призначенням. Наказ Генерального штабу Збройних Сил України від 11.09.2017 № 330.

2. Указ Президента України "Про рішення Ради національної безпеки і оборони України "Про Стратегічний оборонний бюлетень України на період до 2025 року" // [Электронный ресурс] – Режим доступу: www.mediemix.com.ua/.../21501.

*УДК 343.21*

**Книженко О. О.**
доктор юридичних наук, професор,
Національна академія прокуратури України

## ЩОДО ЕФЕКТИВНОСТІ КРИМІНАЛЬНО-ПРАВОВИХ САНКЦІЙ ЗА ЗЛОЧИНИ У СФЕРІ ВИКОРИСТАННЯ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН (КОМП'ЮТЕРІВ), СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ І МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ

Прийняття будь-якої кримінально-правової заборони не є самоціллю. Держава шляхом криміналізації діяння та встановлення за нього відповідного кримінально-правового реагування намагається досягнути виконання певних завдань. Про ці завдання, зокрема, йдеться в ч. 1 ст. 1 Кримінального кодексу України (КК України).

Звернення до зазначеної норми, а також до положень ст. 50 КК України дозволяє стверджувати, що санкції кримінально-правових норм мають бути такими, що здатні виконати поставлене завдання та реалізувати заявлені цілі.

В ідеалі будь-яка кримінально-правова норма мала б бути такою. Однак аналіз положень закону, які викладені в Розділі XVI Особливої частини КК України свідчить про протилежне. Варто зауважити, що проблема, яка буде порушена в межах цієї публікації, нажаль, властива не тільки відзначеному розділу КК України, а й в цілому характеризує сучасне вітчизняне законодавство про кримінальну відповідальність.

Передусім вкотре звертаємо увагу на визначення сум завданої шкоди та штрафу, який держава передбачає у разі вчинення злочину.

У примітці ст. 361 КК України «Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку» визначається, що значною шкодою у ст.ст. 361–363-1, якщо вона полягає у заподіянні матеріальних збитків, вважається така шкода, яка в сто і більше разів перевищує неоподатковуваний мінімум доходів громадян [1].

З урахуванням положень п. 5 Розділу XX «Перехідні положення» Податкового кодексу України, а також Розділу XIX «Прикінцеві положення» цього ж кодексу та ст. 7 ЗУ «Про Державний бюджет України на 2020 рік» на сьогодні один неоподатковуваний мінімум доходів громадян про який йдеться у разі обрахування шкоди складає 1051 (одну тисяча п'ятдесят одну) грн.

Таким чином, сума значної шкоди у 2020 року складатиме більше ніж 105 100 (сто п'ять тисяч сто) грн.

У разі коли йдеться при визначення суми штрафу, то ураховуючи вище зазначені положення Податкового кодексу України, відправною цифрою є вже не 1051 грн, а саме 17 грн.

Яскравим прикладом невідповідності розміру покарання завданій злочином шкоди є ст. 363 КК України «Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється». Аби особу можна було притягнути до кримінальної відповідальності, заподіяна шкода має бути значною, тобто такою що більше ніж 105 100 (сто п'ять тисяч сто) грн.

Покарання за такий злочин законодавець встановив у виді штрафу від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян та обмеження волі на строк до трьох років з позбавленням права обіймати певні посади чи займатися певною діяльністю на той самий строк.

Якщо підрахувати суму штрафу, то вона складатиме від 8 500 (восьми тисяч п'ятсот) грн до 17 000 (сімнадцяти тисяч) грн. Тобто особі з такою

сумою штрафу фактично вигідно було вчиняти злочин. Чи здатна така норма виконати заявлені в КК України завдання та досягнути поставлених перед покаранням цілі… Очевидно, що ні. Щоб виправити такий законодавчий недолік, який наскрізно пронизує чинне законодавство про кримінальну відповідальність у ст. 53 КК України вносять зміни, в яких зазначається, що за вчинення злочину, за який передбачене основне покарання у виді штрафу понад три тисячі неоподатковуваних мінімумів доходів громадян, розмір штрафу, що призначається судом, не може бути меншим за розмір майнової шкоди, завданої злочином, або отриманого внаслідок вчинення злочину доходу, незалежно від граничного розміру штрафу, передбаченого санкцією статті (санкцією частини статті) Особливої частини цього Кодексу [1].

Як бачимо зазначена норма здатна врятувати ті випадки, де законодавець встановлює розмір штрафу понад три тисячі неоподатковуваних мінімумів доходів громадян. У разі ж передбачення санкцією норми штрафу меншого ніж у три тисячі неоподатковуваних мінімумів доходів громадян вчинення злочину й сплата за нього штрафу, навіть максимально передбаченого законом, дійсно для особи буде економічно вигідним.

Про те, що такого не повинно бути говорилося ще Чезаре Бекарія у 1764 році в його трактаті «Про злочини і покарання» [2].

Підсумовуючи, констатуємо, що не може бути визнана ефективною в запобіганні злочинам та норма, яка є економічно вигідною для особи, яка вчиняє злочин, з точки зору негативних наслідків та завданої шкоди.

**Література**

1. Кримінальний кодекс України: Закон України від 5 квітня 2001 року № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення 04.03.2020).

2. Бекариа Ч. О преступлениях и наказаниях. – М.: Стелс, 1995. – 303 с.

*УДК 65.012.8:004.056*

**Кожедуб Ю. В.**
кандидат технічних наук,
ІСЗЗІ Національного технічного
університету України «КПІ імені Ігоря Сікорського»і

## СИСТЕМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ НА ОСНОВІ СИСТЕМИ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Прийняття системи менеджменту інформаційної безпеки (далі – СМІБ) є стратегічним рішенням для організації. Розроблення та запрова-

дження СМІБ організацією залежить від потреб і цілей, розміру і структури організації. Проте слід пам'ятати, що усі ці чинники можуть з плином часу змінюватись, а тому потрібно оновлювати й переглядати СМІБ. СМІБ забезпечує конфіденційність, цілісність і доступність інформації (та інші властивості інформації) за рахунок застосування процесу менеджменту ризиків і надає впевненість зацікавленим сторонам в тому, що ризиками адекватно управляють [1]. Важливо, щоб СМІБ була частиною загальної системи менеджменту і була інтегрована з процесами організації у загальній структурі менеджменту, а також інформаційна безпека була застосована під час розроблення виробничих процесів, інформаційних систем і елементів управління. Органічне застосування СМІБ може бути для внутрішніх і зовнішніх сторін способом оцінювання організації щодо здатності виконувати вимоги із забезпечення інформаційної безпеки.

Є три основні групи вимог до системи інформаційної безпеки для будь-якої організації [2].

Перша група вимог – це унікальний набір ризиків порушення інформаційної безпеки, що складається із загроз інформації, інформаційним активам і інформаційним ресурсам та їх вразливостей та можливого впливу цих ризиків на функціонування організації.

Друга група вимог – це набір правових та договірних вимог, яких має дотримуватись організація, її партнери, підрядники та постачальники послуг.

Третя група вимог – це унікальний (специфічний) набір принципів, цілей та вимог до оброблення інформації, що його розробила організація для власних виробничих потреб. Важливо, щоб у документах СМІБ було відображено ці вимоги, а також інші вимоги без надмірності, щоб наявність чи відсутність інструментів захисту та засобів щодо безпеки в інформаційній інфраструктурі не суперечили б меті виробничої діяльності організації й сприяли ефективному управлінню та були спрямовані на постійне поліпшення.

Вартість заходів щодо забезпечення інформаційної безпеки має бути адекватним розміру можливих збитків у разі реалізації ризиків інформаційної безпеки.

На рівні організаційного забезпечення під час проектування, розроблення і модернізації системи захисту інформації, а також під час експлуатації, обслуговування, підтримання працездатності системи захисту інформації має бути дотримано всіх вимог щодо захищеності інформації.

Функціонування системи інформаційної безпеки і її контролювання мають відповідати необхідному рівню захищеності інформації, ресурсів і технологій.

Інформаційні ресурси держави чи суспільства в цілому, а також окремих організацій і фізичних осіб є певною цінністю, тобто мають відповідне матеріальне вираження і потребують захисту від різноманітних за сво-

єю сутністю впливів, що можуть призвести до зниження цінності інформації, інформаційних активів і інформаційних ресурсів.

Захист інформації полягає в створенні й підтриманні в дієздатному стані системи заходів, як технічних (інженерних, програмно-апаратних), так і нетехнічних (правових, організаційних), що дають змогу запобігти чи ускладнити можливість реалізації загроз, а також знизити потенційні збитки для організації. Іншими словами, захист інформації спрямовано на забезпечення безпеки інформації та/чи інформаційної системи в цілому, тобто такого стану, який забезпечує збереження заданих властивостей інформації, що циркулює в організації та/чи інформаційної системи, що її обробляє інформацію.

Значну частину проблем щодо забезпечення інформаційної безпеки в інформаційній системі організації може бути вирішено певними організаційними заходами, до яких відноситься розроблена, запроваджена і функціонуюча СМІБ.

**Література**

1 Захист інформації. Технічний захист інформації. Основні положення. ДСТУ 3396.0-96. Національний стандарт України. Чинний від 01.01.1997 р. Затверджено та введено в дію наказом Держстандарту України від 11.10.1996 р. № 423. – Держспоживстандарт України, 1996. – 10 с.

2 Інформаційні технології. Настанови з керування безпекою інформаційних технологій (IT) Частина 2. Керування та планування безпеки IT. ДСТУ ISO/IEC TR 13335-2:2003 (ISO/IEC TR 13335-2:1997, IDT). Національний стандарт України. Чинний з 01.01.2005 р. Затверджено наказом Держспоживстандарту України від 31.10.2003 р. № 189. – Держспоживстандарт України, 2004. – 20 с.

*УДК 323: 3*

**Криворучко О. В.**
**Десятко А. М.**
Київський національний торговельно-економічний університет

## БІЗНЕС ТА КІБЕРБЕЗПЕКА

Сьогодні бізнес залежить від Інтернету. І той спосіб, яким люди діляться інформацією, обробляють і керують бізнесом, створює реалії сьогодення, особливо в розрізі кібербезпеки. У 21 столітті власники бізнесу використовують комп'ютерні системи та Інтернет, щоб конкурувати на ринках, що заповнюються технологіями. Вдосконалення глобальних WI-технологій забезпечують підприємствам переваги, в той же час піддають компанії потенційні вразливості [1]. Власникам малих та середніх підприємств часто не вистачає важливих засобів інформаційних технологій та можливостей, необхідних для здійснення нових заходів з кібербез-

пеки [2]. Зокрема, не вистачає належних засобів для контролю швидко зростаючих ризиків кібербезпеки та загрози безпеці інформаційних систем [3]. Крадіжка або втрата приватної інформації несе фінансові втрати у будь-якому бізнесі. Втрати клієнтів, дохід, а в деяких випадках і конфіскація бізнесу через дорогі судові витрати є одними з потенційних негативних наслідків. Управління кібер-ризиками вимагає від організацій впровадження сучасних стратегій безпеки, орієнтованих на прогнозування, запобігання, пом'якшення та реакцію, зосереджуючись на людях, процесах та системах.

Щодня більше 2,3 мільярда людей використовують Інтернет-технології для роботи, навчання, банківської діяльності та магазинів. Кіберзлочинці прагнуть отримати доступ до комп'ютерів, планшетів та телефонів, оскільки гаджети містять цінну інформацію, і вони завжди розробляють нові способи нападу на мережеві технології. У 2018 році кібератаки відповідали за 49% нападів на порушення даних у всьому світі, а бізнес був головною мішенню кібератак. У 2019 році кібератаки проти малих та середніх підприємств продовжували зростати. Нові та інноваційні апаратні та програмні технології є важливими для бізнес-систем, а критична інфраструктура є стійкою [4]. Хакери з безпеки створюють постійну і невблаганну загрозу організаціям, використовуючи їх комп'ютерні системи. Більше того, важливість ефективних практик кібербезпеки є фактором для забезпечення захисту Інтернет-комунікацій та того, що працівники організацій повинні мати обізнаність із безпекою [5, 6]. Кіберзлочини різноманітні та широко розповсюджені. Поінформованість власників про кібербезпеку та активні дії можуть потенційно обмежити майбутні кіберзлочини та підвищити кіберживучість малого бізнесу [7, 8]. У 2019 році підрахунок втрат від кіберзлочинів у європейських компаній перевищив 67,2 млрд доларів. Це тому, що 60% усіх цілеспрямованих кібератак вразили малі та середні підприємства, власники яких опинилися в неблагополучному стані у захисті їх інфраструктури. Власники малих та середніх підприємств часто не розглядають себе як цілі кібератак через їх малі розміри чи сприйняття того, що вони нічого не варті красти. Загальна проблема бізнесу полягає в тому, що 80% власників малих та середніх підприємств не використовують адекватних процесів для захисту від кібератак [9]. Конкретна проблема бізнесу полягає в тому, що у деяких власників малих та середніх підприємств може не вистачати ефективних стратегій кібербезпеки для захисту свого бізнесу від кібератак.

Отже, сучасні технології, розроблені в епоху цифрових технологій, піддають людей, підприємств та державні установи можливим уразливістю в кібербезпеці. Тому спеціальні стратегії розробки та впровадження є ключовим моментом для запобігання щорічних комерційних втрат, що збільшуються з року в рік. Сучасні стратегії безпеки здебільшого мають підхід до кібербезпеки, який включає інтеграцію спеціального програмного забезпечення та загальної політики щодо управління даними для під-

приємств будь-якого розміру і спрямовані на запобігання кібератаки проти себе.

**Література**

1. Weber, R. M., & Horn, B. D. Breaking bad security vulnerabilities. Journal of Financial Service Professionals, 2017.

2. Harris, M. A., & Patten, K. P. Mobile device security considerations for smalland medium-sized enterprise business mobility. Information Management & Computer Security, 2019.

3. Njenga, K., & Jordaan, P. We want to do it our way: The neutralization approach to managing information systems security by small businesses. The African Journal of Information Systems, 2016.

4. Maughan, D., Balenson, D., Lindqvist, U., & Tudor, Z. Government-funded R&D to drive cybersecurity technologies, 2015.

5. Malecki, E. J., (2016): Real people, virtual places, and the spaces in between Socio-Economic Planning Sciences. Volume 58, s. 3-12.

6. Bandar, B. M., & Christian, B. (2013). Perceived risk of information security and privacy in electronic commerce. International Journal of Advanced Research in Computer Science, 8. Retrieved from http://www.ijarcce.com/.

7. Borrajo, M. L., Baruque, B., Corchado, E., Bajo, J., & Corchado, J. M. (2011). Hybrid neural intelligent system to predict business failure in small-to-medium size enterprises. International Journal of Neural Systems, 21, 277-296. 81 http://dx.doi.org/10.1142/S0129065711002833.

8. Borrett, M., Carter, R., & Wespi, A. (2013). How is cyber threat evolving and what do organisations need to consider. Journal of Business Continuity & Emergency Planning, 7(2), 163-171. Retrieved from http://www.henrystewartpublications.com/jbcep.

9. Shackelford, S., Fort, T. L., & Prenkert, J. D. How businesses can promote cyber peace. University of Pennsylvania Journal of International Law, 2015.

*УДК 004.056.5:343.326 (045)*

**Крисяк П. В.**
**Зайцев О. В.**
кандидат технічних наук, доцент
**Семібаламут К. М.**
кандидат технічних наук, доцент,
Воєнно-дипломатична академія
імені Євгенія Березняка

## АНАЛІЗ СУЧАСНИХ СИСТЕМ СЕРТИФІКАЦІЇ ФАХІВЦІВ З КІБЕРБЕЗПЕКИ

Відповідно до законів України «Про національну безпеку України», «Про основні засади забезпечення кібербезпеки України» продовжують

вживатися заходи із забезпечення кібербезпеки та кіберзахисту, розвитку спроможностей забезпечення безпеки кіберпростору. Важливою складовою таких заходів є створення системи безперервної підготовки (навчання) та професійного вдосконалення протягом всієї кар'єри для фахівців з питань кібероборони, відповідно кадрового менеджменту в цій галузі та необхідного виробничого потенціалу. Згідно зі звітом *Cyber Risk Analytics «2019 Midyear Quick View Data Breach Report»* [1], в першій половині 2019 року було виявлено понад 3800 інцидентів кібербезпеки, в результаті чого було скомпрометовано понад 4,1 мільярда інформаційних повідомлень. Ця цифра на 54% більше в порівнянні з тим же періодом 2018 року. Більше 60% виявлених порушень були результатом людських помилок, що свідчить про зростання потреби в освіті в області кібербезпеки.

Вітчизняні та зарубіжні вчені у своїх роботах розглядають сучасні підходи до підготовки фахівців в сфері кібербезпеки, аналізують досвід використання систем кібербезпеки західних партнерів та пропонують загальні підходи щодо організації системи освіти в галузі кіберзахисту [2–5]. Проте недостатньо досліджено питання щодо аналізу світового досвіду підготовки фахівців в рамкам курсів підвищення кваліфікації та сертифікації.

З метою формування якісної програми підготовки фахівців в рамках курсової підготовки, був проведений аналіз відомих світових систем підготовки та сертифікації фахівців в області інформаційної безпеки, які сьогодні вважаються лідерами, серед них: *CEH: Certified Ethical Hacker; CISM: Certified Information Security Manager; CompTIA Security+; CISSP: Certified Information Systems Security Professional; CISA: Certified Information Security Auditor; GSEC: SANS GIAC Security Essentials; та інші.*

В результаті аналізу слід визначити наступне: система підготовки, як правило, передбачає невеликий термін навчання – 1 тиждень; підготовка, містить як базову так спеціалізовану компоненту; базова підготовка націлена на розгляд загальних понять і принципів роботи, а також на використання класичних, загальновизнаних і як правило відкритих апаратних та програмних платформ; спеціалізована підготовка в більшості заснована на використанні окремих, складних комерційних продуктів або власних розробок компанії, які пропонується придбати після проходження підготовки; підготовка є постійним і обов'язковим процесом роботи спеціаліста в сфері інформаційної безпеки, оскільки прийоми та методи проведення кібератак постійно змінюються; підготовка передбачає різні форми проведення: з викладачем, за електронними та паперовими підручниками, відеофільмами, онлайн- тестами та спеціальними платформами для навчання; обов'язковим елементом є проведення складного комплексного екзамену з видачею відповідного сертифікату; термін дії такого сертифікату в більшості випадків не перевищує трьох років, що відповідає загальній тенденції розвитку технологій в сфері кібербезпеки та кіберзахисту; спеціалістам

пропонуються системи курсової підготовки, так звані «дорожні карти», які складаються як в рамках підготовки в одній компанії, так і в рамках підготовки в різних навчальних центрах та компаніях.

Під час розробки власних програми базової підготовки фахівців за напрямом кіберзахисту та кібербезпеки пропонується в першу чергу розглядати наступні питання: вивчення вимог керівних документів, що регламентують питання кібернетичної безпеки та кіберзахисту; вивчення досвіду країн партнерів НАТО в даній галузі; стислий огляд відомих світових та вітчизняних систем підготовки, в першу чергу можливостей пройти додаткове навчання самостійно та дистанційно та отримати відповідний сертифікат; огляд виробів відомих світових та вітчизняних виробників апаратного та програмного забезпечення для кіберзахисту та кібербезпеки; вивчення питань практичного застосування загальнодоступних програмних та апаратних рішень.

Перспективами подальших досліджень – є науково обґрунтований аналіз існуючих платформ кіберзахисту та визначення складу програмних та апаратних рішень, які необхідні для вивчення слухачами в системі курсової підготовки.

**Література**

1. Best InfoSec and Cybersecurity Certifications of 2020. 2020. URL: https://www.businessnewsdaily.com/10708-information-security-certifications.html (дата звернення: 04.03.2020).

2. Кибербезопасность: Типовой учебный план – NATO. 2016. URL: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_10/20171004_1610-cybersecurity-curriculum-r.pdf (дата звернення: 04.03.2020).

3. Sabillon R. and other. Cybersecurity Training Model to Support an Organizational Awareness Program: The Cybersecurity Awareness TRAining Model (CATRAM). *A Case Study in Canada Journal of Cases on Information Technology.* 2019. 21(3). URL: https://www.igi-global.com/article/an-effective-cybersecurity-training-model-to-support-an-organizational-awareness-program/227676 (дата звернення: 04.03.2020).

4. Діорбіца І. Стан підготовки фахівців у сфері кібербезпеки. *Visegrad Journal on Human Rights.* 2016. 6/1. URL: http://vjhr.sk/archive/2016_6/part_1/11.pdf (дата звернення: 04.03.2020).

5. Даник Ю., Зінченко А. Кіберосвіта та її особливості. *Військова освіта*. 2018. №2(38) С. 67–84 URL: http://znp-vo.nuou.org.ua/article/download/160748/161579 (дата звернення: 04.03.2020).

*УДК 316.652 : 355 (477)*
**Купрієнко Д. А.**
доктор військових наук, доцент,
Національний університет оборони України
імені Івана Черняховського

# КОМУНІКАТИВНА МОДЕЛЬ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ У ВОЄННІЙ СФЕРІ

Результати аналізу теорії і практики забезпечення воєнної безпеки держави свідчать, що належне виконання функцій і завдань Міністерством оборони (МО) України та Збройними Силами (ЗС) України без досягнення необхідного стану інформаційної безпеки (ІБ) у воєнній сфері є неможливим. Адже лише у стані ІБ, коли доступні та захищені необхідні інформаційні ресурси, процеси управління за кожним із визначених завдань, що здійснюються виключно інформаційними методами, можуть бути реалізовані. Створення таких інформаційних можливостей на виконання завдання Генерального штабу ЗС України щодо забезпечення ІБ у ЗС України потребує залучення різного роду потенціалів багатьох суб'єктів, а тому виходить за межі власних ресурсів МО України та ЗС України. Отже, ця обставина потребує інтегрування спроможностей різних відомств і установ держави для створення та використання єдиного інформаційного простору в інтересах забезпечення інформаційної безпеки у воєнній сфері та відповідного загальнодержавного управління [1, с. 10].

Тому існує потреба у запровадженні загальнодержавного механізму управління процесом забезпечення ІБ держави у воєнній сфері. Цей процес є складним і багатоаспектним, оскільки він може включати цільові програми, проекти та окремі дії (заходи, роботи), які спрямовані на реалізацію певного порядку забезпечення ІБ держави у воєнній сфері. Виконавцями цього процесу повинні бути як профільні органи у складі МО України та ЗС України, так і інших суб'єктів Сектору безпеки і оборони держави, а також задіяні підприємства, заклад і установи України, що не відносяться до названих суб'єктів [2, с. 4].

Одним із популярних підходів для реалізації в Україні зазначеного механізму управління є підвищення ефективності системи стратегічних комунікацій у воєнній сфері, що є можливим за виконання таких умов:

наявність концептуальних засад забезпечення ІБ України у воєнній сфері;

внесення змін у законодавче поле України щодо уможливлення виконання концептуальних положень;

прийняття рішення щодо створення організаційної структури державної системи забезпечення ІБ держави у воєнній сфері.

Затвердження концептуальних засад забезпечення ІБ держави у воєнній сфері, а також виконання третьої умови, закладають правовий фундамент для запровадження єдиної державної політики та утворення адміністративно упорядкованої системи забезпечення ІБ держави у цій сфері [3, с. 32].

Організаційне забезпечення полягає у здійсненні загальнодержавної та відомчої координації заходів щодо забезпечення ІБ держави у воєнній сфері з контролем їх виконання, а також у забезпеченні взаємодії усіх задіяних суб'єктів при проведенні таких заходів, і, на наш погляд, потребує:

створення спеціального державного органу (служби) з функцією забезпечення реалізації державної політики у сфері ІБ, а відтак здійснення міжвідомчої координації, зокрема серед суб'єктів забезпечення ІБ держави у воєнній сфері;

підвищення ролі Ради національної безпеки і оборони України з питань інформаційної політики та ІБ за рахунок створення при ній постійно діючого органу за напрямом ІБ держави у воєнній сфері;

утворення усіма міністерствами (відомствами) України структурних підрозділів з питань галузевої ІБ із включенням до їх складу відділів (груп) координації зусиль щодо забезпечення ІБ дерави у воєнній сфері, а у МО України як головному органі в системі центральних органів виконавчої влади із забезпечення реалізації державної політики у сфері оборони, – структурного підрозділу (департаменту) з питань забезпечення ІБ держави у воєнній сфері, на який покладаються завдання координації діяльності та організації взаємодії усіх суб'єктів безпосередньо в ході проведення заходів забезпечення ІБ держави у воєнній сфері;

утворення в органах Збройних Сил України та інших органах військового управління структурних підрозділів, на які, відповідно до рівня їх компетенції, покладаються завдання координації діяльності сил і засобів з питань створення та використання бойового інформаційного простору, а також його всебічного захисту.

Таким чином, невід'ємною функцією наведеної комунікативної моделі системи забезпечення ІБ держави у воєнній сфері є методичне керівництво, яке полягає у проведенні заходів за конкретними видами діяльності (цільові програми, проекти, плани, дії тощо) щодо забезпечення ІБ держави у воєнній сфері у формі окремих директив, розпоряджень, інструкцій, вказівок, а також нарад, науково-практичних конференцій та семінарів.

**Література**

1. Воєнна доктрина України: затверджено Указом Президента України від 24 вересня 2015 року № 555/2015 «Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року «Про нову редакцію Воєнної доктрини України» // Офіційний вісник України. 2015. № 22. С. 19.

2. Bonk K., Tynes E., Griggs H. And Sparks Ph. Strategic Communications for Nonprofits: A Step-by-Step Guide to Working with the Media (The Jossey–Bass Nonprofit Guidebook Series) Paperback. By Communications Consortium Media Center Publications 2008. – 208 p. ISBN-10: 0470181540; ISBN-13: 978-0470181546.

3. Tatham Steve. U.S. Governmental Information Operations and Strategic Communications: A Discredited Tool or User Failure? Implications for Future Conflict / Monograph. By SSI Publications, 2013. – 98 c. ISBN 10: 158487600X; ISBN 13: 9781584876007.

*УДК 004.067*

**Ланде Д. В.**
доктор технічних наук, професор,
**Дмитренко О. О.**
Інститут проблем реєстрації інформації НАН України

## ПОБУДОВА НАПРАВЛЕНИХ ЗВАЖЕНИХ МЕРЕЖ ТЕРМІНІВ

Розглядається одна з найбільш актуальних проблем комп'ютерного аналізу природньої мови – формалізація та побудова онтологічних моделей предметних областей на основі масиву інформаційних повідомлень заданої тематики. Актуальність проблеми пов'язана, в першу чергу, зі стрімким збільшенням інформаційних масивів та потоків, що розподілені в мережі Інтернет. Прикладом такої онтологічної моделі може бути мережа із ключових термінів (Network of Terms) [1], вузли якої відповідають окремим словам або словосполученням у тексті, а ребра – зв'язкам між ними. Для побудови ненаправленої мережі термінів застосовується алгоритм горизонтальної видимості [2]. Зокрема, однією із задач є визначення напрямків зв'язків та їх вагових значень у ненаправлених мережах термінів.

Для вирішення задачі визначення напрямків зв'язків був запропонований наступний підхід. Нехай $G$ – ненаправлена мережа термінів: $G$:= ($V$,$T$), де $V$ – множина вузлів, $T$ – множина невпорядкованих пар вузлів з $V$, які відповідають зв'язкам між вузлами. Вважається, що $\forall_{i,j}$: ($t_i, t_j$) $\in T$ причинно-наслідковий зв'язок існує у напрямку від вузла $t_i$ до $t_j$ якщо у реченні термін, якому відповідає вузол $t_i$ зустрічається раніше ніж термін, якому відповідає вузол $t_j$. У роботі [3] було досліджено, що описане вище правило, у порівнянні з іншими, які були запропоновані, більш точно відображає напрямок зв'язків, які існують між термінами у тексті. Тобто

напрямки зв’язків, визначених за цим правилом, більш точно відображають зміст тексту на думку експертів.

Загальний принцип визначення вагових значень зв’язків полягає в наступному: вершини графа, що відповідають однаковим термінам побудованої на попередньому етапі направленої мережі об’єднуються. Оскільки будь-який граф визначається матрицею суміжності, то задача визначення вагових значень зв’язків зводиться до конкатенації стовпців та відповідних рядків – зваженої компактифікації графа горизонтальної видимості [2].

Апробація запропонованого підходу була здійснена на основі текстового корпусу з інформаційних повідомлень за темою «COVID-19».

Для розглянутих предметних областей було визначено найбільш впливові та значущі зв’язки між відповідними вузлами у мережі термінів: «diseas → covid-2019», «health → covid-2019», «case → covid-2019», «covid-2019 → health», «covid-2019 → diseas» та «covid-2019 → case».

Аналіз побудованих мереж термінів побудованих за запропонованим підходом дасть змогу визначити найбільш впливові та значущі зв’язки між відповідними вузлами у мережі, що відповідають певним поняттям розглянутої предметної області. Запропонований підхід спростить процес виявлення найбільш важливих частин документів і дозволить виводити необхідний обсяг цільової інформації в реферат.

**Література**

1. Снарский А.А., и Ландэ Д.В.: Моделирование сложных сетей: учебное пособие. С. 212. К.: ООО «Инжиниринг» (2015). ISBN 978-966-2344-44-8.

2. Lande, D. V., Snarskii, A. A., Yagunova, E. V., & Pronoza, E. V.: The use of horizontal visibility graphs to identify the words that define the informational structure of a text. In: 2013 12th Mexican International Conference on Artificial Intelligence, pp. 209-215 (2013).

3. Ланде, Д.В., Дмитренко, О.О, та Радзієвська, О.Г.: Визначення напрямків зв’язків у мережі термінів. Інформаційні технології та безпека. Матеріали XIX Міжнародної науково-практичної конференції, ІТБ-2019, С. 103-112. К.: ООО «Инжиниринг» (2019).

*УДК 351.004*
**Лапутніна Ю. А.**
кандидат психологічних наук,
Служба безпеки України

# СМИСЛОВА ВІЙНА ПРОТИ УКРАЇНИ: ІНСТРУМЕНТИ, ЗАСОБИ, ДОСВІД ПРОТИДІЇ

В умовах стрімкого розвитку інформаційно-комунікаційних технологій, поряд з позитивними змінами у суспільствах, на жаль, відбувається глобалізація загроз інформаційній безпеці. Україна з 2014 року зазнала військової агресії з боку РФ. Сьогодні, маючи відповідний ретроспективний аналіз, ми можемо стверджувати, що за багато років до військової фази агресії, Росія застосувала проти нашої держави технологію смислової війни (semanticWar).

Смислова війна є видом когнітивної зброї, та в сучасних умовах – невід'ємною складовою гібридної війни. На відміну від інших типів війн, спрямована на віртуальний простір та впливає на пізнавальну сферу людини.

Об'єктами впливу є світоглядні переконання населення та цінності, сформовані у суспільствах.

Мета – зміна відношення до процесів, подій. В результаті у населення країни-потенційної жертви,задовго до застосування військової сили, створюються нові сенси та установки на користь державі-агресору.

Оскільки смисли управляються оцінками і цінностями минулого часу, їх беруть готовими з арсеналів смислової зброї, та зосереджують навколо полюсів–добра і зла. «Наше» – добро , а «чуже» – зло.

Основними каналами, які застосувала РФ проти України з використанням технології смислової війни з 2008 року, стали: телебачення (переважно серіали), кінопродукція, література. Реалізації смислової експансії сприяв: спільний інформаційний, телекомунікаційний та культурний простір пострадянського періоду.

Телепростір України майже десятиліття цілеспрямовано насичувався, головним чином, серіалами, книгами, що переформатовували ціннісно-смислові орієнтації українців. Їх приклади Ви можете побачити на слайді.

Наступним етапом розгортання проти України інформаційного фронту з боку РФ стали російські соцмережі «ВКонтакте» и «Одноклассники», які були чітко орієнтовані на дві цільові аудиторії: ВК на молодь, ОК – на старше покоління, яке виросло в СРСР. Мотивами популярності цих соцмереж в Україні стали: для ВК зручний інтерфейс, можливість користуватися безкоштовним аудіо- та відеоконтентом; для ОК – можливість відновити зв'язок з однокласниками, одногрупниками на теренах колишнього СРСР.

Враховуючи вимоги російського законодавства, згідно з якими власники соцмереж мають передавати інформацію про користувачів правоохоронним органам та спецслужбам, РФ отримала величезний масив інформації про українців, який у період перед початком військової агресії був активно застосований у маніпуляції громадською думкою в Україні.

У 2013-2015 роках в Україні діяло більше 600 антиукраїнських груп у соцмережах, 80 % з яких складали групи в російських «ВК» та «Одноклассники». Спецслужби РФ використовували технології штучного нарощування кількості учасників, відвідуваності груп, т зв. тролів, які забезпечували постійну присутність у мережі, коментування, тощо. Адміністрування цих груп, переважно, здійснювалося з території РФ, анексованого Криму, а після початку військової фази російської агресії – з окупованих населених пунктів Донецької та Луганської областей. Власники найбільшої групи «Антимайдан» втекли до анексованого Криму.

Використання маніпулятивних технологій у соцмережах стало продовженням смислової війни. Адже контентний ряд, впроваджений в український сегмент російських соцмереж відповідав доктринальним геополітичним позиціям ідеологів «руського миру».

Основні ідеологеми, які впроваджувалися в український та іноземний сегмент російських соцмереж були:

«Українці та росіяни – один братній народ»;

«В Україні діє хунта, нелегітимна влада»;

«В Україні зазнає утисків російськомовне населення»;

«В Україні почалася громадянська війна»;

«В Києві на Майдані націоналісти, каратели, хунта розпочали озброєне протистояння з владою»;

«Загони українських бандеровців ідуть до Криму вбивати місцеве населення»;

«Тільки Росія може спасти населення Донбасу від української хунти».

В результаті населення Криму, Донеччини, Луганщини почало сприймати російські війська, як визволителів та протидіяти наведенню порядку українською владою.

Після анексії Криму, вторгнення військ РФ на територію України соцмережі активно використовувалися спецслужбами Росії для розповсюдження фейкових новин, а також для безпосереднього вербування громадян України, спонукання їх до діяльності на користь інтересів країни-агресора.

Після відновлення суверенітету України у значній частині Донецької та Луганської областей, фактичного провалу російського бліц-кригу, інформаційну складову війни РФ проти України було вирішено посилити завдяки розвитку інтернет-ресурсів, які фактично виконують роль ЗМІ.

Вказані видання не мають відвертого антиукраїнського спрямування. Разом з цим, завдяки використанню маніпулятивних технологій стали елементом т.зв. м'якої сили. Мета подібних проектів – зміна ціннісних орієнтацій, підміна смислів цільових аудиторій в Україні в інтересах дестабілізації внутрішньо-політичної ситуації, штучного роздмухування міжетнічної, релігійної ворожнечі, провокування невдоволення населення владою, впливу на вибір українців проросійських політиків на різних рівнях, дискредитації реформ тощо.

До цих процесів спецслужби РФ активно залучають лідерів думок, блогерів, які на фоні нібито незаангажованої риторики формують громадську думку українців в інтересах країни-агресора.

Ще одним напрямком маніпуляцій з боку РФ стала цілеспрямовано робота по підриву європейського та євроатлантичного курсу України. З цією метою через різні канали інформації у цільових аудиторій в Україні здійснюється спроба формування хибних уявлень про європейські цінності. Українцям, які вийшли на Майдан відстоювати своє право розвитку країни у напрямку запровадження європейських цінностей – свободи, прав людини, демократії, верховенства права, через різні канали доводиться, що курс на Євроінтеграцію означатиме обов'язковість лібералізації потрапляння до України мігрантів, масового засилля ЛГБТ-спільнот, утиски для традиційних сімейних цінностей тощо.

Україна, як демократична правова держава, першим чином пішла шляхом удосконалення правового регулювання захисту інформаційної безпеки України.

Після початку військової агресії РФ проти України РНБО України звернулася до Нацради з питань телебачення та радіомовлення з вимогою невідкладного розгляду питання щодо інформаційної безпеки України від дій, спрямованих на повалення конституційного ладу, порушення територіальної цілісності України, пропаганди війни, насильства, жорстокості, розпалювання ворожнечі, вчинення терористичних актів, посягання на права і свободи людини.

За результатами офіційного моніторингу телерадіопрограм «Первый канал. Всемирная сеть», «РТР-Планета», «Российский Информационный канал «Россия-24», «НТВ Мир» були встановлені порушення вимог чинного законодавства, а саме – пропаганда, заклики до зміни конституційного ладу в Україні та її територіальної цілісності.

Виробником програм є Російська Федерація, якою Європейська конвенція про транскордонне телебачення не ратифікована. Тому зміст призначених для ретрансляції на території України програм підлягав адаптації до вимог законодавства України.

Отже, відповідно до Ухвали Київського окружного адміністративного суду № 826/3456/14 від 25.03.2014 р. було прийнято рішення про тимчасо-

ве припинення ретрансляції в багатоканальних телемережах на території України іноземних програм» Первый канал. Всемирная сеть», «РТР-Планета», «Российский Информационный канал «Россия-24», «НТВ Мир». Аналогічним шляхом було припинено трансляцію інших російських каналів, телеконтент яких шкодить інтересам забезпечення безпеки України.

У 2014 році з метою захисту національних інтересів, національної безпеки, суверенітету і територіальної цілісності України, протидії терористичній діяльності, порушенню прав, свобод та законних інтересів громадян, ВР України було прийнято Закон України «Про санкції». Він визначає правові засади, порядок та механізм застосування до фізичних та юридичних осіб спеціальних обмежувальних заходів (санкцій).

На підставі матеріалів, поданих до РНБО України визначеними у Законі суб'єктами, санкції було застосовано по відношенню до фізичних та юридичних осіб, які надають послуги сервісів «Вконтакте», «Одноклассники», «Яндекс», «Лаборатория Касперского», «Mail.ruGroup» тощо.

Наступний шлях, який обрала Україна у протидії гібридним загрозам – це вжиття превентивних заходів, які попереджують можливий негативний вплив смислових війн на населення.

Основна мета – інформування громадськості про зміст інформаційної агресії, форми, методологію, які використовуються РФ на шкоду інформаційній безпеці України, канали, через які здійснюються негативні впливи; сприяння розвитку «інформаційної гігієни» та медіаграмотності. Адже усвідомлення громадянами небезпечності «інформаційної зброї» та обізнаність у сутності та формах можливого негативного впливу є однією з запорук формування стійкості нації в умовах гібридного протиборства.

Саме тому, сектор безпеки та оборони України активно працює з експертним середовищем, ІТ-сферою, громадянським суспільством, медіаспільнотою у напрямку розвитку стратегічних комунікацій, створення платформ для обговорення проблем гібридного протистояння, обміну інформацією, укріплення горизонтальних зв'язків, формування довіри та державно-приватного партнерства.

Враховуючи транснаціональний характер загроз в сфері інформаційної безпеки, одним з пріоритетів залишається розвиток міжнародного співробітництва з протидії гібридним загрозам. Одним з позитивних напрямків міжнародної співпраці вважаю створення в Службі безпеки України Ситуаційного центру протидії кіберінцидентам за підтримки Трастового фонду НАТО. Хоча з моменту його відкриття пройшло не так багато часу, можу впевнено сказати, що завдяки діяльності Центру за цей період попереджено декілька серйозних спланованих кібератак проти України.

*УДК 349.1*
**Літвінов М. Ю.**
кандидат юридичних наук
**Логінов І. В.**
кандидат юридичних наук,
старший науковий співробітник,
Служба безпеки України

# УНОРМУВАННЯ СПІВРОБІТНИЦТВА З "БІЛИМИ ХАКЕРАМИ" ЯК ІНСТРУМЕНТ ЗАБЕЗПЕЧЕННЯ КОНТРРОЗВІДУВАЛЬНОГО РЕЖИМУ

Контррозвідувальна діяльність у будь-якій країні світу спирається на попередньо створене правове підґрунтя. Сукупність адміністративно-правових норм, що сприяє вирішенню завдань контррозвідувальної діяльності, іменується "контррозвідувальним режимом". В Україні існує декілька доволі ретельно розроблених адміністративно-правових режимів, які безпосередньо впливають на ефективність контррозвідувальної діяльності, – охорони державної таємниці, перебування іноземців тощо [1, с. 61-98; 2]. Водночас, з появою нових сфер суспільних відносин, що торкаються питань національної безпеки, виникає потреба добудови існуючого контррозвідувального режиму, доповнення його новими адміністративно-правовими нормами, інколи доволі специфічними.

Так, нині українська держава слідом за іншими цивілізованими країнами світу увійшла в епоху тотальної залежності добробуту суспільства і окремої людини від інформаційних та телекомунікаційних технологій, від безпечності національного кіберпростору. У зв'язку з цим інтенсифіковано спроби спецслужб іноземних держав, злочинних і терористичних угруповань та окремих зловмисників втрутитись у функціонування життєво важливих для держави і суспільства інформаційно-телекомунікаційних систем у сферах енергетики, транспорту, оборони тощо для вирішення розвідувально-підривних завдань або у корисливих інтересах. Цим обумовлено нагальну потребу контррозвідувального захисту вітчизняного кіберпростору, яка визнана на законодавчому рівні [3; 4]. Відповідно, для його ефективного здійснення потрібно формувати контррозвідувальний режим у сфері забезпечення кібербезпеки. Оцінка ж поточного стану правового регулювання суспільних відносин у цій сфері не дає підстав для оптимізму, оскільки викриває численні правові прогалини, часто обумовлені новизною і недостатньою дослідженістю нових видів суспільних відносин.

Так, кібератаки на критичну інформаційну інфраструктуру України, які мали серйозні негативні наслідки, – BlackEnergy, Petya/NonPetya тощо, – завдячують своїм успіхом вразливостям кіберзахисту атакованих сис-

тем. Для завчасного виявлення та усунення таких вразливостей у життєво-важливих інформаційно-телекомунікаційних системах СБУ доручено негласно перевіряти готовність об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів. Але можливості Ситуаційного центру забезпечення кібербезпеки СБУ не безмежні, – негласна перевірка одного об'єкта триватиме від кількох тижнів до кількох місяців, а таких об'єктів в Україні налічується тисячі. Це наводить на думку про доцільність мобілізації в інтересах захисту кібербезпеки наявного в державі приватного потенціалу.

Зокрема, серед фахово обізнаних в інформаційних технологіях осіб досить давно сформувався прошарок так званих "білих" або "етичних" хакерів. "Білі хакери" – це аматори, які в ініціативному порядку вишукують вразливості у кіберзахисті інформаційно-телекомунікаційних систем, але не експлуатують їх для проведення кібератак, а повідомляють про них власника системи, розраховуючи на вдячність чи винагороду [5].

Усвідомлюючи корисність їхньої праці для забезпечення кібербезпеки критичної інформаційної інфраструктури, провідні корпорації світу на добровільній основі залучають "білих хакерів" для виявлення вразливостей у корпоративних системах. Співробітництво між ними налагоджується у формі програм типу "bug bounty" або через портали HackenProof, HackerOne тощо [6].

Програма bug bounty оголошується зацікавленою фірмою із завчасним визначенням гарантованої винагороди "білому хакеру" за кожну виявлену вразливість. Але, зважаючи на високі розцінки послуг в IT-сфері, такі програми під силу лише потужним корпораціям.

Менш витратною для компанії вбачається співпраця через портал типу HackerOne. Такий портал, по суті, є дошкою оголошень, де зацікавлені фірми розміщують публічно доступні дозволи на "злам" кіберзахисту власних систем. Зокрема, в поточний час на порталі HackerOne зареєстровано дозволи корпорацій "ВКонтакте", Mail.ru, Sony, Adobe та деяких інших всесвітньо відомих вендорів. Але на таких порталах розцінки за виявлені вразливості не фіксуються, винагороду для хакера зацікавлена фірма призначає на власний розсуд, – від кількох тисяч доларів до простого сувеніра.

З огляду на викладене постає питання про імплементацію напрацьованого приватними підприємцями позитивного досвіду у діяльність основних суб'єктів забезпечення кібербезпеки України через формування адміністративно-правового режиму співпраці з "білими" хакерами. На наш погляд, це стало б вагомим кроком у зміцненні контррозвідувального режиму захисту кібербезпеки України, сприяло б вирішенню визначеного її стратегією завдання щодо запровадження механізму обміну інформацією між державними органами, приватним сектором і громадянами стосовно загроз критичній інформаційній інфраструктурі.

За попередньою оцінкою, вирішити це питання можливо через розробку і прийняття державної програми bug bounty, яка б, зокрема, передбачала:

– створення єдиного для основних суб'єктів забезпечення кібербезпеки державного порталу "етичного" хакінгу за прикладом HackerOne, де адміністрації об'єктів критичної інфраструктури держави зможуть розміщувати дозволи на випробування кіберзахисту своїх систем;

– запровадження відомчих програм bug bounty суб'єктами забезпечення кібербезпеки, зацікавленими у незалежній перевірці стану кіберзахисту підвідомчих об'єктів критичної інформаційної інфраструктури;

– розробки системи матеріальних та інших заохочень для "білих хакерів", які братимуть участь у реалізації цієї програми.

Зазначимо, що перший крок на шляху реалізації ідеї зроблено шляхом розміщення на сайті СБУ публічного Меморандуму про взаємодію зі Службою безпеки України у сфері відповідального пошуку та розкриття інформації про вразливості інформаційно-телекомунікаційних систем та/або телекомунікаційних мереж [7].

Разом з тим необхідно зауважити, що основною перепоною реалізації задуму залишається відсутність у Служби безпеки ресурсів для адекватного стимулювання співпраці з "білими хакерами" та їхнього заохочення за надані послуги, які досить високо оцінюються на IT-ринку.

Проте, нагальна потреба захисту критичної інфраструктури держави від кібератак і кіберінцидентів примушує почати вирішення проблеми вже зараз, не очікуючи відшукання потрібних ресурсів.

**Література**

1. Настюк В. Я., Бєлєвцева В.В. Адміністративно-правові режими в Україні : монографія. Харків : "Право", 2009. 128 с.

2. Мінка Т. П. Поняття та зміст адміністративно-правового режиму перебування в Україні іноземців та осіб без громадянства. Право і суспільство. 2012. № 4. С. 82-85.

3. Про національну безпеку України : Закон України Закон України від 21 червня 2018 р. № 2469-VIII. Законодавство України : веб-сайт. URL : https://zakon.rada.gov.ua/laws/show/2469-19. (дата звернення: 06.03.2020).

4. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовтня 2017 р. № 2163-VIII. Законодавство України : веб-сайт. URL : https://zakon.rada.gov.ua/laws/show/2163-19. (дата звернення: 06.03.2020).

5. Чем занимается "белый хакер", как им стать и сколько можно заработать. VC.RU : веб-сайт. URL : https://vc.ru/story/86714-chem-zanimaetsya-belyy-haker-kak-im-stat-i-skolko-mozhno-zarabotat. (дата звернення: 06.03.2020).

6. Hack for good. Hackerone : веб-сайт. URL : https://vc.ru/story/86714-chem-zanimaetsya-belyy-haker-kak-im-stat-i-skolko-mozhno-zarabotat. (дата звернення: 06.03.2020).

7. Публічний меморандум. Ситуаційний центр забезпечення кібербезпеки Служби безпеки України. Служба безпеки України : веб-сайт. URL : https://ssu.gov.ua/ua/pages/330. (дата звернення: 06.03.2020).

*УДК 351.746*
**Ліченко І. В.**
Служба безпеки України

# СУЧАСНИЙ СТАН РОЗВИТКУ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Система забезпечення інформаційної безпеки створюється і розвивається відповідно до Конституції України та інших нормативно-правових актів, що регулюють суспільні відносини в інформаційній сфері. Основу даної системи складають органи, сили та засоби забезпечення інформаційної безпеки, які вживають систему адміністративно-правових, інформаційно-аналітичних, організаційно-управлінських, та інших заходів, спрямованих на забезпечення стійкого функціонування системи державного управління.

Відповідно до основ формування можна виокремити основні функції системи забезпечення інформаційної безпеки України.

1. Створення та забезпечення діяльності державних та недержавних органів та організацій – елементів системи забезпечення інформаційної безпеки, що включає:

* розроблення адміністративно-правових засад для побудови та функціонування системи інформаційної безпеки (доктрини інформаційної безпеки, організаційної та функціональної структури системи);

* системне забезпечення діяльності елементів системи: інформаційне, аналітичне, адміністративно-правове, матеріально-технічне, кадрове, ресурсне забезпечення усієї системи державного управління.

2. Управління системою інформаційної безпеки – здійснення свідомого цілеспрямованого впливу суб'єкта управління на загрози та небезпеки, внутрішні та зовнішні чинники, що впливають на стан інформаційної безпеки:

* розроблення на підставі доктрини інформаційної безпеки конкретних планів та технологій забезпечення інформаційної безпеки відповідно до потреб кожного рівня державного управління;

* здійснення прогнозування, планування, організації, регулювання та контролю усією системою інформаційної безпеки та окремими її елементами;

* оцінка результативності дій, витрат на проведення заходів щодо забезпечення інформаційної безпеки.

3. Здійснення планової та оперативної діяльності щодо забезпечення інформаційної безпеки:

* визначення інтересів органів державного управління в інформаційній сфері та їх пріоритетності відповідно до державної інформаційної політики;

* діагностування загроз та небезпек, виявлення джерел їх виникнення, а також прогнозування можливих наслідків у разі настання із відпрацюванням відповідних превентивних заходів.

4. Міжнародне співробітництво в сфері інформаційної безпеки:

* розроблення нормативно-правової бази, що регулює інформаційні відносини між державами та їх взаємодію в галузі інформаційної безпеки;

* входження в існуючі та утворення нових двосторонніх і багатосторонніх структур (організацій), діяльність яких спрямована на розв'язання проблем інформаційної безпеки з урахуванням національних інтересів України [1].

Відповідно до Закону України «Про національну безпеку України» до складу сектору безпеки і оборони входить Служба безпеки України. Згідно з п. 3 ст. 12 вказаного Закону, СБУ неухильно здійснює контррозвідувальний захист державного суверенітету, конституційного ладу і територіальної цілісності, оборонного і науково-технічного потенціалу, кібербезпеки, економічної та інформаційної безпеки держави, об'єктів критичної інфраструктури [2].

Основними чинниками, які характеризують та безпосередньо впливають на розвиток *системи інформаційної безпеки держави* за напрямом протидії розвідувально-підривній діяльності іноземних спецслужб, груп та окремих осіб у кіберпросторі, а також шкідливим кібернетичним впливам на об'єкти критичної інформаційної інфраструктури та електронні інформаційні ресурси держави залишаються:

- спрямування з боку вітчизняних та транснаціональних злочинних хакерських угруповань, в т.ч. за завданнями спецслужб, на блокування роботи об'єктів критичної інфраструктури та фінансово-банківської системи України, комп'ютерних мереж державних органів і установ України, що може призвести до нанесення їм інформаційної шкоди, дестабілізації суспільно-політичної та соціально-економічної ситуації в країні, компрометації діяльності державних та правоохоронних органів, негативного висвітлення в ЗМІ інформації щодо неспроможності врегулювання можливої критичної ситуації в Україні;
- поширення у вітчизняному сегменті мережі Інтернет програмних продуктів для здійснення несанкціонованих втручань у роботу інформаційних систем і локальних мереж передачі даних, спрямованих на отримання несанкціонованого доступу до інформації, яка циркулює в них;
- високий рівень інформатизації та телекомунікації у суспільстві усіх сфер як на державному рівні, так і на рівні звичайних користувачів на тлі низького фахового рівня кінцевих користувачів з одночасним розвитком злочинних механізмів;
- зростаюча популярність використання електронно-обчислювальних машин у протиправній діяльності окремих груп та осіб.

Національна безпека України все більше залежить від доступності, цілісності та конфіденційності інформаційних ресурсів, що забезпечуються інформаційними та комунікаційними технологіями. При цьому, зростання залежності від інформаційно-комунікаційних технологій робить як державні, так і приватні установи уразливими перед можливими негативними наслідками протиправного використання кіберпростору. В цих умовах головними завданнями є вжиття заходів, що дозволяють принципово зменшити або унеможливити повністю негативні наслідки від кібератак.

У гібридній війні, яку проводить РФ проти України, все більшу роль займає кібернетична складова, що супроводжується зростаючою інтенсивністю актів кіберагресії з використанням новітніх розробок методів та інструментів проти України та постійними спробами проведення кібератак на інформаційно-телекомунікаційні системи (ІТС) об'єктів критичної інфраструктури з боку спецслужб та підконтрольних їм хакерських угруповань. У випадку вдалих спроб, нові атаки підвищеної складності використовуються з метою компрометації життєво важливих об'єктів країн Європейського Союзу, НАТО, а також Сполучених штатів Америки та їх союзників.

Виходячи із аналізу чинників та загроз у сфері захисту державних електронних інформаційних ресурсів, є суттєве збільшення кількості кібератак (як правило, вчиняються з територій РФ, Криму й ОРДЛО) на сайти органів державної влади, силових структур і дипломатичних установ для блокування їх роботи, отримання віддаленого доступу до інформації, у т.ч. з обмеженим доступом, та розміщення фейкової інформації. Зазначене спричинено, з-поміж іншого, недотриманням посадовими особами органів державної влади законодавства у сфері технічного захисту інформації, розміщенням офіційних сайтів на серверах хостинг-провайдерів іноземних країн, використанням програмного забезпечення, що має встановлені вразливості та можливість віддаленого доступу/контролю, а також поштових сервісів іноземного походження, особливо з РФ.

До витоку інформації призводять і непоодинокі випадки недбалого ставлення до створення та адміністрування власних веб-ресурсів, що зумовлюється невисокою заробітною платою, яку пропонують державні органи, у зв'язку з чим спеціалісти високої категорії в умовах конкуренції ринку ІТ-послуг обирають більш високооплачувані посади у приватних компаніях.

Також одним із проблемних питань є встановлення комп'ютерних систем захисту на об'єктах критичної інфраструктури, оскільки механізм та цінова політика такої системи не дозволяють багатьом з них забезпечити належний захист інформації відповідно до встановлених державою стандартів.

Таким чином, проблема зростання кіберзагроз стає вкрай актуальною. Злочини із використанням сучасних інформаційно-комунікаційних техно-

логій стають все більш звичним явищем у житті сучасного суспільства. Найбільше фіксується спроб до несанкціонованого втручання та використання можливостей інформаційно-комунікаційних систем державного, кредитно-банківського, комунального, оборонного, виробничого секторів. Інформація з обмеженим доступом, що циркулює в ІТ-системах, є стійким об'єктом зацікавленості з боку інших держав, організацій та окремих осіб. Тому існує велика ймовірність зростання у майбутньому кількості атак на веб-ресурси та ІТС державних установ, організацій, об'єктів критичної інфраструктури, що потребуватиме додаткових затрат на забезпечення їх безперешкодного функціонування та залучення кваліфікованих фахівців в сфері використання комп'ютерних технологій.

**Література**

1. Ліпкан В.М., Максименко Ю.Е., Желіховський В.М. «Інформаційна безпека України в умовах євроінтеграції» https://pidruchniki.com/12631113/politologiya/sistema_zabezpechennya_informatsiynoyi_bezpeki.

2. З У «Про національну безпеку України» // Відомості Верховної Ради, 2018. № 31. ст.241. https://zakon.rada.gov.ua/laws/show/2469-19.

*УДК 340*

**Марченко М. А.**
Служба безпеки України

## ЗАХИСТ ГІДНОСТІ ЛЮДИНИ ТА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Однією із головних якостей людини є гідність, оскільки вона завжди знаходить своє місце поряд із такими якостями, як чесноти, совість, добропорядність. Без перебільшення можна стверджувати, що гідність – це одне із найбільших надбань людства, як загальноісторичних, так і загальнокультурних. Недарма в площині наукового доробку гідність належить до кроссекторальних, міждисциплінарних феноменів, що підлягали вивченню протягом століть представниками філософської, соціологічної і правничої думки.

Саме тому, повага до людини як унікальної біопсихосоціальної цінності, визнання та забезпечення її прав і свобод, честі та гідності, а також гарантування з боку держави захисту від посягань на вищевказані правові категорії є запорукою провідних демократичних країн.

Оніщенко Н.М., у своїх дослідженнях стверджує, що під час розгляду взаємозв'язку держави, права і свободи особи, необхідно зазначити, що

існують права і свободи, які в жодному разі не повинні обмежуватися – це природні права і свободи людини. Основний зміст багатьох юридичних гарантій свободи особи полягає в забезпеченні необхідних умов для нормального життя та активної діяльності громадян у суспільстві [1, с. 72].

Так, відповідно до ст. 3 Закону України «Про національну безпеку України» встановлюються принципи забезпечення державної політики у сферах національної безпеки і оборони, відповідно до змісту яких держава зобов'язана захищати життя і гідність людини та громадянина, їх конституційних прав і свобод [2].

Також, п. 4 ч. 1 ст. 7 КПК України закріплено конституційну норму поваги до людської гідності як одну з основних засад кримінального провадження. Ця норма деталізована також в ст. 11 КПК України, в якій зазначено, що під час кримінального провадження повинна бути забезпечена повага до людської гідності, прав і свобод кожної особи. Забороняється під час кримінального провадження піддавати особу катуванню, жорстокому, нелюдському або такому, що принижує її гідність, поводженню чи покаранню, вдаватися до погроз застосування такого поводження, утримувати особу у принизливих умовах, примушувати до дій, що принижують її гідність [3].

Недарма, діяльність уповноважених органів кримінальної юстиції, в контексті забезпечення інформаційної безпеки держави, відповідно до чинного законодавства України, повинна реалізовуватися із дотриманням принципу «законність».

Взагалі, сам факт наявності кримінального провадження щодо певної людини вже підриває довіру до неї, викликаючи негативне ставлення в оточуючих. У такому випадку повага до гідності людини, по відношенню до якої відкрите кримінальне провадження, вже знаходиться у хиткому становищі: суспільство має до неї вже певні підозри щодо її доброчесності, і це може стати підставою для упередженого її визнання негідною – тобто такою, що не має моральних якостей, зневажає їх, а отже, не заслуговує від суспільства на розуміння та допомогу [4].

Варто погодитись із думкою О.Кучинської, яка стверджує, що гідність особи страждає у результаті доведення до відома громадськості інформації про те, що особа підозрюється або обвинувачується у вчиненні злочину або засуджена за злочин. Більшість слідчих дій, які проводяться з метою встановлення причетності особи до скоєння злочину, наприклад, такі як затримання підозрюваного або арешт, усунення від посади, проведення судово-медичної чи судово-психіатричної експертизи з поміщенням особи на стаціонарне обстеження, обшук і виїмка, не можуть залишитися непоміченими. Не виключається також і можливість поширення відомостей, що порочать особу, в результаті протиправного розголошування да-

них досудового слідства, подробиць інтимного життя та інших відомостей, які особа бажає зберегти в таємниці [5, с. 18].

У багатьох дослідженнях присвячених забезпеченню зазначеної правової категорії під час кримінально-процесуальної діяльності, акцентується увага на тому, що у кримінальному судочинстві під повагою до гідності особи слід розуміти сукупність засобів і методів, що мають на меті забезпечити такий режим провадження у кримінальній справі, за якого визнаються і дотримуються законні інтереси суб'єктів кримінально-процесуальної діяльності, охороняються їх честь і гідність, створюються умови для реального забезпечення і захисту прав та свобод учасників кримінального судочинства, а також гарантується відновлення порушених прав [6, с. 10].

Отже, для поваги до будь-чиєї гідності як важливої соціальної цінності, а також невідчужуваного та непорушного права, необхідні не лише знання норм процесуального та матеріального права, важливо мати належний культурний та моральний рівень розвитку у представників органів кримінальної юстиції, уповноважених на забезпечення інформаційної безпеки нашої держави, оскільки їх специфіка роботи, подекуди, полягає у здійсненні окремих правових обмежень по відношенню до осіб, які підозрюються у здійсненні діяльності, яка містить протиправні ознаки.

**Література**

1. Свобода, гідність та рівність людини крізь європейський фокус / Н.Оніщенко // Матеріали міжнародного науково-практичного семінару присвяченого пам'яті Л.Юзькова. – 2018. – с. 72- 74.

2. Закон України «Про національну безпеку України» від 21.06.2018 р. № 2469-VIII / Верховна Рада України – Режим доступу: https://zakon.rada.gov.ua/laws/show/2469-19.

3. Кримінальний процесуальний кодекс України в редакції від 13.02.2020. р. №4651-VI [Електронний ресурс] / Верховна Рада України – Режим доступу: https://zakon.rada.gov.ua/laws/show/4651-17.

4. Щодо правової природи поваги до людської гідності як загальної засади кримінального провадження / А.О.Полянський [Електронний ресурс] / Режим доступу: http://oaji.net/articles/2017/976-1493193103.pdf

5. Кучинська О.П. Принцип поваги до честі і гідності людини у кримінальному процесі / О.П. Кучинська // Адвокат. – 2012. – № 4 (139). – С. 17–19.

6. Бартащук Л. П. Гарантії забезпечення права людини на повагу до честі і гідності у кримінальному судочинстві України : автореф. дис… канд. юрид. наук / Л. П. Бартащук. – К., 2011. – 22 с.

*УДК 378:004.9:355.085.5*
**Марченков С. М.**
Житомирський військовий інститут
імені С. П. Корольова

# ІНТЕГРАЦІЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ КОМПЕТЕНТНОСТІ ОСОБИСТІ В ПРОЦЕС АНАЛІЗУ ІНФОРМАЦІЙНИХ ПОВІДОМЛЕНЬ, ЯК ЗАГРОЗ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Важливою і невід'ємною складовою національної безпеки держави є інформаційна безпека. Яка значною мірою впливає на рівень і темпи соціально-економічного, науково-технічного, й культурного розвитку. Тому розвиток України як суверенної, демократичної, правової та економічно стабільної держави можливий за умови забезпечення інформаційної безпеки [1, с. 5]. Із зростанням науково-технічного прогресу буде зростати і важливість питання інформаційної безпеки громадянина, суспільства, держави. Відповідно зростає вага інформаційного впливу як фактору формування суспільної свідомості. З огляду на аналіз тенденцій розвитку міжнародної та регіональної обстановки, наявних регіональних проблем, а також національних інтересів України стає актуальним питання своєчасного виявлення ознак інформаційно-психологічного впливу в потоці інформаційних повідомлень. Події останніх років підтвердили недостатній рівень інформаційної захищеності як особистості так і нашої держави в цілому. Завдяки багаторічній безперешкодній пропаганді російських засобів масової інформації на різні види цільової аудиторії, головним об'єктом на якому концентрується безпосередній вплив деструктивного характеру у межах заходів психологічного впливу, є громадська думка та свідомість окремої людини. Тому російським пропагандистам вдалося заручитися підтримкою значної частини українських громадян, що призвело до зниження спочатку авторитету держави та її громадських інститутів в очах українського суспільства, а потім і авторитету держави на міжнародній арені, втрати контролю над АР Крим та значними ділянками на територіях Донецької та Луганської області. Все це підтверджує відсутність дієвої цілісної системи інформаційно-аналітичного забезпечення органів влади та управління, що значно ускладнює прийняття ними зважених рішень, а навпаки породжує конфліктні ситуації у владних структурах держави та суспільстві. Сьогодні кожний громадянин України має володіти високим рівнем культури у сфері інформаційної безпеки країни, суспільства, особистості, розуміти механізми інформаційного (інформаційно-психологічного впливу) та захисту від нього.

Тому актуальним постає питання інтеграції інформаційно-аналітичної компетентності особисті в процес аналізу інформаційних повідомлень, як загроз національної безпеки України.

Розглянемо базові поняття щодо визначення таких понять як: інформаційна безпека держави, інформаційна безпека суспільства, інформаційна безпека особистості, а також інформаційно-аналітична компетентність.

Інформаційна безпека держави – це стан її захищеності та інформаційного розвитку, при якому акції інформаційного впливу, спеціальні інформаційні операції, інформаційний тероризм, незаконне зняття інформації за допомогою спеціальних технічних засобів та комп'ютерна злочинність не завдають суттєвої шкоди національним інтересам [1, с. 10].

Інформаційна безпека суспільства – можливість безперешкодної реалізації суспільством й окремими його членами своїх конституційних прав, пов'язаних з із вільним одержанням, обробленням, створенням і поширенням інформації, а також ступінь їх захисту від деструктивного інформаційного впливу [1, с. 10].

Інформаційна безпека особистості – це стан захищеності психіки та здоров'я особистості від деструктивного інформаційного впливу, який призводить до неадекватного сприйняття нею дійсності або погіршення її фізичного стану [1, с. 10].

Інформаційно-аналітична компетентність – це ставлення до інформації та критичне усвідомлення її цінності, інформаційно-аналітичні знання, навички, вміння, здатності, професійно важливі якості, особистий досвід у сфері пошуку, оцінювання, використання, збереження, аналізу, оформлення та передачі інформації за допомогою різних засобів, методів і форм інформаційно-аналітичної діяльності, що дозволяє оперативно орієнтуватися в інформаційному просторі, брати участь у його формуванні [2, с. 320].

Відповідно до визначення основних реальних та потенційних загроз інформаційній безпеці України, які зазначені у доктрині інформаційної безпеки України, а саме: поширення у інформаційному просторі недостовірної та упередженої інформації, що завдає шкоди національним інтересам України; негативні інформаційні та психологічні впливи, спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності й недоторканості кордонів України; зовнішні негативні інформаційні та психологічні впливи на суспільну свідомість через засоби масової інформації, соціальні мережі та мережу інтернет; використання різних каналів розповсюдження для пропаганди сепаратизму за етнічною, мовною, релігійною та іншими ознаками та інші.

Таким чином враховуючи основні загрози та спираючись на визначення інформаційно-аналітичної компетентності, можна стверджувати, що інтеграція інформаційно-аналітичної компетентності особисті в процес аналізу інформаційних повідомлень, як загроз національної безпеки Укра-

їни підвищує можливість своєчасного виявлення негативного впливу із глобального інформаційного потоку, його аналізу, та в подальшому прогнозуванні сценаріїв, за якими можуть розвиватися події, для адекватного усвідомлення інформації яка поширюється у інформаційному просторі.

**Література**

1. В. Петрик, М. Присяжнюк, Д. Мельник Інформаційна безпека держави: підручник. – Київ: ДНУ Книжкова палата України, 2016. – 264 с.
2. Ягупов В. Педагогіка : навч. посіб. Київ : Либідь, 2002. – 560 с.

*УДК 355.40:356.35*

**Мілих Є. Г.**
Національний університету оборони України
імені Івана Черняховського

## ІМПЕРАТИВИ СИСТЕМИ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ

Стратегічні комунікації є тим інструментом, що відповідає всім вимогам щодо протидії гібридній агресій Російської Федерації, а також застосовується в сучасній практиці провідних країн світу. З огляду на специфічний стан неоголошеної війни в Україні для застосування нашою державою інструменту стратегічних комунікацій вважаємо за доцільне звернутися передусім до досвіду НАТО.

Стратегічні комунікації в НАТО являються особливою формою гармонізації тем, ідей, образів і дій. Прийнято вважати, що стратегічні комунікації це не просто питання “повідомлення”, “відправника” і “отримувача” за класичною схемою комунікативного акту. Стратегічні комунікації передбачають діалог і підхід до побудови відносин на основі уважного ставлення до культурних та історичних особливостей, місцевих способів ведення справ і виявлення місцевих лідерів думок. У військовій сфері, як правило, йдеться про гармонізацію всіх заходів у сфері публічної дипломатії, зв’язків із громадськістю та (військових) інформаційних операцій. Тому стратегічні комунікації є одночасно і процесом (узгодження слів і справ з метою впливу та надання інформації), і результатом цього процесу [1, с. 12].

Стратегічні комунікації в інтересах операції Збройних Сил України передусім мають бути спрямовані на підрив і делегітимізацію противника у спосіб набуття підтримки й визнання з боку місцевого населення, електорату своєї країни, міжнародної громадськості та всіх інших цільових груп. Сутність стратегічних комунікацій полягає в тому, що сформульовані для різних цільових аудиторій меседжі не конфліктують один з одним [2, с. 6].

Ключові компоненти процесу реалізації стратегічних комунікацій [3, с. 24]:

розуміння владою суспільства, його інформування та залучення для просування інтересів і цілей через вплив на сприйняття, установки, переконання та поведінку;

узгодження дій, зображень, висловлювань на підтримку політики й планування з метою досягнення всеосяжних стратегічних цілей (overarching strategic objectives);

визнання того, що всі операції і види діяльності є важливими компонентами процесу комунікації, оскільки все, що говорить і робить НАТО, має передбачувані й непередбачувані наслідки для цільових і нецільових аудиторій;

визнання того, що стратегічні комунікації є не додатковими діями, а невід'ємною частиною планування та реалізації усіх воєнних операцій та видів діяльності.

У МОУ та ЗСУ сьогодні існує нагальна потреба запровадження загальнодержавного механізму управління процесом забезпечення інформаційної безпеки держави у воєнній сфері. Цей процес є складним і багатогранним, оскільки може охоплювати цільові програми, проекти та окремі дії (заходи, роботи), спрямовані на реалізацію певного порядку забезпечення інформаційної безпеки держави у воєнній сфері. Виконавцями цього процесу повинні бути профільні структури як у складі МОУ та ЗСУ, так і інших суб'єктів сектора безпеки та оборони держави, а також задіяні підприємства й установи України, котрі не належать до названих суб'єктів.

Для того, щоб такий механізм управління комунікативними можливостями держави міг бути запроваджений у МОУ та ЗСУ і став дієздатним (ефективним), необхідно створити потужний орган управління та відповідну структуру, яка безпосередньо відповідатиме за організацію та функціонування системи забезпечення інформаційної безпеки МОУ та ЗСУ. При цьому створення системи потребує виконання певних заходів у самих МОУ та ЗСУ.

Використовуючи наведені підстави, можна запропонувати варіант системи стратегічних комунікацій МОУ та ЗСУ:

1. Система стратегічних комунікацій МОУ та ЗСУ входить до загальнодержавної системи стратегічних комунікацій (яка очолюється на рівні Ради національної безпеки і оборони України та Адміністрації Президента України.

2. Координуючим органом у системі стратегічних комунікацій МОУ та ЗСУ є Ситуаційний центр стратегічних комунікацій, безпосередньо підпорядкований заступникові міністра оборони України з питань євроінтеграції.

Отже, змістовим ядром стратегічних комунікацій є формування базисного стратегічного наративу з переконливою сюжетною лінією, яка може пояснити події аргументовано і з якої можна дійти висновків щодо причин перебування держави в конфлікті, значення цього становища та щодо перспектив держави в разі успішного виходу з нього.

**Література**

1. Paul C.Getting Betterat Strategic Communication / Christopher Paul; RAND Corporation. – SantaMonica, 2011. – 18 p.

2. Strategic Communications and National Strategy : A Chatham House Report/ Paul Cornish, Julian Lindley French and ClaireYorke. – London, 2011. – 42 p.6 Код OF5 (стосується сухопутних військ) системи уніфікованих військових звань НАТО є еквівалентним званню полковника.Стратегічні пріоритети, № 1 (34), 2015 р.

3. US Department of Defense : Report on Strategic Communication [Електронний ресурс]. – Режим доступу: http://www.au.af.mil/au/awc/awcgate/dod/dod_report_strategic_communication_11feb10.pdf.

*УДК 32.019.5:351.86*

**Міхєєв Ю. І.**
кандидат технічних наук,
Житомирський військовий інститут
імені С. П. Корольова

## ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ РОЗРОБЛЕННЯ ІНФОРМАЦІЙНИХ МАТЕРІАЛІВ В ІНТЕРЕСАХ ПРОВЕДЕННЯ ПСИХОЛОГІЧНИХ АКЦІЙ

Аналіз досвіду ведення Російською Федерацією “гібридної війни” проти України підтверджує факт постійного нарощування противником своїх ресурсів для реалізації мети психологічної операцій (акцій), спрямованих на цивільне населення, особовий склад Збройних Сил України та інших силових відомств. Запобігти реалізації мети таких психологічних операцій (акцій) можливо за рахунок своєчасного впровадження відповідних контрзаходів. Не зважаючи на те, що сьогодні завданню з забезпечення інформаційно-психологічної психологічної безпеки приділяється достатня увага [1–3], основними проблемними питаннями при цьому в Україні на даному етапі залишаються: своєчасне виявлення матеріалів з ознаками психологічного впливу; оцінювання ситуації та планування відповідних контрзаходів; розробка та поширення інформаційних матеріалів; оцінювання ефективності проведених заходів.

В умовах обмеження часового ресурсу єдиним можливим шляхом забезпечення ефективного виконання заходів з протидії є автоматизація та інтелектуалізація завдань на всіх вищезазначених етапах. Тому вкрай необхідно своєчасно розробляти власні, якісні та різноманітні за видом інформаційні матеріали, які спрямований на визначену цільову аудиторію. Складність реалізації зазначеного завдання пов'язана з тим, що, по-перше, для розроблення таких матеріалів необхідна наявність певних вихідних даних (мета операції, характеристики цільової аудиторії, аргументи, правила створення відповідного типу матеріалів), а по-друге, накладаються значні обмеження за часом.

У доповіді розглядається процес автоматизації етапів проведення психологічних операцій (акцій): планування операції; аналіз цільової аудиторії; розвиток серії; розроблення інформаційних матеріалів; затвердження матеріалів; розповсюдження матеріалів; аналіз результатів проведення операції.

Розглянуто архітектуру спеціалізованого програмного забезпечення для створення інформаційних матеріалів, спрямованих на визначену цільову аудиторію. Під час розроблення програмного забезпечення враховано підхід з планування психологічних акцій, дій та заходів спеціальними підрозділами Збройних Сил України та країн НАТО [4]. Для аналізу цільової аудиторії доцільним визначено застосування маркетингових технологій. Кінцевий результат роботи програмного забезпечення являє собою концепт створення друкованих інформаційних матеріалів психологічного впливу.

**Література**

1. Сніцаренко П. М. Методика оцінки рівня деструктивного інформаційного впливу на об'єкти інформаційної інфраструктури держави / П. М. Сніцаренко, Ю. О. Саричев, П. Д. Рогов // Зб. наук. праць. – К. : ВІТІ ДУТ, 2014. Вип. № 1. – С. 88–96.

2. Горбулін В. П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання : монографія / В. П. Горбулін, О. Г. Додонов, Д. В. Ланде. – К. : Інтертехнологія, 2009. – 164 с.

3. Інформаційний вплив: теорія і практика прогнозування : монографія / за ред. П. Д. Фролова. – К. : Міленіум, 2011. – 303 с.

4. Field Manual 33-1-1 – Psychological Operations Techniques and Procedures [Electronic resource]. – Mode of access: http://www.enlistment.us/field-manuals/fm-33-1-1-psychological-operations-techniques-and-procedures.shtml.

*УДК 007: 304.070+004.738*
**Недзельський Ю. О.**
кандидат історичних наук
**Куксенко В. С.**
Воєнно-дипломатична академія
імені Євгенія Березняка

# ДЕМОКРАТИЧНИЙ ВИМІР ПРОЄКТУ ЗАКОНУ УКРАЇНИ "ПРО МЕДІА"

Турбулентність організаційних процесів спрямованих на упорядкування діяльності суб'єктів інформаційного простору України в умовах гібридної війни обумовлює їх актуальність. У цьому контексті не аби якого значення набуває необхідність перегляду наявної нормативно-правової бази для приведення її у відповідність до вимог часу сучасного інформаційного суспільства демократичної держави.

Представлений на розгляд Верховної Ради України проєкт Закону України від 27.12.2019 р. № 2693 "Про медіа" в значній мірі спрямований на вирішення цієї проблеми, проте аналіз цього законопроекту викликає певні занепокоєння у представників ЗМІ, зокрема журналістів.

У пояснювальній записці до цього законопроєкту зазначено, що його метою є створення єдиної, впорядкованої та взаємоузгодженої системи правових норм, спрямованих на регулювання правовідносин у сфері медіа, виконання Україною зобов'язань перед європейськими партнерами та імплементація норм європейського законодавства у національне законодавство України шляхом забезпечення реалізації права на свободу вираження поглядів, права на отримання різнобічної, достовірної та оперативної інформації, на забезпечення плюралізму думок і вільного поширення інформації, на захист національних інтересів України та прав користувачів медіа-сервісів, регулювання діяльності в сфері медіа відповідно до принципів прозорості, справедливості та неупередженості, стимулювання конкурентного середовища, рівноправності та незалежності медіа [1].

Проте, не всі представники медіа середовища, зокрема журналісти світових ЗМІ вважають, що новий проєкт закону у достатній мірі відповідає демократичним цінностям суспільства та держави. І дійсно, заборона цензури на інформацію, ще не є ознакою демократичного відкритого діалогу між державою та суспільством, адже існують і інші дієві механізми управління суб'єктами інформаційного простору [2].

Зокрема, про такі механізми їдеться у розділі IV законопроєкту (вимоги до змісту інформації та організації надання медіа-сервісів), статті 36 (обов'язки суб'єктів у сфері медіа щодо організації надання медіа-сервісів), де зазначено про те, що суб'єкти у сфері медіа зобов'язані:

“отримувати ліцензію, проходити реєстрацію або отримувати дозвіл на тимчасове мовлення, якщо запланована діяльність потребує отримання ліцензії, обов’язкової реєстрації або отримання дозволу на тимчасове мовлення…”.

Таким чином вбачається, що цей законопроєкт юридично обмежує повноваження та сферу діяльності журналістів та блогерів, які, у разі прийняття цього закону не отримавши з тих чи інших причин ліцензію, не зможуть пройти акредитацію, і відповідно не зможуть виробляти та поширювати інформацію у медіа-простору нашої держави.

Більш того, відповідно до законопроєкту органом державного регулювання діяльності у сфері медіа, а також органом нагляду (контролю) є Національна рада України з питань телебачення і радіомовлення, яка має своє бачення щодо змісту діяльності сучасних ЗМІ у медіа-просторі. До речі, відповідно до Закону України “Про Національну раду України з питань телебачення і радіомовлення”, до її складу входить вісім осіб. З них чотири члени Національної ради призначаються Верховною Радою України і чотири члени Національної ради призначаються Президентом України [3].

Стратегію інформаційної політики в медіа-просторі демократичної держави також визначає регулятор – Національна рада України з питань телебачення і радіомовлення. Таким чином є підстави, вважати, що медіа простір України буде залишатися сферою конфліктів інтересів між суб’єктами інформаційного простору.

Таким чином можна зробити висновок, що не всі суб’єкти мас-медіа (які діють на теперішній час) будуть “вписуватись” у майбутні плани реалізації Стратегії інформаційної політики в медіа-просторі.

Узагальнюючи вищезазначене, варто зрозуміти status-quo сучасного медіа простору України та перспективи його розвитку в контексті законопроєкту “Про медіа”, текст якого в три рази більший ніж текст Конституції України.

Відтак, офіційні висновки Головного науково-експертного управління Апарату Верховної Ради України: за результатами розгляду у першому читанні законопроєкт про медіа, реєстр № 2693 та законопроєкт про медіа в Україні реєстр № 2693-1 доцільно повернути суб’єктам права законодавчої ініціативи на доопрацювання [4] можна вважати правильним з точку зору сучасних демократичних перетворень громадського суспільства України.

**Література**

1. Пояснювальна записка до проекту Закону України “Про медіа” [Електронний ресурс]. – Режим доступу: http://search.ligazakon.ua/l_doc2.nsf/link1/GI01091A.html.

2. Законопроєкт про дезінформацію - боротьба з фейками чи цензура ЗМІ? [Електронний ресурс]. – Режим доступу: https://www.youtube.com/watch?v=vZoFzdbaO0A.

3. Закон України Про Національну раду України з питань телебачення і радіомовлення [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/538/97-%D0%B2%D1%80.

4. Проект Закону про медіа [Електронний ресурс]. – Режим доступу: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=67812.

*УДК 004.056.5*

**Пальчик М. Л.**
кандидат юридичних наук,
Національна академія СБ України

## РОЛЬ ОСВІТНІХ ПРОГРАМ У ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ

На сьогодні неможливо уявити наше життя без інформаційно-комунікаційних технологій. Майже кожен має аккаунт у соціальній мережі, користується електронною поштою, численними месенджерами та сервісами, вносить свої персональні дані в додатки для здійснення численних платежів та покупок у мережі Інтернет. Щодня відбувається передача величезної кількості інформації між фізичними особами, підприємствами та державними інституціями. На об’єктах критичної інфраструктури циркулюють значні масиви інформації, а за допомогою інформаційних технологій автоматизовано численні операційні процеси.

Активне впровадження інформаційних технологій та комп’ютерних мереж в усі сфери сучасного життя відкриває широкі можливості, забезпечує доступ до значних обсягів інформації, сприяє швидкому поширенню новітніх ідей, стимулює розвиток економіки та в цілому є рушійною силою розвитку сучасності. Водночас, поряд із значними перевагами, розвиток цифрових технологій створює нові ризики та можливості для незаконної діяльності у кіберпросторі, зміщення акцентів розвідувально-підривної та іншої протиправної діяльності на шкоду національним інтересам України у кібернетичний простір.

Варто зауважити, що вказані виклики актуалізуються в умовах постійного збільшення кількості користувачів, у тому числі всесвітньої мережі Інтернет. Так, за результатами дослідження Інтернет асоціації України кількість користувачів інтернетом у 2019 році збільшилась на 8% порівняно з показником 2018 року, та склала 22,96 млн або 71% населення. За даними дослідження, 66% інтернет-користувачів використовують для виходу в інтернет смартфон, 40% – домашній ноутбук, 36% – стаціонарний домашній комп’ютер, 5% – стаціонарний комп’ютер на роботі [1].

В умовах постійного збільшення аудиторії актуалізуються питання дотримання елементарних правил поводження у кіберпросторі, а також розуміння основ забезпечення як особистісної безпеки, так і захисту персональних даних у мережі. Про це також зазначають і міжнародні експерти, які одним з основних трендів кібербезпеки на 2019 рік визначили «підвищення обізнаності», що є одночасно і трендом і напрямом як інформаційної, так і кібербезпеки. При чому на їх думку, навчати елементарним навичкам забезпечення інформаційної безпеки сьогодні потрібно ще в школі. Адже незважаючи на те, що діти та підлітки здебільшого краще обізнані в технологіях, ніж батьки, водночас саме молодь не завжди володіє знаннями про те як захистити себе та свої дані у мережі [2].

Варто зазначити, що в окремих іноземних державах вже розроблено та активно впроваджено освітні програми з кібербезпеки, у тому числі, для навчальних закладів. Так, у Великій Британії з вересня 2017 року реалізується освітній проект, розрахований на 5 років, у межах якого, у школах країни почали викладати новий предмет – кібербезпека. Вказаний предмет викладається учням віком від 14 років, щотижня, у межах додаткових 4 годин навчання, на яких школярів знайомлять з основними методами захисту від хакерських атак [3].

Розпочато роботу за вказаним напрямом і в України, тим більше, що, затвердженою у 2016 році Стратегією кібербезпеки України, підвищення цифрової грамотності громадян та культури безпекового поводження у кіберпросторі, а також впровадження державних і громадських проектів підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту визначено одним із пріоритетних напрямів забезпечення кібербезпеки України [4].

Так, працівниками кіберполції регулярно проводяться освітньо-просвітницькі заходи, зокрема лекції з кібербезпеки у школах, тематичні зустрічі з представниками вищих учбових навчальних закладів тощо. У березні минулого року кіберполіція запустила окрему інформаційну кампанію з обізнаності про кібербезпеку. У межах цієї кампанії здійснюється поширення інформації про основи захисту у мережі Інтернет та забезпечення кібербезпеки. Громадянам доводиться інформація про наслідки нехтування елементарними заходами безпеки в мережі, починаючи від слабкого паролю, закінчуючи використання неліцензійного програмного забезпечення та ін. Також, у рамках вказаної програми кіберполіція ініціює поширення соціальної реклами, націленої на підвищення рівня обізнаності громадян з кібербезпеки та створення окремого ресурсу на сайті кіберполіції для перевірки легітимності інформації (сайт, номер мобільного телефону, номер банківської картки). Крім того, серед громадян буде поширюватися друкована інформація з елементарними правилами кіберзахисту [5].

У 2019 році у цьому напрямку розпочало роботу новостворене Міністерство цифрової трансформації України, яке запустило онлайн-

платформу з цифрової грамотності – «Дія. Цифрова освіта». На сьогодні, на вказаній платформі доступні кілька навчальних відео курсів, серед яких: базовий із цифрової грамотності (має три рівні знань); для вчителів; для батьків «Онлайн-безпека дітей». У подальшому плануються до запуску ще п’ять категорій курсів з медіаграмотності [6].

Як можемо бачити проблема підвищення обізнаності громадян є однією з актуальних проблем забезпечення кібербезпеки на сучасному етапі. Її вирішення здійснюється, у тому числі, через реалізацію освітньо-просвітницьких програм, направлених на формування впевненості користувачів різних вікових груп у користуванні кіберпростором.

Гарним доповненням до вже розпочатої роботи з підвищення обізнаності з кібербезпеки може бути долучення інших державних та правоохоронних органів, а також громадських організацій, приватних суб’єктів до розроблення та впровадження подібних освітніх програм з метою формування стійкого розуміння основних ризиків використання кіберпростору серед звичайних громадян. Окремим напрямом може стати запровадження, подібних до іноземних, освітніх програм у загальноосвітніх навчальних закладах на кшталт запроваджених програм з медіа грамотності.

**Література**

1. В Україні кількість інтернет-користувачів зросла до 23 мільйонів, Укрінформ, 10.10.2019 [Електронний ресурс]. – Режим доступу: https://www.ukrinform.ua/rubric-technology/2797152-v-ukraini-kilkist-internetkoristuvaciv-zrosla-do-23-miljoniv.html.

2. Top Seven Cybersecurity Trends for 2019, Binary District Journal, 2018 [Електронний ресурс]. – Режим доступу: https://journal.binarydistrict.com/7-top-cybersecurity-trends-for-2019/.

3. У школах Англії з’являться уроки з кібербезпеки, 12.02.2017 [Електронний ресурс]. – Режим доступу: https://www.ukrinform.ua/amp/rubric-technology/2174346-v-skolah-anglii-zavlatsa-uroki-kiberbezpeki.html.

4. Указ Президента України про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» від 15 березня 2016 року № 96/2016. – Офіційний Вісник України від 29 березня 2016 року. – Офіц. вид. – К., 2016. – № 23. – Ст. 899.

5. Кіберполіція запустила кампанію з обізнаності про кібербезпеку, 06.03 2019 [Електронний ресурс]. – Режим доступу: https://cyberpolice.gov.ua/news/kiberpolicziya-zapustyla-kampaniyu-z-obiznanosti-pro-kiberbezpeku-8091/].

6. «Дія. Цифрова освіта»: Мінцифра запустила онлайн-платформу з цифрової грамотності, [Електронний ресурс]. – Режим доступу: https://nachasi.com/2020/01/21/online-platforma-series-education/.

*УДК 32.019.53*
**Партоленко І. В.**
кандидат політичних наук
**Чулкова О. В.**
Академія зовнішньої розвідки України

# ПРОБЛЕМНІ ПИТАННЯ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОЇ БЕЗПЕКИ УКРАЇНИ

В українських реаліях ера інформаційного суспільства характеризується домінуючою роллю інформації та знань, створенням глобального інформаційного простору, в якому завдяки високорозвинутим інформаційно-комунікативним мережам і технологіям забезпечуватиметься стале економічне та соціальне зростання, вільний доступ до світових інформаційних ресурсів, що дасть змогу людям повною мірою використовувати свій потенціал та реалізовувати власні прагнення.

У цьому контексті закономірно зростає роль і самої державної інформаційної політики, адже за останні роки суттєво змінилася парадигма інформаційної безпеки нашої держави.

Саме інформаційна політика є складовою частиною загальнодержавного вектора розвитку і цілковито наслідує методи формування та реалізації у відповідному нормативно-правовому полі через низку таких документів: доктрини, стратегії, концепції, плани.

Значущість інформаційної безпеки як складової національної безпеки України пояснюється залежністю реалізації найбільш важливих інтересів України в зовнішньополітичній сфері від інформаційних загроз.

Інформаційна безпека (згідно із законодавством України) – стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, за якого завдають шкоди через: неповноту, несвоєчасність та недостовірність поширюваної інформації; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання, порушення цілісності, конфіденційності та доступності інформації [1].

Перша Доктрина інформаційної безпеки України, була затверджена Указом Президента України від 8 липня 2009 р. № 514/2009, вона передбачала, що "…за умов глобальної інтеграції та жорсткої міжнародної конкуренції головною ареною зіткнень і боротьби різновекторних національних інтересів держав стає інформаційний простір", у новій Доктрині інформаційної безпеки України від 25 лютого 2017 р. № 47/2017, як особливий інструмент досягнення мети Доктрина-2017 визначено систему комунікацій (стратегічних, урядових, кризових), за допомогою яких можна реалізовувати заходи по забезпеченню інформаційної безпеки [2].

У Стратегії національної безпеки України, затвердженій Указом Президента України від 26 травня 2015 р., пріоритетами забезпечення інформаційної безпеки визначено, зокрема: протидію інформаційним операціям проти України, маніпуляціям суспільною свідомістю і поширенню спотвореної інформації, захист національних цінностей та зміцнення єдності українського суспільства; розробку і реалізацію скоординованої інформаційної політики органів державної влади; створення і розвиток інститутів, що відповідають за інформаційно-психологічну безпеку, з урахуванням практики держав – членів НАТО та ін. [3].

Усе це зумовлює потребу в теоретичному осмислені основних політичних процесів, визначенні об'єктів, на які постійно впливають в Україні інші держави, руйнуючи українську державність та цілісність, а також коригують нашу ідеологію та свідомість. Власне кажучи, тому інформаційну сферу можемо віднести до особливої сфери національної безпеки.

Отже, для визначення засобів протидії інформаційно-психологічному впливу передусім варто артикулювати структурні елементи цього процесу, від успішного вирішення питань даної сфери залежить забезпечення загальної світової безпеки. На нашу думку, мету, з якою здійснюються інформаційні впливи, необхідно визначати відповідно до кожного із суб'єктів агресивного інформаційно-психологічного впливу. Слід пам'ятати, що головними критеріями успішності інформаційно-психологічних впливів є їхній так званий пролонгований ефект та осучаснення векторності діяльності держави у захисті інформаційного простору країни від зовнішньої інформаційної агресії.

**Література**

1. Закон України «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» (Закон від 09.01.2007 № 537-V).

2. Указ Президента України №47/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 р. «Про Доктрину інформаційної безпеки України». – [Електронний ресурс]. – Режим доступу: http://www.president. gov.ua/documents/472017-21374.205.

3. Указ Президента України від 26 травня 2015 р. № 287/2015 «Стратегія національної безпеки України» – [Електронний ресурс]. – Режим доступу: http://goo/gl/OvFRER.

*УДК 378.1:658.5*
**Перегуда О. М.**
кандидат технічних наук,
старший науковий співробітник
**Піонтківський П. М.**
кандидат технічних наук,
старший науковий співробітник
**Черкес О. П.**
Житомирський військовий інститут
імені С. П. Корольова

# ФОРМУВАННЯ ЄДИНОГО ІНФОРМАЦІЙНОГО ОСВІТНЬО-НАУКОВОГО СЕРЕДОВИЩА ВВНЗ В УМОВАХ ІНТЕГРАЦІЇ УКРАЇНИ ДО ЄВРО-АТЛАНТИЧНОГО ПРОСТОРУ

Розробка та впровадження в усіх сферах діяльності Збройних Сил України стандартів та процедур, прийнятих у державах – членах НАТО, запровадження інформаційно-комунікаційних технологій (ІКТ), в процеси управлінської діяльності вищого військового навчального закладу (ВВНЗ), дозволяє формувати єдине інформаційне середовище, забезпечувати набуття інформаційних спроможностей для отримання, опрацювання, зберігання, передачі, контролю та надання інформації для всіх суб'єктів освітнього процесу від керівної ланки до курсантів [1].

Відтак стратегія створення у ВВНЗ передумов єдиного інформаційного освітньо-наукового середовища має концентруватися на створенні умов сприятливих для інноваційної діяльності та впровадження ІКТ в усіх сферах діяльності ВВНЗ від освітнього процесу та наукових досліджень до виконання завдань житлового, фінансового, тилового, технічного забезпечення.

Для досягнення цих цілей важливо ефективніше використовувати переваги нових інформаційних технологій і систем; впроваджувати телекомунікаційні мережі, що дозволить нарощувати спроможності ВВНЗ у підготовці військових фахівців за стандартами НАТО, здійснювати інтеграцію у світовий освітньо-науковий простір, підвищувати конкурентоспроможність навчального закладу [2-3].

Інформація про успішний досвід провідних ВВНЗ та потреби потенційних замовників освітніх послуг, є важливими знаннями, необхідними для формування та втілення стратегії розвитку ВВНЗ, прогнозування ризиків, здійснення вибору альтернативних управлінських рішень в короткостроковій і довгостроковій перспективі, накопичення корпоративних знань.

Спрямованість на проведення наукових досліджень виключно за найбільш актуальними для військ і, у першу чергу, для ведення реальних бо-

йових дій темами, супроводження науково-дослідних робіт потребує створення єдиної бази даних наукових розробок та інноваційних проектів, забезпечення доступу до інформаційних ресурсів світових наукових центрів. Використання методології бенчмаркінгу, інноваційного менеджменту дає можливість адаптувати нові моделі управління для удосконалення власної діяльності. Переважна більшість дослідників єдині в своїх поглядах на бенчмаркінг як на процес, що включає вивчення інформації, запозичення досвіду і адаптацію найкращої практики для удосконалення своєї діяльності.

Необхідно проводити аналіз використання методології стратегічного менеджменту, інноваційного, інформаційного менеджменту та управління знаннями (information and knowledge management) в процесі підготовки військових фахівців, що реалізовані у державах – членах НАТО. Завданням інформаційного менеджменту в НАТО є набуття інформаційної переваги, яка досягається шляхом створення сприятливих умов для забезпечення відповідних посадових осіб різних ланок управління.

Технологія пошуку та здобуття нових знань, їх систематизація вимагає застосування інформаційно-пошукових систем, експертних систем тощо. Застосування вищезазначених технологій забезпечує досягнення результату, але потребує доволі багато часу. Це вимагає необхідності використання методів штучного інтелекту, математики і статистики, використання програмного забезпечення, призначеного для збирання, обробки та створення єдиного інформаційного середовища [4].

Сучасна система пошуку знань дає змогу здійснювати моніторинг інформації, забезпечити об’єднання інформаційно-освітніх ресурсів, накопичених науково-дослідними інститутами і освітніми установами.

**Література**

1. Google Scholar Citations. URL: https://scholar.google.com.ua/citations?user=LuctT5cAAAAJ&hl=ru (last accessed: 03.03.2020).

2. Автореферат. Автоматизована система управління повсякденною діяльністю вищого військового навчального закладу на базі локальної обчислювальної мережі. URL: http://referatu.net.ua/newreferats/7569/181662 (дата звернення: 26.11.2019).

3. Карпенко М. Ю., Манакова Н. О., Гавриленко І. О. Технології створення програмних продуктів та інформаційних систем : навч. посібник. Харків : нац. ун-т міськ. госп-ва ім. О. М. Бекетова. Харків : ХНУМГ ім. О. М. Бекетова, 2017. 93 с.

4. To Make Choice: программные системы поддержки принятия оптимальных решений. URL: http://www.tomakechoice.com/program.html (дата обращения: 03.03.2020).

*УДК 321.011:65.012.8*
**Плетньов О. В.**
кандидат юридичних наук,
**Коваленко Є. В.**
кандидат юридичних наук,
Інститут підготовки юридичних
кадрів для Служби безпеки України
Національного юридичного
університету імені Ярослава Мудрого

# ЗАВДАННЯ ПІДРОЗДІЛІВ СБ УКРАЇНИ У СФЕРІ ЗАХИСТУ ІНФОРМАЦІЙНОГО СУВЕРЕНІТЕТУ УКРАЇНИ

Наразі поняття «інформаційного суверенітету» передбачено у ст. 1 Закону України «Про Національну програму інформатизації», де він визначається як здатність держави контролювати і регулювати потоки інформації з-поза меж держави з метою додержання законів України, прав і свобод громадян, гарантування національної безпеки держави [1]. Таким чином в законодавстві передбачено 3 ключових суспільних інтереси, яким завдається шкода внаслідок порушення державного суверенітету, серед яких законодавець визначає також національну безпеку України.

Водночас, вперше в українській нормативно-правовій практиці поняття «інформаційний суверенітет» з'явилось в Законі України «Про інформацію» (редакціях 2002 – 2011 рр.) [2]. Ст.53 цього закону передбачала, що «основою інформаційного суверенітету України є національні інформаційні ресурси. До інформаційних ресурсів України входить вся належна їй інформація, незалежно від змісту, форм, часу і місця створення. Україна самостійно формує інформаційні ресурси на своїй території і вільно розпоряджається ними, за винятком випадків, передбачених законами і міжнародними договорами». Ст. 54 («Гарантії інформаційного суверенітету») зазначала, що «інформаційний суверенітет України забезпечується: виключним правом власності України на інформаційні ресурси, що формуються за рахунок коштів державного бюджету; створенням національних систем інформації; встановленням режиму доступу інших держав до інформаційних ресурсів України; використанням інформаційних ресурсів на основі рівноправного співробітництва з іншими державами». Змінами, внесеними 09.05.2011 р. вказані статті були виключені з тексту цього закону.

Наразі згадування інформаційного суверенітету України міститься в Рішенні Ради національної безпеки і оборони України від 29 грудня 2016 року Про Доктрину інформаційної безпеки України, введеному в дію Указом Президента України від 25 лютого 2017 року № 47/2017[3]. Так,

відповідно до Розділу 6 («Механізм реалізації Доктрини»), на Міністерство інформаційної політики України, окрім іншого, мають бути покладені в установленому порядку організація та забезпечення координації діяльності центральних та місцевих органів виконавчої влади у сфері забезпечення інформаційного суверенітету України. В цьому ж розділі вказано, що для сприяння координації діяльності органів виконавчої влади у сфері забезпечення інформаційного суверенітету України та взаємодії з іншими державними органами в інформаційній сфері у Міністерстві інформаційної політики України може утворюватися в установленому порядку допоміжний орган.

Отже, якщо розглядати норми, які розкривають поняття інформаційного суверенітету та визначають його окремі аспекти, можемо зробити висновок про відносну невизначеність його змісту та місця в системі національної безпеки України. Разом із тим, відповідно до визначення, наведеного у Законі України «Про Національну програму інформатизації», інформаційний суверенітет є елементом національної безпеки України. Тому погодимось із О.М. Степко, який зазначив, що захист інформаційного суверенітету держави тісно пов'язаний із поняттям інформаційної безпеки, що може бути розглянута, як захищеність внутрішньої інформації як такої, тобто захищеність якості інформації, її надійність, захищеність різних галузей інформації від розголошення, а також захищеність інформаційних ресурсів. З іншого боку, інформаційна безпека означає контроль над інформаційними потоками, обмеження використання провокаційної, ворожої суспільної інформації, включаючи контроль над рекламою; захист національного інформаційного простору від зовнішньої інформаційної експансії [4, с. 83].

На думку О. Олійника, О. Сосніна, Л. Шиманського, інформаційний суверенітет Української держави – це виключне право України відповідно до Конституції, законодавства України та норм міжнародного права самостійно і незалежно з додержанням балансу інтересів особи, суспільства і держави визначати й здійснювати внутрішні та геополітичні національні інтереси в інформаційній сфері, державну внутрішню і зовнішню інформаційну політику, розпоряджатися власними інформаційними ресурсами, формувати інфраструктуру національного інформаційного простору, створювати умови для його інтегрування у світовий інформаційний простір та гарантувати інформаційну безпеку держави [5].

Головна мета забезпечення інформаційної безпеки має визначатися на основі широкого розуміння цього поняття як важливої складової національної безпеки та системоутворюючого фактору усіх сфер життєдіяльності особи, суспільства, держави, політичної, економічної, соціокультурної, науково-технологічної, оборонної, екологічної, власне інформаційної тощо складових національної безпеки [6, с. 75].

Одночасно зауважимо, що невід'ємним елементом інформаційної безпеки є кібербезпека, яка у Законі України «Про основні засади забезпечення кібербезпеки України» визначається як «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» [7].

Відповідно до ст. 19 Закону України «Про національну безпеку України», СБ України є державним органом спеціального призначення з правоохоронними функціями, що забезпечує державну безпеку, здійснюючи з неухильним дотриманням прав і свобод людини і громадянина, окрім іншого, контррозвідувальний захист державного суверенітету, конституційного ладу і територіальної цілісності, оборонного і науково-технічного потенціалу, кібербезпеки, економічної та інформаційної безпеки держави, об'єктів критичної інфраструктури. Згідно ж ст. 10 Закону «Про Службу безпеки України», до складу Центрального управління СБУ входить підрозділ контррозвідувального захисту інтересів держави у сфері інформаційної безпеки [8].

У Розділі 6 Доктрини інформаційної безпеки України передбачено, що Служба безпеки України у межах компетенції має здійснювати:

– моніторинг спеціальними методами і способами вітчизняних та іноземних засобів масової інформації та мережі Інтернет з метою виявлення загроз національній безпеці України в інформаційній сфері;

– протидію проведенню проти України спеціальних інформаційних операцій, спрямованих на підрив конституційного ладу, порушення суверенітету і територіальної цілісності України, загострення суспільно-політичної та соціально-економічної ситуацій.

Ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України» покладає на СБ України наступні завдання:

– запобігання, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі;

– здійснення контррозвідувальних та оперативно-розшукових заходів, спрямованих на боротьбу з кібертероризмом та кібершпигунством, негласна перевірка готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів;

– протидія кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави;

– розслідування кіберінцидентів та кібератак щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури;

– забезпечення реагування на кіберінциденти у сфері державної безпеки.

Оминаючи наукову дискусію щодо змісту та ознак інформаційного суверенітету та інформаційної безпеки України, підкреслимо, що виконання покладених Доктриною інформаційної безпеки України та Законом України «Про основні засади забезпечення кібербезпеки України» на СБ України завдань є цілком необхідним в контексті забезпечення національної безпеки України та потребує більш детального наукового аналізу з метою створення ефективного механізму протидії загрозам інформаційному суверенітету України.

**Література**

1. Закон України «Про Національну програму інформатизації» / [Електронний ресурс] // Режим доступу : http://zakon4.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80/ed20121202.

2. Закон України «Про інформацію» / [Електронний ресурс] // Режим доступу:http://zakon2.rada.gov.ua/laws/show/2657-12/ed20110106/page2.

3. Рішення Ради національної безпеки і оборони України від 29 грудня 2016 року Про Доктрину інформаційної безпеки України/ [Електронний ресурс] // Режим доступу:https://www.president.gov.ua/documents/472017-21374.

4. Степко О.М. Аналіз головних складових інформаційної безпеки держави // Науковий вісник Інституту міжнародних відносин НАУ. – Сер. : Економіка, право, політологія, туризм. – К. : Вид-во Нац. авіац. ун-ту “НАУ-друк”, 2011. – Вип. 1(3). – С. 83.

5. Олійник О. В., Соснін О. В., Шиманський Л. Є. Політико-правові аспекти формування інформаційного суспільства суверенної і незалежної держави [Електронний ресурс] / О. В. Олійник, О. В. Соснін, Л. Є. Шиманський. – Режим доступу : http://www. niss. gov. ua/book/Sosnin_2.htm. – С. 2.

6. Олійник О. В.Принципи забезпечення інформаційної безпеки України / О. В. Олійник // Юридичний вісник. Повітряне і космічне право. – 2016. – № 4. – С. 72-78.

7. Закон України «Про основні засади забезпечення кібербезпеки України» / [Електронний ресурс] // Режим доступу : https://zakon.rada.gov.ua/laws/show/2163-19.

8. Закон України «Про Службу безпеки України» / [Електронний ресурс] // Режим доступу : https://zakon.rada.gov.ua/laws/show/2229-12.

*УДК 004.056.5*
**Попович В. В.**
доктор технічних наук, доцент,
Львівський державний університет
безпеки життєдіяльності

# ДОСВІД ПІДГОТОВКИ КУРСАНТІВ ТА СТУДЕНТІВ СПЕЦІАЛЬНОСТІ «КІБЕРБЕЗПЕКА» В ЛЬВІВСЬКОМУ ДЕРЖАВНОМУ УНІВЕРСИТЕТІ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ

Львівський державний університет безпеки життєдіяльності (ЛДУБЖД) – провідна навчально-наукова установа зі специфічними умовами навчання, яка здійснює підготовку фахівців за різними спеціальностями, здебільшого у галузі безпеки людини. ЛДУБЖД входить до Асоціації вищих навчальних закладів Європейського Союзу, які працюють у галузі безпеки людини (EFSCA). Підготовку фахівців за першим бакалаврським рівнем вищої освіти денної та заочної форми навчання (4 роки) та другим рівнем вищої освіти "магістр" денної форми навчання (1,5 роки) за спеціальністю 125 "Кібербезпека" в ЛДУБЖД здійснює Кафедра управління інформаційною безпекою, яка є структурним підрозділом Навчально-наукового інституту цивільного захисту.

Кафедру управління інформаційною безпекою ЛДУБЖД створено у січні 2011 року внаслідок реорганізації кафедри інформаційних технологій та телекомунікаційних систем (ІТТС), яка була розділена на дві кафедри – інформаційної безпеки та управління проектами, інформаційних технологій та телекомунікацій. Кафедрі виділено приміщення в навчальному корпусі Університету та закріплено відповідні лабораторії. Вона забезпечує навчальну, виховну й методичну роботу серед курсантів і студентів ЛДУБЖД [1].

Курсанти і студенти спеціальності "Кібербезпека" здобувають необхідні знання та навики з управління безпекою інформаційних систем, організацій та підприємств, володіють теорією та практикою розроблення і адміністрування інформаційних систем, а також програмно-технічних засобів захисту інформації. Сферою їхньої діяльності є сучасні системи управління, охорони і спостереження, які використовуються у структурних підрозділах ДСНС України та багатьох інших відомствах [1].

Освітня програма спеціальності "Кібербезпека" розроблена спільно з фахівцями провідних ІТ-компаній Львова. Більшість предметів в навчальній програмі – це цілком нові дисципліни, зорієнтовані на потреби ринку, перш за все, ІТ-галузі. В програмі докорінно змінено набір дисциплін, що стало можливим завдяки тісній співпраці кафедри з провідними фахівцями фірм Softserve і Eleks в галузі Кібербезпеки. Викладачі кафедри регулярно проходять стажування у вище згаданих ІТ-компаніях [1].

Відмінною особливістю курсантів та студентів ЛДУБЖД спеціальності “Кібербезпека” є те, що під час навчання вони проходять стажування на таких базах практик: органи та підрозділи ДСНС України; відділи інформаційної та корпоративної безпеки компаній SoftServe, Eleks, Epam; різноманітні ІТ-компанії, які займаються наданням послуг у сфері інформаційної безпеки; відділи інформаційної безпеки банківських установ; органи та підрозділи державної фіскальної служби. В результаті навчання на спеціальності “Кібербезпека” випускники володіють знаннями, щодо: законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; принципів супроводу систем та комплексів інформаційної та/або кібербезпеки; теорії, моделей та принципів управління доступом до інформаційних ресурсів; теорії систем управління інформаційною та/або кібербезпекою; методів та засобів виявлення, управління та ідентифікації ризиків; методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; методів та засобів технічного та криптографічного захисту інформації; сучасних інформаційно-комунікаційних технологій; сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; автоматизованих систем проектування [2].

Випускники спеціальності після закінчення навчання на спеціальності Кібербезпека можуть працювати на таких посадах:

В підрозділах ДСНС України, ІТ-компаніях та інших установах:

- фахівець сектору технічного захисту інформації та радіотехнічного контролю;
- провідний фахівець центру оперативного зв’язку, телекомунікаційних систем та інформаційних технологій.
- спеціаліст відділу кіберзлочинності;
- спеціаліст відділу криптографічного захисту;
- спеціаліст відділу розслідувань та контролю ризиків;
- аналітик інформаційної безпеки;
- менеджер інформаційної безпеки;
- фахівець devsecops;
- розробник спеціалізованого програмного забезпечення у галузі інформаційної безпеки;
- інженер-програміст;
- системний адміністратор;
- аналітик з комп’ютерних комунікацій, систем і комп’ютерного банку даних.

Слід зазначити, що випускники можуть працювати у структурних підрозділах захисту інформації Міністерства внутрішніх справ України, Служби безпеки України, Державної служби спеціального зв’язку та захисту інформації, банківських установах, управліннях залізниці та митниці.

**Література**

1. Офіційний веб-сайт Львівського державного університету безпеки життєдіяльності. [Електронний ресурс] – Режим доступу з https://ldubgd.edu.ua/institut-department/kafedra-upravlinnya-informaciynoyu-bezpekoyu.

2. Стандарт вищої освіти спеціальності 125 Кібербезпека для першого бакалаврського рівня вищої освіти [Електронний ресурс] – Режим доступу з https://osvita.ua/consultations/spec-bach/63103/.

У*ДК 355.40:356.35*

**Порохня І. М.**
Національний університету оборони України
імені Івана Черняховського

## ОСОБЛИВОСТІ ВИЯВЛЕННЯ ІНФОРМАЦІЙНИХ ЗАГРОЗ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Дії російсько-терористичних військ у зоні проведення операції об’єднаних сил суттєво підвищують вимоги до розвідки. Важливим напрямком розвідувальної діяльності в інтересах органів військового управління й надалі залишається постійний та цілеспрямований моніторинг відкритих джерел інформації, у тому числі й інформаційних ресурсів мережі інтернет на предмет виявлення в їх контенті ознак інформаційних операцій проти України. Одержувані у результаті такого моніторингу оцінки рівня загроз інформаційній безпеці держави у воєнній сфері суттєво доповнюють загальну оцінку рівня загрози національній безпеці України [1, с. 21].

Застосування Російською Федерацією технологій гібридної війни проти України перетворило інформаційну сферу на ключову арену протиборства. Проти України застосовуються різноманітні інформаційні технології впливу на свідомість громадян, спрямовані на розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України.

Боротьба за перевагу у світовому інформаційному просторі провокує різке зростання реальних та потенційних загроз інформаційній безпеці України. Для ефективного формування системи захисту та протидії негативному інформаційному впливу існує необхідність розглядати загрози національній безпеці нашої держави в інформаційній сфері комплексно за всіма сферами. Загрози проявляються у зовнішньополітичній та внутрішньополітичній сферах, у сфері державної безпеки, науково-технологічній, економічній, соціальній та гуманітарній сферах [2, с. 30].

Водночас за сучасних умов найбільшу небезпеку становлять загрози у воєнній сфері, і саме проблема інформаційної безпеки воєнній організації держави у контексті жорсткого інформаційного протистояння під час проведення антитерористичної операції викликає найбільшого занепокоєння і потребує найбільшого зосередження органів державної влади та спеціальних служб [3, с. 18].

В умовах гібридної агресії Росії проти України державна інформаційна політика передусім зосереджується на реалізації системи заходів щодо протидії руйнівному інформаційному впливу Кремля, насамперед:

запобігання інформаційним загрозам (викликам, впливам) шляхом здійснення превентивних заходів із забезпечення інформаційної безпеки держави;

виявлення інформаційних загроз та деструктивних впливів, яке полягає у систематичному моніторингу, аналізі й прогнозуванні появи реальних або потенційних інформаційних загроз;

ліквідацію наслідків негативних інформаційних впливів.

Важливим етапом при реалізації заходів пов'язаних з виявленням деструктивних впливів, є процедура моніторингу та оцінювання загроз інформаційній безпеці України в цілому та у воєнній сфері зокрема. При цьому у воєнній сфері така процедура має свої та властиві лише їй специфічні особливості, які передбачають:

по-перше, виявлення негативного зовнішнього впливу на особовий склад Збройних Сил нашої держави, його аналіз за якісними і кількісними показниками, визначення форм та способів інформаційної боротьби;

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.

Наявні факти наочно доводять ефективність інформаційної зброї на сучасному етапі розвитку військового мистецтва. Інформаційні загрози сьогодні стали настільки 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.

Основна небезпека від проявів інформаційних загроз у воєнній сфері полягає в тому, що на перший план все більше висуваються технології інформаційно-психологічного впливу, які дозволяють перетворити державу-опонента в регіон керованої кризи. Такі технології представлені різноманітними засобами маніпулювання індивідуальною та суспільною свідомістю. Зокрема вони призводять до етнічного сепаратизму і внутрішньої ре-

гіоналізації, нав'язування чужої мови і культури тощо. У поєднанні з політико-дипломатичним тиском, що спирається на економічну та військову силу, такі технології стають більш ефективними, ніж застосування сучасних засобів збройної боротьби.

Отже, досвід АТО показав, що сьогодні перед органами військового управління, відповідальними за інформаційну безпеку держави у воєнній сфері, стоїть ряд важливих та складних завдань, одним з яких є визначення джерел воєнної небезпеки, встановлення характеру та ступеня воєнних загроз державі, а також факторів, що можуть вплинути на хід та результати збройного конфлікту.

**Література**

1. Світова гібридна війна: український фронт: монографія / за заг. ред. В.П. Горбуліна. – К.: НІСД, 2017.

2. Стан та проблеми забезпечення державної інформаційної політики: зона АТО та окуповані території: аналітична доповідь / за заг. ред Д. Дубова. – К.: НІСД, 2016;

3. Уразливість інформаційної політики Євросоюзу щодо впливу російської пропаганди. Аналітична доповідь. – К.: НІСД, 2017. – 17 с.

*УДК 316.625 (075.8) (043.2)*

**Присяжнюк М. М.**
кандидат технічних наук,
старший науковий співробітник,
Національна академія СБ України

## СУГЕСТІЯ В КІБЕРПРОСТОРІ

Науково-технічна революція початку XXI ст. спричинила в усьому світі глибокі системні перетворення. Поєднання досягнень у сфері новітніх інформаційних технологій та стрімкого розвитку інформаційно-телекомунікаційних систем викликало появу так званого віртуального простору, який ще отримав назву «кіберпростір».

Відкритий кіберпростір розширює свободу і можливості людей, збагачує суспільство, створює новий глобальний інтерактивний ринок ідей, досліджень та інновацій, забезпечує публічність та прозорість влади, сприяє запобіганню корупції. Проте, разом з перевагами використання кіберпростору принесло чималу кількість загроз, серед яких – сугестивний маніпулятивний вплив.

Під сугестією розуміють передачу інформації за допомогою частково неусвідомлюваного, направленого сигналу на вербальному чи невербаль-

ному рівні при міжособистісній або міжгруповій комунікації [1]. Сугестія відрізняється від переконання зниженим рівнем критичності та потреби у верифікації інформації.

Таке явище, як сугестія, існує з древніх часів. Але з розвитком людства відбувалася й еволюція цього явища – від звичайних колдунів, шаманів і відьом до новітніх ефективних методів і способів прихованого маніпулятивного впливу на людську свідомість.

Для обґрунтування сугестивного маніпулятивного впливу на свідомість окремого користувача кіберпростору найбільше підходить психологічна доктрина, в основі якої лежать праці психофізіолога В. Бехтєрєва. Він пов'язує цей процес впливу із насильницьким навіюванням – вторгненням у свідомість або прищепленням до неї сторонньої ідеї, яке відбувається без участі волі й уваги сприймаючої особи і нерідко навіть без ясного з її сторони усвідомлення цього процесу [2].

Стрімкий розвиток новітніх інформаційних технологій призвів до створення глобального інформаційного суспільства з широкими інформаційно-комунікаційними можливостями, яке послужило благодатною ареною для впровадження сучасних методів сугестії.

Створення глобальної мережі Інтернет надало людям не лише можливості вільного обміну інформацією та спілкування в реальному масштабі часу, але й призвело до використання Інтернет-простору для здійснення сугестивних впливів на обраний об'єкт з метою маніпулювання індивідуальною й суспільною свідомістю.

В сучасних умовах зовнішньої інформаційної експансії та агресії з використанням сучасних методів маніпулятивного впливу актуальним постає дослідження феномену «сугестія» у вимірах лінгвістики, психології та суміжних наук (нейролінгвістики, психолінгвістики, соціальної психології тощо).

З точки зору сугестивної лінгвістики до найбільш популярних технік сугестії належать такі: конкретність та образність ключових слів, емоційне перенасичення тексту; використання риторичних запитань невизначених і наказових конструкцій; звертання до базового для того чи іншого співтовариства концепту та наповнення його новим змістом; експлуатація ідеї – «кола своїх»; включення в дискурс мовних конструкцій спільності й довіри тощо [3].

Для здійснення сугестивного маніпулятивного впливу на світову спільноту у кіберпросторі використовуються новітні інформаційні технології, серед яких: медіавіруси, блоги, симулякри, фейки, оверквотинг, флейми, тролінг, флуд, спам, офтоп, кроспостинг, комп'ютерні ігри, холівари тощо.

Варто зазначити, що ефективності реалізації сугестивного маніпулятивного впливу в глобальному інформаційно-комунікаційному середови-

щі сприяють: безперешкодний доступ до інформації та обмін нею; відсутність територіальних обмежень та цензури. Також підвищує ефективність сугестії в кіберпросторі висока довіра до мережевої інформації, одночасне охоплення широкої аудиторії, схильність людей до емпатії.

З огляду на вищезазначене та враховуючи стан інформаційної агресії проти України з боку Російської Федерації, з метою протидії кіберагресору, в нашій державі конче необхідно:

1) створити ефективну систему забезпечення інформаційної та кібернетичної безпеки держави, що потребує у першу чергу привести у відповідність до світових стандартів нормативно-правову базу, яка б враховувала як національні, так і міжнародні принципи регулювання інформаційних відносин;

2) вдосконалити систему підготовки фахівців з кібернетичної безпеки в навчальних закладах України з метою подальшого кадрового забезпечення відповідних структур.

**Література**

1. Сугестивні технології маніпулятивного впливу: навч. посіб. / В.М. Петрик, М.М. Присяжнюк, Л.Ф. Компанцева / за заг. ред. Є.Д. Скулиша. – К.: ВІПОЛ, 2011. – 248 с.

2. Неклесса А. Глобализация: новый цивилизационный контекст / А.Неклесса. – [Електронний ресурс]. – Режим доступу: www.futurerussia.ru/conf/ forum_ infosociety_neklessa.html.

3. Принципи сугестивної лінгвістики в інтернетній комунікації. / Л. Ф. Компанцева // Наукові записки [Ніжинського державного університету ім. М. Гоголя]. Серія: Філологічні науки. – 2013. – Кн. 3. – С.13-20. – Режим доступу: http://nbuv. gov. ua/j-pdf/Nzfn_2013_3_4. pdf.

*УДК 340.5; 351*

**Прощаєв В. В.**
кандидат юридичних наук, доцент

## КОНСТИТУЦІЙНО-ПРАВОВЕ РЕГУЛЮВАННЯ ДІЯЛЬНОСТІ РОЗВІДУВАЛЬНИХ ОРГАНІВ У КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Одним із основних показників демократичного розвитку держави є конституційно-правове регулювання організації та діяльності її розвідувальних органів як органів державної влади. Визначення у вітчизняному законодавстві [1, ст. 1; 2, преамбула] розвідувальних органів як державних органів яскраво свідчить про те, що їх діяльність відноситься до різновиду державної діяльності, що вони функціонують у рамках визначених зако-

нодавством повноважень, що демократичний контроль, у тому числі й з боку громадськості, також є притаманним для розвідки: «загалом державні органи як провідники державної влади створюються з метою вирішення життєво важливих проблем та функціонують у рамках визначених законодавством повноважень, що у кінцевому результаті впливає на реалізацію основних прав і свобод людини у правовій державі» [3, с. 28].

З прийняттям у 2015-2016 роках низки Указів Президента України в сфері забезпечення національної безпеки почався черговий етап в конституційно-правовому регулюванні діяльності розвідувальних органів.

У новій редакції Воєнної доктрини України зазначається, що необхідно посилити розвідувальну діяльність в інтересах підготовки та проведення Україною стратегічних комунікацій, контрпропагандистських заходів та інформаційно-психологічних операцій [4, п. 32]. Але, робити це можна лише в умовах «удосконалення системи демократичного цивільного контролю над сектором безпеки і оборони держави відповідно до стандартів ЄС та НАТО» [4, п. 17]. Тобто, розвідка, виконуючи нові завдання, має розв'язувати їх в умовах прийняття також нових правових приписів стосовно удосконалення системи демократичного цивільного контролю за її діяльністю відповідно до стандартів ЄС та НАТО. Це означає, що вітчизняний законодавець має уявити ці стандарті, на підставі яких прийняти нові або внести редакційні зміни у чинні законодавчі акти.

В Концепції розвитку сектору безпеки і оборони України [5] зазначено, що основною метою розвитку розвідувальних органів є посилення розвідувальних спроможностей України на основі їх узгодженого чіткого функціонування, координації їх діяльності та зміцнення взаємодії з партнерськими спецслужбами держав – членів НАТО, що утворено Об'єднаний комітет з питань розвідувальної діяльності при Президентові України [6], який координуватиме діяльність розвідувального співтовариства, що подальший розвиток розвідувальних органів здійснюватиметься шляхом реалізації заходів, передбачених національною розвідувальною програмою, і спрямовуватиметься на зосередження зусиль розвідувальних органів та Об'єднаного комітету на: пріоритетних напрямах забезпечення національної безпеки; усунення децентралізації, дублювання функцій і завдань; посилення взаємодії та координації діяльності; комплексне використання можливостей для вирішення пріоритетних завдань; поєднання окремих передових ресурсів і технологій у рамках розвідувального співтовариства; залучення до сфери розвідувальної діяльності споживачів розвідувальної інформації та інших суб'єктів сектору національної безпеки і оборони; удосконалення системи бюджетного фінансування розвідувальних органів України; зміцнення взаємодії розвідувальних органів з партнерськими спецслужбами, передусім держав – членів НАТО, побудова відносин взаємної довіри; запровадження сучасних механізмів демократичного цивільного контролю за діяльністю розвідувальних органів України.

Як бачимо, в цьому підзаконному акті також визначені нові пріоритети подальшого конституційно-правового регулювання діяльності розвідувальних органів. Більш того, прямо зазначено, що основними шляхами досягнення необхідних оперативних та інших спроможностей складових сектору безпеки і оборони є удосконалення законодавчої бази з питань функціонування та розвитку сектору безпеки і оборони з урахуванням відповідних принципів і стандартів ЄС і НАТО [5, п. 2].

У Стратегії кібербезпеки України [7, п. 3] на розвідувальні органи покладено здійснення розвідувальної діяльності щодо загроз національній безпеці у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки, що передбачає, насамперед, комплексне вдосконалення правової основи кіберзахисту об'єктів критичної інфраструктури, визначення критеріїв віднесення інформаційних (автоматизованих), телекомунікаційних, інформаційно-телекомунікаційних систем до критичної інформаційної інфраструктури.

У підґрунті подальшого конституційно-правового регулювання діяльності розвідувальних органів є достатня та необхідна кількість вітчизняних підзаконних актів, які конкретно спрямовують законотворців у сфері зовнішньої розвідки на якісне формулювання необхідних правових приписів.

**Література**

1. Про Службу зовнішньої розвідки України: Закон України від 1 грудня 2005 р., № 3160-IV. URL: https://zakon.rada.gov.ua/laws/show/3160-15/ed20150715.

2. Про розвідувальні органи України: Закон України від 22 березня 2001 р., № 2331-III. URL: https://zakon.rada.gov.ua/laws/show/2331-14.

3. Глущенко С. В. До питання про конституційно-правовий статус державного органу. *Адвокат № 6 (141),* Наука і практика. 2012. С. 28 – 33.

4. Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 р. «Про нову редакцію Воєнної доктрини України»: Указ Президента України від 24 вересня 2015 р. № 555/2015. URL: http://zakon2.rada.gov.ua/laws/show/555/2015/page.

5. Про рішення Ради національної безпеки і оборони України від 4 березня 2016 р. «Про Концепцію розвитку сектору безпеки і оборони України»: Указ Президента України від 14 березня 2016 р. № 92/2016. URL: http://zakon5.rada.gov.ua/laws/show/92/2016.

6. Про вдосконалення системи забезпечення керівництва, координації та контролю за діяльністю розвідувальних органів України: Указ Президента України від 30 січня 2015 р. № 42/2015. URL: https://zakon.rada.gov.ua/laws/show/42/2015.

7. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 р. «Про Стратегію кібербезпеки України»: Указ Президента України від 15 березня 2016 р. № 96/2016. URL: http://zakon2.rada.gov.ua/laws/show/96/2016.

*УДК 004.056.53*
**Рахімов В. В.**
Національний університет оборони України
імені Івана Черняховського

# ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ КІБЕРАТАК

Фінансові збитки різних організацій та витоки сотень тисяч облікових записів користувачів різних інтернет ресурсів вже стали нашим сьогоденням про які можна почути як від звичайного пересічного громадянина нашої держави та і від експертів в кібернетичній галузі. Разом з тим, інформація про те, скільки коштувало проведення такої атаки, або про те, наскільки складно було її реалізувати залишається закритою.

Водночас, фахівці з кібербезпеки виділяють, що в своїй більшості кібератаки засновані на використанні куплених і орендованих у третіх осіб розробок і серверів. Отже, мінімальна вартість в доларах США за умови, що всі необхідні засоби та інструменти організатор кібератаки вже має, буде приблизно складати: цільова атака на організацію від 4500$; злом сайту з отриманням повного контролю в межах 150$; злом пошти 40$; DDoS-атака 50$ на добу; викрадення грошей (даних) за допомогою фішингу 270$ [2].

Також, експерти продовжують акцентувати увагу на APT-атаках у всьому світі. Як бачимо APT-кібератака (розвинена стала загроза або постійна загроза підвищеної складності, англ. advanced persistent threat) це різновид складних кібератак для отримання несанкційованого доступу до інформаційних систем жертви та встановлення прихованого доступу до них з метою використання або контролю в майбутньому [1, с. 110]. Визначимо основні властивості APT-кібератаки, а саме:

розвинена атака (англ. advanced) – здатна обійти наявні системи захисту (мережеві екрани, антивіруси, різні фільтри, тощо;

стала (англ. persistent) – здатна залишатись непоміченою для систем виявлення загроз (антивіруси, системи виявлення вторгнень тощо); зловмисник спрямований на досягнення мети, може мати відповідний наказ від замовника;

загроза (англ. threat) – здатна завдати певну шкоду; зловмисник добре організований, має необхідні засоби, мотивацію.

В свою чергу, неможливо не відмітити роль соціальної інженерії в усіх можливих формах її застосування. При цьому соціальна інженерія стає більш технологічною. Як повідомляє американська газета The Wall Street Journal в серпні 2019 році вперше зафіксували атаку за допомогою штучного інтелекту для підробки голосу. Під виглядом гендиректора міжнародної компанії шахраї зателефонували генеральному директору енер-

гетичної компанії з Великобританії і переконали перевести їм 243 тисячі доларів. Технологія є відкритою та в 2020 році варто очікувати масового поширення таких атак [5]. Тому маніпулювання людьми залишає за собою необмежені можливості та дає велику сукупність методів, основаних на психологічних особливостях людей: цікавість, довіра, звичка тощо. Вся система соціальної інженерії базується на тому факті, що саме людина є найслабкішою ланкою будь-якої системи інформаційної чи кібербезпеки.

Водночас, фішинг на сьогоднішній день є одним з найпоширеніших видів соціальної інженерії. По суті це вивідування інформації для доступу до персональних даних довірливих користувачів [3, с. 56]. За підсумками 2019 року були визначенні найпоширеніші шкідливі файлові розширеннями, які були використані в електронних листах doc (41,8%), .zip (26,3%), js (14,0%), pdf (9,9%), rar (3,9%), .exe (1,7%), .docx (0,8%), ace (0,5%), gz (0,5%), xlsx (0,2%) [4].

На сьогодні доречно прислуховуватись до парад фахівців з інформаційної безпеки та звертати особливу увагу на листи, в яких:

попереджають про “відключення вашого профілю” і пропонують авторизуватися, щоб запобігти цьому;

від імені вищого керівництва вимагають зробити який-небудь грошовий переказ;

шантажують користувача записами і протоколами його візитів на порносайти (т.зв. sextortion) – як правило, неіснуючими;

повідомляють про посилку або підписці на послуги, яких людина не набував або не замовляв ( “Вам прийшов вантаж через компанію МММ. Відкрийте PDF-файл, щоб дізнатися подробиці”);

пропонують внести невеликий аванс, щоб отримати велику винагороду (сучасний різновид класичних “нігерійських листів”).

В свою чергу, вводячи логін/пароль в акаунтах на сайтах, звертайте увагу на незвичайні зміни зовнішнього вигляду сторінок. Якщо щось викликає підозру – краще перевірити оригінальність ресурсу ще раз [6].

Таким чином, враховуючи зазначене кібератаки стають більш багатоетапними, які вимагають досконалої підготовки та ведення. Одним із основних підготовчих етапів кібератаки залишається збір інформації. Цей етап включає аналіз веб-ресурсів компаній, інформаційних ресурсів інтернету, соціальних мереж.

**Література**

1. Основи кібербезпеки та кібероборони: підруч. / Ю. Г. Даник, П. П. Воробієнко, В.М. Чернега. – О.: ОНАЗ ім. О.С. Попова, 2018. − 228 с.

2. Рынок преступных киберуслуг https://www.ptsecurity.com/ru-ru/research/analytics/darkweb-2018/.

3. Социальная инженерия и социальные хакеры / М. В. Кузнецов, И. В. Симдянов. – СПб.: БХВ-Петербург, 2007. – 368 с.

4. Cisco. https://talosintelligence.com/.

5. The Wall Street Journal, https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402.

6. Zillya! Антивірус. https://zillya.ua/sotsialna-inzheneriya-abo-manipulyatsi-svidomistyu.

*УДК 34.096*

**Руденко І. В.**
кандидат філологічних наук,
Національно академія СБ України

## ОКРЕМІ ПИТАННЯ УДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОГО ЗАКОНОДАВСТВА

У результаті еволюційного поступу сьогоденне суспільство в Україні має перейти до цифрової епохи, що, безперечно, зумовить швидкі та суттєві зміни в усіх сферах існування та діяльності особистості. Проте чи варто говорити про спрощення, уніфікацію та прозорість інформації в цифровому форматі, залишається питанням. Колізії, неточності, неоднозначності та банальні помилки можуть призвести до абсолютно протилежного ефекту від очікуваного, не кажучи вже про загрозу масової недовіри чи паніки. Тому, аби йти в ногу з часом, наразі виникає необхідність удосконалення законодавства України щодо переходу та переведення інформації в цифровий формат. Таку місію мають взяти на себе, перш за все, Комітет Верховної Ради України з питань цифрової трансформації та Міністерство цифрової трансформації України, створене у вересні 2019 року [2].

Варто зазначити, що в першу чергу має бути чітко окреслений на законодавчому рівні понятєвий апарат, адже розходження в тлумаченні певних термінів обов'язково потягне за собою викривлення правових норм. Певні кроки в цьому напрямку було зроблено ще до утворення профільного міністерства, наприклад, певні поняття розкривають Закон України «Про електронні довірчі послуги» від 05.10.2017 р., Закон України про «Про електронні документи та електронний документообіг» від 11.05.2003 р., Закон України «Про захист персональних даних» від 01.06 2010 р. тощо. Однак залишається численна група термінів і сполучень, якими у процесі правозастосовної діяльності буде дуже складно правильно оперувати. Так, наприклад, термін «електронна демократія», зазначений в пп. 14 п. 4 Положення КМУ «Про Міністерство цифрової трансформації України» від 18.09.2019 р. [1] на законодавчому рівні наразі не визначено.

На нашу думку, Мінцифри має створити цілу низку законодавчих документів, ініціювати значну кількість поправок до законів і кодексів України, і в першу чергу до КУпАП та Закону України «Про адміністративні послуги». Це зумовлено потребою забезпечення взаємодії державних органів та надавачів адміністративних послуг в електронному форматі; формування і ведення Реєстру адміністративних послуг . Вважається, що наявність інформації саме в електронному форматі дозволить спростити порядок надання адміністративних послуг, наведених у Законі України «Про адміністративні послуги».

Іншою актуальною проблемою залишається забезпечення національної безпеки під час та після оцифрування інформації. Зокрема, постає питання, чи доцільно взагалі переводити в цифровий формат певну інформацію у сфері функціонування об'єктів критичної інфраструктури, яке наразі немає чіткої відповіді, оскільки існує велика вірогідність збільшення випадків протиправного використання та знищення зазначеної інформації. Відсутність захищеного обміну ідентифікаційними даними як юридичних так і фізичних осіб, неузгодженість у виборі ідентифікаторів, відсутність підтвердження ідентифікаційних даних, використання в системах реєстрації та контролю доступу до інформаційних систем технологічно несумісних механізмів, недосконаліть системи впізнання становлять суттєву загрозу для переходу на використання інформації в цифровому форматі.

Отже, для вирішення завдань сучасного інформаційного забезпечення громадянського суспільства та системи державного управління наразі існує нагальна необхідність переведення інформації в цифровий формат, але на цьому шляху існує ряд серйозних проблем. Зокрема, першочергового вирішення потребує чітке законодавче визначення відповідного понятєвого апарату, а також правова регламентація забезпечення інформаційної безпеки об'єктів критичної інфраструктури.

**Література**

1. Положення про Міністерство цифрової трансформації України. URL https://zakon.rada.gov.ua/laws/show/856-2019-п (дата звернення – 08.03.2020).

2. Україна «в цифрі»: напрямки реформування. URL https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/ukrayina-v-cifri-napryamki-reformuvannya.html (дата звернення – 08.03.2020).

*УДК 004.056*
**Самойленко О. О.**
Національна академія СБ України

# СЕРЕДОВИЩА ДЛЯ ВІЗУАЛЬНОГО ПРОГРАМУВАННЯ ДЛЯ ПІДГОТОВКИ БАКАЛАВРІВ З КІБЕРБЕЗПЕКИ

Візуалізація – один з найбільш ефективних прийомів навчання, що допомагає набагато простіше і глибше розібратися в сутності різних явищ, недарма наочні посібники використовувалися ще в глибокій старовині. Особливо корисні візуалізація та моделювання при вивченні бакалаврами з кібербезпеки динамічних структур, що змінюються в часі, об'єктів і явищ, які буває складно зрозуміти, дивлячись на просту статичну картинку в звичайному підручнику. В умовах освітньо-цифрового середовища-лабораторні роботи та навчальні експерименти не тільки корисні, але і вельми цікаві при відповідній організації.

Мови візуального програмування для бакалаврів з кібербезпеки в умовах освітньо-цифрового середовища можуть бути додатково класифіковані в залежності від типу і ступеня візуального вираження, на типи:

*Природньо-візуальні мови* мають невід'ємне візуальне вираження, для якого немає очевидного текстового еквіваленту, наприклад, графічна мова G в середовищі LabVIEW.

*Візуально-перетворені мови* є невізуальними мовами з накладеним візуальним представленням (Середовище візуального програмування. Форма. Інспектор об'єктів. Редактор коду. Палітра компонентів).

Значна кількість сучасних мов програмування має розвинуті візуальні засоби для розробки графічного інтерфейсу, причому здійснюється програмування розміщених на спеціальних формах об'єктів з настроюванням їх властивостей та поведінки.CodeGear Delphi і C++ Builder,Microsoft Visual Studiота мови, які включає в себе цей засіб (Visual Basic, Visual C#, Visual J# тощо) часто плутають з візуальними мовами програмування. Всі ці мови є текстовими, а не візуальними (графічними). MS Visual Studio та Delphi євізуальними середовищами програмування, але не візуальними мовами програмування (Ковалевський, 2018).

Візуальні мови програмування, які дозволяють бакалаврам з кібербезпеки розробляти програми за допомогою маніпуляцій з графічними елементами (блоками, стрілками), що використовуються як елементи синтаксису мови, на відміну від написання тексту вихідного коду. На сьогодні виділяють більше 70 візуальних мов програмування, які мають вагоме місце для підготовки бакалаврів з кібербезпеки.

Однією з сфер, де візуальні мови програмування досягли успіху є освіта. Бакалаврам з кібербезпеки такі мови допомагають зрозуміти як створити комп'ютерну програму. Серед таких мов є App Inventor, Blockly,

Hopscotch, Microsoft TouchDevelop, Scratch, Snap, та ін. Ці візуальні мови програмування покликані зробити процес професійної підготовки бакалаврів з кібербезпеки більш доступним, зменшити труднощі, з якими стикаються новачки, коли починають програмувати. У них основні елементи програмування, як правило, представлені у вигляді блоків, з візуальними орієнтирами для використання їх один з одним (Костишина, 2017). Так чином, для створення програми користувач збирає блоки, розташовуючи їх так, щоб вони правильно стикувалися один з одним відповідно до логіки чи алгоритму розроблюваної програми. Завдяки цьому недопустимі вирази може бути просто неможливо зібрати. Крім того, блоки, як правило, представлені у каталозі освітньо-цифрового середовища та розділені за типами, і користувачу не потрібно читати документацію, щоб зрозуміти, які функції доступні у цій мові програмування. Така концепція мови позбавляє проблем, які з'являються при вивченні синтаксису мов програмування, а це дозволяє їм зосередитися на логіці своєї програми, а не на тому, яку синтаксичну конструкцію обрати, як прописати властивості (атрибути), як правильно оформити запис відповідною мовою програмування.

Слід зазначити, що освітньо-цифрове середовище розробки для таких мов часто має спрощене середовище виконання програм, де користувач може швидко і легко запускати свою програму і бачити результати. У деяких візуальних мовах програмування такого типу код може інтерпретуватися на різні текстові мови програмування, наприклад, як у Blockly код інтерпретується на такі мови як JavaScript, Python, PHP, Lua, Dart та XML.

Використовувані у таких мовах форми, кольори, відступи дозволяють бакалаврам з кібербезпеки швидко отримати уявлення про те, що програма робить, тобто розроблювана програма є зручною для читання та рефакторингу (Гласс, 2009). Адже структура блоків дозволяє легко змінити графічний код, на відміну від рефакторингу тексту на основі текстової мови.

Інший тип візуальних мови програмування подібний до попереднього, але замість блоків використовуються графічні елементи, що використовуються у блок-схемах. До таких мов відносяться Bonita BPM, Discovery Machine, Flowgorithm, Flowhub, Grafcet, Raptor, WebML, Widget Workshop та ін.. Програми являють собою спрямовану послідовність виконання дій між блоками, де також використовується розгалуження з умовою, щоб вибрати, який блок виконується далі. Такий акцент на простій візуальній граматиці дозволяє швидко зрозуміти синтаксис мови, проте логічні конструкції, що створюються безпосередньо за допомогою візуальної мови програмування, є обмеженими. Також багато що залежить у програмі від того, що знаходиться всередині блоків. Останнє може бути змінено за допомогою графічного інтерфейсу.

Так, середовища для візуального програмування допомагають у підготовці бакалаврів з кібербезпеки за рахунок логічного мислення, аналітичних потреб, професійної інтеграції та диференціації.

**Література**

1. Гласс, Р. (2009). *Креативное программирование 2.0.: Пер. с англ.* СПб.: Символ-Плюс.

2. Ковалевський, В. М. (2018). Технології розробки програмного забезпечення. Практикум по використанню компоненти MainMenu і обробки подій мишки в C++ Builder при візуальному програмуванні прикладної програми до мнемосхеми технологічного процесу з хімічного виробництва : навчальний пос. Київ. Отримано 24. 04. 2020 р. з https://ela.kpi.ua/handle/123456789/23506.

3. Костишина І. Генеративний дизайн: на перетині мистецтва й програмування. Отримано 24. 04. 2020 р. з https://telegraf.design/generativnij-dizajn-na-peretini-mistetstva-j-programuvannya/.

4. Середовище візуального програмування. Форма. Інспектор об’єктів. Редактор коду. Палітра компонентів. (без дати). 2016. Отримано 24. 04. 2020 р. з https://studfile.net/preview/7013685/page:2/.

*УДК 355.40: 356.35*

**Саричев Ю. О.**
кандидат технічних наук,
старший науковий співробітник
**Гріненко О. І.**
кандидат військових наук, доцент
**Хоменко Л. В.**
Національний університет оборони України
імені Івана Черняховського

## ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИЙ ВПЛИВ ЯК ВИД ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ СИСТЕМИ ДЕРЖАВНОГО УПРАВЛІННЯ У ВОЄННІЙ СФЕРІ

За законами кібернетики будь-яка функція управління реалізується виключно інформаційним шляхом, а тому очевидно, що процес державного управління, зокрема у воєнній сфері, потребує реалізації низки інформаційних процесів, що справляють вплив на усі елементи в системі державного управління у воєнній сфері. Сукупність цих інформаційних процесів власне і об’єднується поняттям інформаційного забезпечення, яке пронизує весь замкнений контур державного управління, а його сутність полягає, з однієї сторони, у необхідності формування ідеї, мети і завдань державного управління та їх донесення від органу державного (військового) управління до елементів системи шляхом реалізації комплексу організуючих інформаційних процесів, а з іншої – в можливості отримання ор-

ганом державного управління зворотної інформації для контролю процесу управління та його корегування.

Аналіз показує, що реалізація усього процесу державного управління за кібернетичною схемою потребує саме комплексного підходу до виконання різнорідних функцій інформаційного забезпечення на усіх рівнях та етапах державного управління у воєнній сфері. Це дозволяє зробити акцент на необхідності розгляду усіх складових інформаційного забезпечення, зокрема тієї складової, що пов'язана з інформаційно-психологічним впливом як різновидом інформаційного впливу в системі державного управління у воєнній сфері. Якість такого впливу на усіх рівнях системи суттєво впливає на її загальну ефективність функціонування. Зважаючи на те, що розглядається система соціального управління, увага зосереджується на інформаційно-психологічному впливі як різновиді інформаційного впливу з урахуванням специфіки та особливостей управління у воєнній сфері. Сьогодні теоретичний аспект цього питання розкритий недостатньо, що породжує проблему, яка пов'язана як з теоретичною недосконалістю цього питання, так і з його практичною реалізацією.

Незважаючи на значну кількість публікацій, що стосуються теми державного управління, питання його інформаційного забезпечення, зокрема, у воєнній сфері, в теоретичному плані в Україні досі не опрацьоване. Останнім часом ця тема висвітлюється в роботах за участі авторів, де значна увага приділяється саме питанням інформаційного забезпечення системи державного управління, в тому числі й у воєнній сфері. У цих роботах визначено, що інформаційний вплив є одним із видів інформаційного забезпечення системи державного управління з його різновидом – інформаційно-психологічним впливом. Такий різновид інформаційного впливу безпосередньо пов'язаний з людиною – носієм інформації, тому він є невід'ємною складовою загального процесу інформаційного забезпечення системи державного управління, зокрема у воєнній сфері.

Відповідно до чинних нормативних документів, *інформаційно-психологічний вплив – цілеспрямоване інформаційне втручання у свідомість (підсвідомість) цільової аудиторії з метою корекції її поведінки та (або) світогляду, зміни морально-психологічного стану*. Засобами інформаційно-психологічного впливу є ЗМІ, спеціальна друкована продукція, публічна голосова агітація, агентурна діяльність, спеціальні інформаційні технології тощо.

Загалом, інформаційно-психологічний вплив, який може бути як позитивним, так і негативним, здійснюється у формі кампаній, операцій, акцій, атак та окремих актів, що можуть реалізовуватися як самостійні заходи (дії), так і складовими більш масштабних форм дій: інформаційних кампаній, операцій або акцій. Слід зауважити, що за напрямом інформаційно-психологічний вплив поділяють таким чином:

*внутрішнього спрямування* – метою є зміцнення морально-психологічного стану своїх військ, населення, а також захист їх від негативного інформаційно-психологічного впливу противника та нейтралізація наслідків такого впливу;

*зовнішнього спрямування* – метою є поширення у противника (уряду країни чи блоку країн, населення, військового командування та особового складу військових частин) сумнівів у правоті його власних дій, дезінформування, деморалізація та дезорганізація його (противника) діяльності, а також створення позитивного іміджу про свою державу в зовнішньому (міжнародному) інформаційному просторі.

Як в мирний час, так і в особливий період (воєнний час) метою здійснення негативного інформаційно-психологічного впливу з боку кожної із протидіючих сторін на особовий склад військ (сил) є погіршення морально-психологічного стану особового складу військ (сил) противника, що є умовою зниження їх психологічної готовності до діяльності або відмови її здійснювати.

Загалом, негативний інформаційно-психологічний вплив з боку противника несе загрозу функціонуванню системи державного управління у воєнній сфері, особливо у частині її інформаційного забезпечення через вплив (тиск) на певну цільову аудиторію. Зазначений процес більш характерний для особливого періоду, коли інформаційно-психологічний вплив противника є реальним явищем. Для періоду мирного часу необхідно проводити упереджувальні заходи протидії на основі моніторингу інформаційного простору воєнної сфери, коли явища впливу ще немає, але є ситуація можливого виявлення викликів і загроз щодо зовнішнього інформаційно-психологічного впливу на особовий склад військ (сил) та органи військового управління. Такі упереджувальні заходи протидії є захистом від негативного інформаційно-психологічного впливу, коли зусилля спрямовані на власну аудиторію.

*УДК 355.40*

**Саричев Ю. О.**
кандидат технічних наук,
старший науковий співробітник
**Сокуренко В. В.**
**Зубков В. П.**
Національний університет оборони України
імені Івана Черняховського

## НАВІГАЦІЙНА СКЛАДОВА ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ СИСТЕМИ ДЕРЖАВНОГО УПРАВЛІННЯ У ВОЄННІЙ СФЕРІ

Будь-яка функція державного управління, зокрема у воєнній сфері, реалізується виключно інформаційним шляхом, а тому очевидно, що інформаційне

забезпечення необхідно розглядати як складову системи державного військового управління, яка у сукупності з іншими складовими повинна забезпечити збалансоване та ефективне функціонування цієї системи. При цьому сутність інформаційного забезпечення в державному військовому управлінні полягає, з одного боку, у необхідності донесення сформованої ідеї та мети від органу управління (командування) до об'єкту управління (військ (сил)) шляхом певного інформаційного впливу, а з іншого – в можливості отримання зворотньої інформації для контролю та корегування організуючого впливу, тобто інформаційне забезпечення має складну структуру.

Оскільки ведення бойових дій здійснюється на великій території, має комплексний характер і впливає на особливості застосування військ (сил) і озброєння та військової техніки, розгортається у просторі і часі, то неможливо проігнорувати такий вид інформаційного забезпечення як *навігаційне*. Аналіз ведення бойових дій у війнах, конфліктах переконливо свідчить, що навігаційне забезпечення є одним з найважливіших, без якого фактично неможливо здійснювати будь-які дії. На сьогодні у збройних силах провідних країн світу навігаційне забезпечення розглядається як необхідний і важливий вид забезпечення військ, який має на меті забезпечення військ геопросторовими даними з прив'язкою до місцевості, які необхідні для планування і ведення бойових дій військами (силами). Сучасний досвід ведення бойових дій на Сході України показав, що ефективність застосування систем управління військами та зброєю знаходиться в прямій залежності від інформаційного забезпечення, і зокрема від повноти і достовірності забезпечення військ (сил) вихідними геопросторовими даними про місцевість, яка використовується військами (силами). Основні вимоги, які при цьому висуваються до навігаційної інформації – достовірність, точність та оперативність.

Як складова (вид) інформаційного забезпечення навігаційне забезпечення має надавати можливість:

вивчення та оцінки місцевості, орієнтування на ній з визначеною точністю;

виконання вимірювань, розрахунків;

побудови розрахункових моделей ситуацій і процесів, які відбуваються на місцевості.

Досвід розвинутих країн світу свідчить про те, що як сьогодні, так і в найближчій перспективі альтернативи щодо точності і надійності координатно-часового забезпечення на основі інформації супутникових навігаційних систем немає. Основними відмітними рисами навігаційного забезпечення на базі супутникових систем є: глобальність, безперервний доступ, скритність роботи, автономність, простота застосування, здатність функціонувати в будь-який час доби, будь-яких кліматичних і метеорологічних умовах.

Проведений аналіз свідчить, що сучасні принципи організації навігаційного забезпечення у ЗС України впроваджуються недостатньо ефекти-

вно, і подальше підвищення бойових можливостей військ неможливе без пошуку нових шляхів інформаційного забезпечення (перш за все, забезпечення геопросторовими даними) військ (сил). Сучасні вимоги до навігаційного забезпечення ЗС України обумовлені необхідністю:

створення, підтримки та удосконалення заданих параметрів локального навігаційного поля для використання ЗС України;

повного оснащення сил та засобів ЗС України засобами навігації;

виконання великих обсягів картографічних робіт при оновленні топографічних карт, що уповільнює процес їх актуалізації;

розвитку інформаційних технологій у сфері топографо-геодезичного та картографічного виробництва, впровадження цифрових методів створення та оновлення картографічних даних;

належного навігаційного забезпечення та забезпечення геопросторовими базами даних ЗС України, створеними у відповідних форматах на єдиній топографічній основі та за єдиними підходами.

Цілком очевидно, що ЗС України потрібна ефективна система навігаційного забезпечення, яка зможе забезпечити виконання завдань як під час повсякденної діяльності, так і під час бойового застосування. Навігаційне забезпечення ЗС України повинно бути єдиним, міжвидовим, багатофункціональним, комплексним, споживачами якого є органи управління, військові частини, підрозділи усіх видів ЗС України, родів військ (сил). Все це ставить вимоги оперативно, безперервно, надійно та необхідною точністю забезпечувати ЗС України навігаційною інформацією для виконання завдань за призначенням незалежно від часу доби, метеоумов, напрямку дій.

На підставі вищевикладеного для воєнної сфери пропонується наступні визначення: *навігаційне забезпечення – комплекс заходів, які організовуються і здійснюються з метою постійного та об'єктивного отримання в масштабі реального часу військовими об'єктами інформації про власне місцезнаходження для ефективного ведення операцій (бойових дій) і застосування озброєння та військової техніки, а також точного і безпечного переміщення наземних, повітряних, надводних та підводних об'єктів військового призначення*.

Запропоноване визначення навігаційного забезпечення як виду інформаційного забезпечення в системі державного управління у воєнній сфері реалізує специфічні інформаційні функції забезпечення ефективної діяльності органів військового управління, а також військ (сил) в просторі та часі в будь-яких кліматичних умовах.

*УДК 341.824:338.47 (043.2)*
**Сидоренко С. М.**
Національна академія СБ України

# СТАН ТА ПЕРСПЕКТИВНІ НАПРЯМКИ СПІВРОБІТНИЦТВА СЛУЖБИ БЕЗПЕКИ УКРАЇНИ З КРАЇНАМИ НАТО У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Співробітництво Служби безпеки України з Північноатлантичним Альянсом у сфері забезпечення кібербезпеки триває з 2009 року і здійснюється у межах щорічних Національних програм співробітництва Україна-НАТО, які затверджуються відповідними указами Президента України.

У 2009 році за ініціативи СБ України було започатковано новий (на той час) формат стосунків з Альянсом – кібернетичні консультації Україна-НАТО з питань кібербезпеки, в рамках Спільної робочої групи Україна-НАТО з питань військової реформи.

Зокрема, в ході останнього раунду кіберконсультацій у 2013 році з експертами Альянсу були узгоджені положення проекту Стратегії кібербезпеки України, більшість з яких знайшла своє відображення у затвердженій Указом Президента України від 15 березня 2016р. № 96/216 «Стратегії кібербезпеки України».

Показовим є той факт, що до запровадження механізму консультацій НАТО вважав Україну джерелом кіберзагроз для інфраструктури Альянсу.

Іншим важливим механізмом інституціональної співпраці Служби безпеки України та Північноатлантичного Альянсу є участь СБ України у Процесі планування та оцінки сил Програми НАТО «Партнерство заради миру» [1].

СБ України долучена до Процесу планування та оцінки сил (ППОС) в рамках програми «Партнерство заради миру» з 2012 року. Звітування учасників програми передбачено процедурами Альянсу і здійснюється у заздалегідь визначені строки. Подані звіти слугують основою для підготовки фахівцями НАТО проектів підсумкових документів (оцінок) участі країн-партнерів у ППОС та прийняття відповідних політичних рішень.

Окрім матеріально-технічної допомоги, спрямованої на розширення спроможностей СБ України протидіяти кіберзагрозам, Північноатлантичний Альянс надає Службі освітню, а також консультативну та методичну допомогу у сфері забезпечення кібербезпеки.

З 2014 року в Офісі зв'язку НАТО в Україні працює радник Альянсу з кібербезпеки.

Щодо освітнього компоненту співробітництва Служби безпеки України та НАТО, то окрім тренінгів за сприяння уряду Естонії в рамках реалізації першого етапу Трастового фонду Україна-НАТО представники Слу-

жби на постійній основі беруть участь у різноманітних навчальних заходах [2].

Перспективними напрямками співробітництва з Альянсом вбачаються наступні:

– надання консультативної та технічної допомоги у створенні на базі Служби безпеки України відомчого навчального центру з функцією імітаційного полігона для реалізації навчальних програм, семінарів та тренінгів у сфері інформаційної безпеки та кібербезпеки (відповідно до Річної національної програми співробітництва Україна – НАТО на 2017 рік);

– узгодження з Науковим комітетом НАТО ініціативи щодо започаткування спільних з державами – членами НАТО науково-технічних проектів (досліджень), у тому числі з розбудови системи кіберзахисту в Україні (відповідно до Річної національної програми співробітництва Україна – НАТО на 2017 рік);

– організація зустрічей/семінарів з експертами Консорціуму з питань співпраці заради миру (PfPC – Partnership for Peace Consortium);

– у межах оновленої (липень 2016 року) політики НАТО з кібернетичної оборони вдосконалити механізм консультацій та співпраці, зокрема в освітній та науково-дослідній сфері, із Спільним центром передового досвіду з кіберзахисту у м. Таллін, Естонія, який дозволяв би ефективно співробітничати країнам – не членам НАТО із вказаною структурою Північноатлантичного альянсу;

– активізувати співпрацю СБ України з НАТО та з державами-членами Альянсу на двосторонній основі щодо обміну досвідом у сфері захисту компонентів критичної інформаційної державної інфраструктури в контексті постійних кібератак з боку російських спецслужб та контрольованих ними осіб проти України;

– опрацювати можливість звернення, у разі критичної кібератаки на вразливі компоненти інформаційної структури держави, за відповідною допомогою до Північноатлантичного альянсу в рамках застосування механізму роботи так званої Групи швидкого реагування Rapid Reaction Teams (RRTs) [4].

Послідовна позиція СБ України щодо налагодження та активізації співробітництва з Північноатлантичним Альянсом у сфері кібербезпеки, забезпечила сприйняття України країнами-членами НАТО як надійного і ефективного партнера.

**Література**

1. Указ Президента України «Про затвердження Річної національної програми співробітництва Україна – НАТО на 2017 рік» від 8 квітня 2017 року № 103/2017/ Президент України [Електронний ресурс]. – Режим доступу : http://www.president.gov.ua/documents/1032017-19779.

2. Щодо заснування Трастового Фонду Україна-НАТО з питань кібербезпеки, н.с. 129, т. 1, с. 123, 2014.

3. Наказ Центрального Управління СБ України від 26.01.2017 №46 «Щодо оголошення додаткової угоди з РСІ Румунії щодо постачання та передачі обладнання та програмного забезпечення до СБ України в рамках реалізації Трастового Фонду Україна-НАТО з питань кібербезпеки», К., СБ України, 2017.

4. Щодо виконання СБ України заходів передбачених Річної національної програми співробітництва Україна-НАТО на 2017 рік, н.с. 132, т.2, с145.

*УДК 355.40*

**Сніцаренко П. М.**
доктор технічних наук,
старший науковий співробітник,
Національний університет оборони України
імені Івана Черняховського

## СУТНІСТЬ ОЦІНКИ СТАНУ ІНФОРМАЦІЙНОЇ СФЕРИ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ ТА ЇЇ ЗНАЧЕННЯ ДЛЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Узагальнення словникових джерел свідчить, що *"інформаційна сфера – це суспільно значима сукупність видів діяльності в інформаційному просторі та система регулювання суспільних відносин, що виникають при цьому"*. Одночасно у словниках значиться, що *"інформаційний простір – середовище, в якому відбуваються інформаційні процеси та інформаційні відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони і захисту інформації (інформаційних ресурсів)"*. Сучасний інформаційний простір має дві інформаційні складові – сектор неелектронних інформаційних ресурсів (друкована продукція, когнітивні суспільні можливості, засоби символьних комунікацій) та сектор електронних інформаційних ресурсів (кіберпростір).

Необхідною умовою збереження суверенітету України, її сталого та прогресивного розвитку в сучасних умовах є достатність, належна якість і висока стабільність інформаційних ресурсів обох складових національного інформаційного простору, що забезпечується необхідним для цього рівнем *інформаційної безпеки держави*, з підкресленням того, що *кібербезпека – це інформаційна безпека в просторі (секторі) електронних інформаційних ресурсів*. Забезпечення певного рівня інформаційної безпеки держави визначається її здатністю до адекватного реагування на загрози інформаційній безпеці та їх нейтралізації, для чого має діяти відповідний загальнодержавний механізм. *Отже оцінка обстановки (стану) в інфор-*

*маційній сфері України полягає у визначенні загроз інформаційній безпеці держави та її здатності до адекватного реагування на ці загрози і їх нейтралізації.*

Відповідно до законодавства України загрозами інформаційній безпеці держави, в тому числі у кіберпросторі, є такі, що, матеріалізуючись на практиці, *можуть нанести шкоду людині, суспільству чи державі* (незалежно від джерела або причини їх походження та форми реалізації – інформаційна агресія, умисні маніпулятивно-злочинні інформаційні дії, механічне руйнування, інформаційна неспроможність, непрофесійна діяльність, службова бездіяльність), а саме:

*неповнота, невчасність та невірогідність інформації, що використовується*;

*негативний інформаційний вплив;*

*негативні наслідки застосування інформаційних технологій*;

*несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації*.

Ці загрози мають загальний та імовірнісний характер і залежать від ряду чинників та умов. Сектор безпеки і оборони України (в тому числі сили оборони або воєнна сфера), як невід'ємна частина життєдіяльності держави, піддається впливу цих же загроз, а тому висвітлення загроз інформаційній безпеці у цьому секторі є характерним і для усієї держави. Розглядаючи перелік наведених загроз з позиції оцінки стану в інформаційній сфері (з акцентом на сектор безпеки і оборони), зазначаємо таке.

Неповнота, невчасність та невірогідність інформації, що використовується (а також відсутність інформації за її потреби!), спричиняються обмеженими функціональними можливостями національної інформаційної інфраструктури, елементи якої формують інформаційний простір держави (у тому числі кіберпростір), зокрема в інтересах виконання завдань сектором безпеки і оборони України. Сьогодні такі можливості є дійсно обмеженими, що є окремим чинником загрози інформаційній безпеці держави.

На сьогодні в інформаційній інфраструктурі сектору безпеки і оборони України, зокрема сил оборони держави, наприклад, відсутні або нестійкі в бойових умовах ряд інформаційних систем реального часу – спостереження, навігація, зв'язок; потребують створення Єдина АСУ Збройних Сил України; автоматизований комплекс інформаційної інфраструктури Міністерства оборони України; автоматизована геоінформаційна система Збройних Сил України; автоматизована система (лінгвістичний робот) моніторингу медійного простору та соцмереж як складова протидії негативному інформаційному впливу; виникає проблема інтерфейсу та взаємодії цих систем у ході застосування сил оборони за призначенням.

Негативний інформаційний вплив, а також негативні наслідки застосування інформаційних технологій спричиняються цілеспрямованими діями елементів ворожої інформаційної інфраструктури або навмисними чи ненавмисними діями елементів національної інформаційної інфраструктури, які формують інформаційний простір держави (у тому числі кіберпростір).

Такі загрози можуть бути реалізовані у різних формах і способах, що спричиняє необхідність розглядати два різновиди негативного інформаційного впливу – *інформаційно-технічний*, що призводить до порушення або руйнації процесу функціонування технічних об'єктів інформаційної інфраструктури та *інформаційно-психологічний*, що призводить до необхідної для противника корекції поведінки та (або) світогляду певної цільової аудиторії, зміни її морально-психологічного стану.

На сьогодні обидва різновиди негативного інформаційного впливу найбільш активно та планомірно застосовуються, в агресивних діях Росії проти України, зокрема, проти її сил оборони. Найчастіше такий вплив здійснюється у способи радіоелектронної боротьби, несанкціонованого проникнення у військові інфокомунікаційні системи (кіберпростір) для їх руйнування, а також насичення інформаційного простору України (як шляхом вербально-агітаційних заходів, так і через кіберпростір, в тому числі електронні ЗМІ) продукцією маніпулятивно-пропагандистського змісту, вражаючи індивідуальну та масову свідомість особового складу її військових формувань для послаблення їх готовності до оборони держави та погіршення іміджу збройних сил, військової служби загалом. Ці дії проти України також є окремою реальною комплексною загрозою інформаційній безпеці держави у воєнній сфері.

Крім зазначеного, шкідливе застосування інформаційних технологій може бути спричинене некваліфікованими або недисциплінованими діями персоналу на об'єктах інформаційної діяльності власної інформаційної інфраструктури, що час від часу трапляється і також є джерелом загрози інформаційній безпеці.

Несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації може статися із-за недосконалості систем безпеки (захисту) інформації на елементах національної інформаційної інфраструктури, які формують інформаційний простір держави, зокрема і воєнної сфери (у тому числі кіберпростір).

Це найбільш утаємничена загроза інформаційній безпеці України, в тому числі у воєнній сфері, яка пов'язана із доступністю до інформаційних ресурсів. Для обох складових існування інформаційного ресурсу воєнної сфери держави ця загроза може бути матеріалізована, зокрема традиційними шляхами, що, на жаль, іноді стає реальним фактом:

механічним способом (викрадення носія, внесення правок у паперовий документ, його фото- або механічне копіювання, сторонній візуальний розгляд тощо);

використання знання окремих посадових осіб, яке збагачене із-за санкціонованого доступу, зокрема, інформацією з обмеженим доступом, для її несанкціонованого розповсюдження і використання, а також порушення конфіденційності (з мотивів корисливих або політичних).

Матеріалізація загрози зазначеного типу *у кіберпросторі*, що пов'язане із доступом до електронних інформаційних ресурсів, які поділяються на динамічні ресурси (інформаційних систем реального часу) та статичні ресурси (інформаційних систем типу довготермінових баз або сховищ даних чи знань), крім зазначеного, має додаткові особливості.

Для інформаційних систем, що створюють кіберпростір динамічних електронних інформаційних ресурсів (переважно *спостереження, навігація, зв'язок*) загрозу зазначеного типу спричиняє їх *перехоплення* шляхом ведення противником радіоелектронної розвідки або несанкціонованого зовнішнього проникнення в телекомунікаційні мережі транспортування таких ресурсів.

Для інформаційних систем, що створюють кіберпростір статичних електронних інформаційних ресурсів (*це галузь інформатизації – документи електронних бібліотек, архівів, баз та банків даних*) загрозу зазначеного типу спричиняє проникнення противника (зловмисника) через технічні засоби комунікації поза регламентом технічного доступу з метою *викрадення* змісту таких ресурсів.

В умовах нинішньої агресії Росії проти України прояви зазначеного типу загроз спостерігаються та реалізуються постійно, що негативно позначається на якості виконання суб'єктами інформаційної діяльності завдань за призначенням, зокрема, силами оборони держави.

До зазначених додаються також загрози інформаційній безпеці держави, які конкретизовані у положеннях Стратегії національної безпеки України:

відсутність комунікативної політики держави, слабкість системи стратегічних комунікацій;

недостатній рівень медіакультури суспільства та комп'ютерної (цифрової) грамотності.

Наслідки цих типів загроз, зокрема, відчутно впливають, по-перше, на когнітивні процеси в армійському середовищі, що негативно позначається, зокрема, на рівні морально-психологічного стану особового складу сил оборони України, а по-друге, зменшуються можливості та знижується якість протидії негативному інформаційно-психологічному впливу противника.

Наведені аналітичні результати свідчать про об'єктивні факти наявності (реалізації) усіх типів загроз інформаційній безпеці України. Най-

більш відчутними та небезпечними, зокрема для сектору безпеки і оборони України, слід вважати загрози, які пов'язані з існуючою недосконалістю ряду елементів інформаційної інфраструктури воєнної сфери, що призводить до загрози типу *неповнота, невчасність та невірогідність інформації, що використовується, а також відсутність інформації за її потреби,* а крім цього, це щоденна сьогодні загроза *негативного інформаційного впливу* на особовий склад військових формувань сектору безпеки і оборони України, яка знижує морально-психологічний стан військ (сил), та загроза типу *відсутність комунікативної політики держави, слабкість системи стратегічних комунікацій,* що найбільше шкодить процесу протидії негативному інформаційному впливу від противника.

Об'єктивні факти наявності (реалізації) усіх типів загроз інформаційній безпеці України одночасно свідчать про те, що загальнодержавний механізм своєчасного та адекватного реагування на такі загрози та їх нейтралізації сьогодні є недосконалим і не відповідає нагальним потребам, незважаючи на те, що опираючись на окремі норми законодавства, на відомчому рівні держави здійснюються певні заходи щодо забезпечення інформаційної безпеки як у кіберпросторі, так і поза його межами, але, як правило, без належної гармонізації та взаємної синхронізації зусиль і процедур.

На наш погляд, кореневою причиною недосконалості такого загальнодержавного механізму і, ймовірно, головною, *системною* загрозою інформаційній безпеці України, слід вважати відсутність законодавчого визначення сутності державної інформаційної політики України, наслідком чого сталося роздвоєння дій за двома не гармонізованими між собою напрямами – власне інформаційним та кібернетичним, що є методологічною помилкою та призводить до нерозуміння прийнятої нормативно-правової бази, а звідси неминучого дублювання практичних дій і труднощів щодо взаємодії.

Вищенаведене відобразило основну сутність та характерні особливості існуючого стану інформаційної сфери держави, ґрунтуючись на положеннях законодавства України, зокрема через характеристику реальних загроз інформаційній безпеці на прикладі сектору безпеки і оборони України, переважно сил оборони. Це надає можливість висновку щодо загальної оцінки стану інформаційної сфери.

Таким чином, на основі зазначеного, оцінюючи інформаційну сферу сектору безпеки і оборони України, загалом держави, з врахуванням її нинішнього стану, можна стверджувати, що *сьогодні вона є недосконалою та вразливою від загроз, особливо зовнішнього генерування*.

Ця оцінка має те значення, що вона відображає загальний стан забезпечення інформаційної безпеки України та спричиняє необхідність подальших кроків щодо удосконалення за рядом напрямів діяльності, у тому числі в інтересах виконання особливо актуальних сьогодні завдань оборони держави.

Найпершим кроком має бути законодавче визначення сутності інформаційної політики України. Зважаючи на положення статті 17 Конституції України, таку політику для реалізації окремої функції держави може визначити прийняття рамкового Закону України “Про забезпечення інформаційної безпеки України”, з подальшим внесенням відповідних змін до ряду Законів України, зокрема, “Про національну безпеку України”, “Про інформацію”, “Про основні засади кібербезпеки України”, “Про оборону України”, а також до Стратегії національної безпеки України та залежних від цих актів наступних нормативно-правових документів.

Очевидними для підвищення рівня інформаційної безпеки України, зокрема у воєнній сфері, також є наступні пріоритетні напрями діяльності:

а) удосконалення теоретичних основ забезпечення інформаційної безпеки держави, з урахуванням умов України та функціонування воєнної сфери;

б) розвиток елементів інформаційної інфраструктури воєнної сфери, що створюють мобільний кіберпростір управління військами та зброєю (бойовий інформаційний простір) на основі концепції C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance – командування, управління, зв’язок, розрахунки, розвідувальна інформація, спостереження та рекогносцировка);

в) створення автоматизованого комплексу інформаційної інфраструктури Міністерства оборони України для управління оборонними ресурсами та поєднання її з елементами бойової системи C4ISR;

г) створення комплексних систем захисту інформації на усіх об’єктах інформаційної діяльності інформаційної інфраструктури воєнної сфери;

ж) проактивна протидія негативному інформаційному впливу на особовий склад військ (сил) на основі виявлення та кількісного оцінювання рівня такого впливу, а також розвитку можливостей державних ЗМІ, зокрема військових, та системи державних комунікацій (стратегічних, урядових, кризових);

з) розвиток розвідувальних спроможностей, зокрема у кіберпросторі, в інтересах оборони держави;

і) створення системи протидії воєнній агресії у кіберпросторі (системи кібероборони України);

к) підготовка кваліфікованих кадрів за усіма основними напрямами забезпечення інформаційної безпеки держави, зокрема у воєнній сфері.

*УДК 355.40: 356.35*
**Сніцаренко П. М.**
доктор технічних наук,
старший науковий співробітник,
**Ткаченко В. А.**
кандидат військових наук,
**Грицюк В. В.**
Національний університет оборони України
імені Івана Черняховського

# МЕТОДИЧНИЙ ПІДХІД ДО АВТОМАТИЗОВАНОЇ КЛАСИФІКАЦІЇ ІНФОРМАЦІЙНИХ ПОДІЙ

Сучасний світ характеризується широким використанням урядами (та зокрема арміями) багатьох країн наукового, технічного та практичного досвіду проведення інформаційних операцій, акцій, атак і актів при вирішенні завдань досягнення національних цілей, в тому числі у ході воєнних конфліктів, коли об'єктами інформаційного впливу, зокрема, його різновиду – інформаційно-психологічного впливу, є збройні сили (військові формування) противника. Особливої важливості для України ця обставина набула напередодні та в період військової агресії проти неї з боку Російської Федерації, коли гостро та відчутно проявилися наслідки зовнішнього негативного інформаційного впливу, зокрема на особовий склад Збройних Сил України (далі ЗС України). Тому невідкладним є завдання протидії такому впливу, невід'ємною складовою якої мати бути класифікація (кластеризація) інформаційних подій в інформаційному просторі з метою подальшого аналізу та прийняття рішення на протидію.

*Класифікація документів* – це одне з завдань інформаційного пошуку, яке полягає у зарахуванні документа до однієї з кількох категорій на підставі його змісту [1]. Зазвичай під класифікацією документів мається на увазі класифікація тексту, якщо не вказано інше .

Зважаючи на значний обсяг інформації, яка обробляється в сучасних умовах та обмежений час на прийняття рішення, пропонується вирішувати завдання підвищення оперативності у процесі протидії такому інформаційному впливу за рахунок автоматизації складових цього процесу [2], зокрема процесу класифікації інформаційних подій. На сьогодні такий процес можна реалізувати ручним, напівавтоматичним (автоматизованим) та автоматичним методом. При цьому розуміється, що автоматичний метод слугує для виконання складових напівавтоматичного методу.

Відповідно до [3] під *автоматичною класифікацією* розуміється віднесення автоматичним пристроєм об'єктів з деякої множини до того або іншого класу із заданого (кінцевого) набору класів.

В основі автоматичної класифікації доцільно покласти аналіз інформації про кожний об'єкт, яка вводиться в пристрій. В такому випадку, ін-

формацію про об’єкт, що класифікується, слід інтерпретувати як сукупність ознак. Тоді, кожній ознаці доцільно зіставити координату (багатоградаційну або двійкову, залежно від природи ознаки) в деякому просторі ознак, де будь-який пред’явлений об’єкт буде відповідати певній точці простору. При вдалому виборі ознак точки одного класу будуть групуватися в компактні скупчення з межами, що порівняно легко апроксимуються, або, в постановці ймовірності, розподілами ймовірності. Пред’явлений об’єкт залежно від того, куди потрапляє в просторі ознак точка, що відображає, буде класифікуватися відповідно до прийнятого вирішального правила [3].

Запропонований автоматизований підхід полягає в написанні правил, згідно яких автоматичним методом можна зарахувати текст до тієї чи іншої категорії. Наприклад, одне з таких правил може виглядати наступним чином: “якщо текст містить слова “похідна” і “рівняння”, то віднести його до категорії “математика””. Спеціаліст, який знайомий з предметною областю і володіє навичкою написання регулярних виразів, може скласти низку правил, які потім автоматично застосовуються до класифікації нових документів. Такий підхід кращий за ручний метод, оскільки процес класифікації автоматизується і оперативність оброблення великого обсягу документів значно пришвидшується.

Поряд з тим, слід відмітити переваги напівавтоматичного (автоматизованого) над повністю автоматичним методом. Останній у процесі класифікації передбачає “машинне навчання” (Machine Learning) з нечіткою кількістю класів (тобто кількість класів і підкласів може змінюватись (бути гнучкою) в процесі роботи). Але створювана множина класів може не відповідати за якістю запитам та вимогам до системи. На відміну від автоматичного методу, побудова правил класифікації оператором при напівавтоматичному (автоматизованому) методі підвищить точність класифікації у порівнянні з “машинним навчанням”. В той же час, при такому методі, слід приділяти додаткову увагу процесам створення і підтримки в актуальному стані правил (критеріїв) класифікації, що вимагає додаткових витрат ресурсів (людей, часу тощо).

**Література**

1. Christopher D. Manning, Hinrich Schütze An Introduction to Information Retrieval Draft. Online edition. Cambridge University Press. – 2009. –544 p.

2. Загоруйко Н. Г. Прикладные методы анализа данных и знаний. – Новосибирск: ИМ СО РАН, 1999.

3. Енциклопедія кібернетики : у 2 т. / за ред. В. М. Глушкова. – Київ : Гол. ред. Української радянської енциклопедії, 1973.

*УДК 321.011:65.012.8*
**Солодка О. М.**
кандидат юридичних наук,
старший науковий співробітник,
Національна академія СБ України

# ІНФОРМАЦІЙНИЙ СУВЕРЕНІТЕТ: ПРАВОВІ ПІДХОДИ ДО РОЗУМІННЯ ТА ЗАБЕЗПЕЧЕННЯ

Боротьба за інформаційний простір не залишає топових позицій світових безпекових чартів та змушує держави шукати балансу між здобутками інформаційного суспільства та забезпеченням інформаційної безпеки і збереженням власного інформаційного суверенітету. Зазначене підтверджується тим, що серед ключових питань 56-ї Мюнхенської конференції з безпеки 2020 року стали загроза Росії та експансія Китаю. Якщо питання Росії є очевидними, то антикитайські настрої цього разу викликала не торгівля, як останні кілька років, а мережі 5G від Huawei. Купите їхні 5G – і ви завжди будете вразливі до їх шпигунства, – такий меседж США набирає обертів протягом останніх кількох місяців, особливо після заяв Великобританії, Франції і Німеччини разом з ЄС про те, що вони використовуватимуть обладнання Huawei у галузях, які не мають оборонного значення.

Відтак, і надалі зростає усвідомлення важливості проблем регулювання суспільних інформаційних відносин, зокрема узгодження принципово різних підходів до концептуального вирішення питання виокремлення та формулювання поняття «інформаційний суверенітет», уточнення його характеристик для пошуку відповіді на питання про методи й засоби його забезпечення. Для України така правова категорія є особливо важливою, оскільки, гібридна війна, розв'язана Росією, ставить питання існування суверенної Української держави в безпосередню залежність від забезпечення інформаційного суверенітету держави.

Загалом, тлумачення поняття «суверенітет держави» в енциклопедичних джерелах, як правило, пов'язані з визначенням меж суверенітету державними кордонами. Однак, сучасні процеси інформатизації, інформаційні обміни в рамках глобального інформаційного простору значною мірою розмивають територіально-географічні особливості суверенітету як такого, а під впливом тенденцій розвитку інформаційного суспільства акценти державного суверенітету зміщаються і на перший план виходить його інформаційна складова або інформаційний суверенітет держави.

Поняття «інформаційний суверенітет держави» є відносно відокремленим видом державного суверенітету, оскільки ознаки державного та інформаційного суверенітетів не завжди збігаються. Відтак, інформаційний суверенітет держави, хоча і може розглядатися як видовий відносно суве-

ренітету держави, відрізняється від останнього юрисдикційними межами, колом уповноважених суб'єктів та ступенем участі недержавних структур у забезпеченні, власними моделями і комбінаціями методів правового регулювання, рівнем міжнародної співпраці тощо.

Єдине визначення інформаційного суверенітету міститься в Законі України «Про Національну програму інформатизації» від 1998 р. як «здатність держави контролювати і регулювати потоки інформації з-поза меж держави з метою додержання законів України, прав і свобод громадян, гарантування національної безпеки держави» [1].

Разом з тим, у науковій літературі зустрічається поняття «цифровий суверенітет». У випадку інформаційного суверенітету йдеться про ширше коло понять, яке включає не лише здатність впливати на інформаційно-комунікаційні технології загалом, але і на контент, причому далеко не завжди вплив слід розуміти як контроль, бо йдеться водночас про протидію інформаційно-психологічним операціям чи здійснення власних операцій. У розуміння ж цифрового суверенітету вкладається смисл пріоритетних завдань щодо забезпечення ІКТ-незалежності держави, тоді як до контентної частини терміна звертаються лише епізодично, на рівні збирання певних конкретних даних. Дедалі частіше у західних наукових працях з'являється поняття «кібермогутність», під яким мають на увазі або «здатність до використання кіберпростору для створення переваг та впливу в усіх інших операційних просторах через інструменти могутності» або «можливість країни здійснювати заходи та впливати на кіберпростір» [2].

Особливістю забезпечення цифрового суверенітету країн Західної Європи та США є те, що акцент робиться на державно-приватне партнерство (йдеться про пріоритет компаній, які займаються розробкою інформаційних технологій), а у таких країнах як Росія, Китай цифровий суверенітет реалізується виключно за рахунок створення національних сил і засобів в галузі інформаційно-комунікаційних технологій, проте це здійснюється під чітким контролем держави (в умовах відсутності конкуренції).

На нашу думку, інформаційний суверенітет – це властивість державної влади, що полягає у її верховенстві, самостійності, повноті і неподільності в інформаційному просторі України та рівноправності і незалежності у відносинах з іншими державами у глобальному інформаційному просторі. Цифровий суверенітет є різновидом інформаційного суверенітету.

Україна, як держава демократичних принципів, повинна в основу своєї інформаційної політики покладати принципи пріоритетності захисту індивідуальних, аніж державних інтересів. У цьому сенсі необхідно досягти балансу між правом на інформацію та вимогами щодо забезпечення інформаційного суверенітету держави, а у розрізі цифрового суверенітету держави необхідно враховувати право особи на приватність комунікацій.

**Література**

1. Закон України «Про Національну програму інформатизації» від 04.02.1998 // Сайт Верховної Ради України. URL: http://zakon4.rada.gov.ua/laws/show/559/2011 (дата звернення 20.02.2020).

2. Ожеван М.А., Дубов Д.В. Homo ex Machina. Філософські, культурологічні та політичні передумови формування конвергентного суспільства. Київ: НІСД. 2017, 272 с.

*УДК 342:378*

**Суслін С.В.**
кандидат юридичних наук, доцент,
Національна академія СБ України

## ОСОБЛИВОСТІ ТА ПЕРСПЕКТИВИ РЕАЛІЗАЦІЇ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ «ПРАВО ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

Ефективність державної політики в інформаційній сфері, засади якої визначені Доктриною інформаційної безпеки України [1], значною мірою залежить від якості кадрового забезпечення органів державної влади та недержавних структур, що реалізують таку політику. Зростання рівня загроз інформаційній безпеці в умовах триваючого збройного конфлікту на території України актуалізувало потребу у фахівцях, спроможних реалізовувати правові механізми забезпечення інформаційної безпеки. На основі критичного аналізу кадрового потенціалу України у сфері правового забезпечення інформаційної безпеки, накопиченого Службою безпеки України досвіду щодо забезпечення інформаційної безпеки держави в Національній академії СБ України (далі – Академія) розроблено та з 2016 року запроваджено освітньо-професійну програму «Право інформаційної безпеки» першого бакалаврського рівня вищої освіти за спеціальністю 081 «Право» (далі – ОП).

Освітня діяльність за цією програмою здійснюється на базі структурного підрозділу Академії – Навчально-наукового інституту інформаційної безпеки, в якому здобувачам освіти створені необхідні умови для навчання, проживання та саморозвитку. Досягнення студентами програмних результатів навчання забезпечують кваліфіковані науково-педагогічні працівники 15 кафедр Академії, з яких 10 осіб мають науковий ступінь доктора наук та/або вчене звання професора, 31 особа має науковий ступінь кандидата наук та/або вчене звання доцента.

Програма спрямована на оволодіння студентами концептуальними й спеціалізованими знаннями та вміннями в галузі права. З огляду на це її основу становлять освітні компоненти, що обумовлені вимогами стандар-

ту вищої освіти за спеціальністю 081 «Право» для першого (бакалаврського) рівня вищої освіти [2]. Водночас ОП містить компоненти, спрямовані на формування компетентностей у сфері правового забезпечення інформаційної безпеки (навчальні дисципліни «Інформаційні системи та технології», «Інформаційне право», «Інформаційна безпека», «Кримінологічний аналіз злочинів в інформаційній сфері» тощо). Особливість та унікальність цієї програми полягає в тому, що вона уперше в Україні розвиває перспективи професійної підготовки юристів, обізнаних із правовим механізмом обігу та захисту різних видів інформації з обмеженим доступом на підприємствах, в установах та організаціях різних форм власності. Студенти отримують навички щодо забезпечення типових потреб таких суб'єктів у захисті персональних даних працівників та конфіденційної інформації фірми, комерційної, банківської таємниці, а також забезпечення режиму секретності, передбаченого законодавством України про державну таємницю.

Якість освітньої діяльності та вищої освіти за ОП забезпечується здійсненням цілеспрямованих заходів, зокрема, щорічним моніторингом відповідності кадрового, навчально-методичного, інформаційного та матеріально-технічного забезпечення Ліцензійним умовам провадження освітньої діяльності та виробленням на його основі заходів, спрямованих на покращання складових освітньої діяльності; аналізом виконання здобувачами освіти навчальних (робочих навчальних) планів; контролем якості викладання навчальних дисциплін; моніторингом та періодичним переглядом ОП тощо.

Таким чином, система необхідних освітніх компонентів ОП, належні кадрове та ресурсне забезпечення її реалізації, а також система забезпечення якості освітньо-професійної програми «Право інформаційної безпеки» дозволяють досягти її мети – підготувати бакалаврів з права, які володіють компетентностями, достатніми для розуміння природи й функцій права, змісту його правових інститутів, а також застосування права в умовах євроінтеграційних процесів, що відбуваються в Україні, зокрема пов'язаних із забезпеченням інформаційної безпеки.

Сильною стороною даної програми є її унікальність, оскільки це єдина ОП в Україні, що дозволяє здобути вищу освіту зі спеціальності 081 «Право» першого (бакалаврського) рівня з акцентом на спеціалізацію у сфері правового забезпечення інформаційної безпеки. Розвиток в Україні та за її межами інформаційного суспільства на фоні процесів глобалізації й загострення економічної конкуренції мають наслідком збільшення загроз інформаційній безпеці державних та недержавних інституцій. Тому зазначена особливість ОП в умовах зростання попиту на фахівців, здатних реалізувати правові механізми протидії загрозам в інформаційній сфері, надає здобувачам освіти переваги щодо працевлаштування у Службі безпеки України, інших правоохоронних та державних органах, що реалізу-

ють функції щодо забезпечення інформаційної безпеки, а також на підприємствах, в установах та організаціях недержавної форми власності.

Водночас реформування СБ України матиме наслідком уточнення її компетенції у сфері забезпечення інформаційної безпеки, системи підготовки кадрів, що визначатиме необхідність відповідного удосконалення освітньої програми з метою підвищення якості професійної підготовки випускників та їх конкурентоспроможності на ринку праці. З огляду на це, до основних напрямів розвитку ОП, на нашу думку, належатимуть актуалізація переліку та змісту освітніх компонентів ОП, збільшення в її структурі питомої ваги практичної підготовки, активізація участі стейкхолдерів (насамперед, здобувачів освіти та роботодавців) у процесі оновлення змісту програми.

**Література**

1. Указ Президента України від 25 лютого 2017 року № 47/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України».

2. Наказ Міністерства освіти і науки України від 12.12.2018 року № 1379 «Про затвердження стандарту вищої освіти за спеціальністю 081 «Право» для першого (бакалаврського) рівня вищої освіти».

*УДК: 340+35.078.3*

**Тарасюк А. В.**
кандидат юридичних наук,
НДІ інформатики і права НАПрН України

## ОНТОЛОГІЧНІ ЗАСАДИ ПОНЯТТЯ «КІБЕРБЕЗПЕКА»

Поняття кібербезпеки є вкрай багатогранним, відтак складно формалізуються, адже тут існує дуже багато різних уявлень і поглядів. У даний час, у глобальному медіапросторі, в публіцистичних і наукових працях, а також у політичних і державних документах багатьох країн поряд з доктринальноюінституціалізацією кібербезпеки, активно відбувається становлення її понятійного-категоріального апарату.

Слід зазначити, що термін «кібербезпека» є похідним від родового терміну «безпека», відтак «кібербезпека» становить частину більш загального поняття «безпека», що вирізняється специфічними особливостями, і одночасно має виступати результатом синтезу поняття «безпека» та прикметника «кібернетична» (скорочено – «кібер»).

Базовою категорію у дослідження кібербезпеки виступає категорія «безпеки». У своєму дослідженні ми будемо керуватися поняттям «безпе-

ка», яке визначив український дослідник І. Корж. Вчений вважає, що в соціальному розумінні «безпека» означає збалансований стан функціонування соціальної системи (людини, держави, світового співтовариства), антропогенних, природних систем тощо, за якого людина завдяки знанням про навколишнє природне середовище і тенденції його розвитку своїми діями спроможна своєчасно виявити та мінімізувати негативний вплив наявних та потенційних загроз або уникнути їх, що, своєю чергою, дає їй можливість зберігати систему своїх цінностей і забезпечувати подальший їх розвиток [1 с. 71]. Такий підхід нами взятий як базовий у дослідження змісту кібербезпеки.

Створена ще в 1967 році Асоціація аудиту і контролю інформаційних систем (ISACA)у виданому 2014 року глосарії визначає*кібербезпеку* якзахист інформаційних активів шляхом боротьби із загрозами безпеці інформації, яка обробляється, зберігається та передається за допомогою інформаційних систем, котрі взаємодіють в мережах [2]. А в аналітичному виданні «Трансформація кібербезпеки» детальніше тлумачить це поняття: «…Кібербезпека охоплює все, що захищає організації та фізичних осіб від умисних атак, порушень, інцидентів та їх наслідків. На практиці кібербезпека стосується насамперед тих типів атак, порушень та інцидентів, які є цільовими, високотехнологічними та складними у виявленні чи управлінні. …Кібербезпека зосереджується на так званих складних спрямованих постійних загрозах (APT), кібервійнахта їхньому впливі на організації та людей» [3].

Також, виходячи з аналізу базових категорій, які наводяться в Законі України «Про основні засади забезпечення кібербезпеки України», вважаємо за доцільне на законодавчому рівні визначити наступне:

- поняття «стан захищеності»;
- поняття «цифрове комунікативне середовище»;
- критерії забезпечення кібербезпеки.

Визначення терміну «кібербезпека» базується на дефініції терміну «*кіберпростір*», який пропонується розуміти як *»середовище (віртуальний простір), яке надає можливості (послуговує) здійсненню комунікацій та/або реалізації суспільних відносин, утворене внаслідок функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням Інтернет та/або інших глобальних мереж передачі даних».*

Кібербезпека має на меті передусім забезпечення нормального функціонування кіберпростору, захищаючи його від виникаючих загроз ефективним чином. Відтак визначати кібербезпеку доцільно не лише як «стан захищеності», але й доцільно враховувати її діяльнісний аспект. Крім того, поняття кібербезпеки має включати як аспект «кіберзахищеності», так і аспект «кібербезпечності». Отже, за результатами проведеного дослі-

дження може бути запропоноване наступне визначення кібербезпеки – *це безпечність об'єктів кіберпростору й 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, а також постійний процес попередження й протидії відповідним загрозам*.

У даному визначенні реалізується визначальна мета державної політики в кіберпросторі: забезпечення стану захищеності основних прав і свобод громадян на життя, здоров'я, фізичну й духовну недоторканність, доступ до інформації, законних інтересів людини, суспільства й держави в кібернетичному просторі від внутрішніх і зовнішніх загроз, що полягає в дотриманні загальновизнаних і встановлених міжнародною спільнотою обмежень на поширення завідомо недостовірної та шкідливої інформації, збереженні інформаційних ресурсів, їх цілісності, конфіденційності й недоступності для стороннього втручання, а також захисту інформаційно-телекомунікаційних мереж і відповідного обладнання, котрі забезпечують розміщення, накопичення, обіг і використання інформації.

**Література**

1. Корж І.Ф. Безпека: методологічні підходи до поняття. JURNALUL JURIDIC NAȚIONAL: TEORIE ȘI PRACTICĂ. Серпень 2019. С. 68-72.

2. ISACA, Глосарій з кібербезпеки, 2014 р.: http://www.isaca.org/Knowledge-Center/Documents/Glossary/Cybersecurity_Fundamentals_glossary.pdf.

3. ISACA, Трансформація кібербезпеки, США, 2013 р., с. 11: www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Transforming-Cybersecurity-Using-COBIT-5.aspx.

*УДК 004.6:004.451.5*

**Тиква В. Л.**
Національна академія СБ України

## «ПОНЯТТЯ BIGDATA. ІСТОРІЯ ВИНИКНЕННЯ. ПРИКЛАДИ ЗАСТОСУВАННЯ»

BigData (великі дані) – набори інформації (як структурованої, так і неструктурованої) настільки великих розмірів, що традиційні способи та підходи (здебільшого засновані на рішеннях класу бізнесової аналітики та

системах управління базами даних) не можуть бути застосовані до них [1]. Альтернативне визначення називає «великими даними» феноменальне прискорення накопичення даних та їх структурування[1]. Важливо також відзначити те, що часто під цим поняттям у різних контекстах можуть мати на увазі як дані великого об'єму, так і набір інструментів та методів. Наприклад, засоби масово-паралельної обробки даних системами наступних категорій:NoSQL – база даних, що забезпечує інший механізм зберігання та видобування даних, ніж звичний підхід таблиць-відношень в реляційних базах даних; алгоритмами MapReduce – програмна модель та програмний каркас, що її реалізує, розроблені компанією Google для проведення розподіленої паралельної обробки великих масивів даних з використанням кластерів звичайних недорогих комп'ютерів, чи програмними каркасами проекту Hadoop.

ApacheHadoop – вільна програмна платформа і каркас для організації розподіленого зберігання і обробки наборів «великих даних» з використанням моделі програмування MapReduce, при якій завдання ділиться на багато дрібніших відособлених фрагментів, кожен з яких може бути запущений на окремому вузлі кластера, що складається з серійних комп'ютерів.

Сама по собі концепція «великих даних» не нова, вона виникла в часи мейнфреймів та пов'язаних з ними наукових комп'ютерних обчислень, оскільки наукомісткі обчислення завжди відрізнялися складністю і зазвичай нерозривно пов'язані з необхідністю обробки великих обсягів інформації.

Авторство терміну «великі дані» належить КліффордуЛінчу, редакторові журналу Nature, який зібрав матеріали про явище вибухового зростання обсягу, різноманітності даних та підготував у вересні 2008 року спеціальний випуск журналу, де відобразив феномен великих даних; термін був запропонований за аналогією з подібними в діловому англомовному середовищі метафорами «велика нафта» чи «велика руда» [2].

Чималий галас навколо поняття BigData виник після того, як в червні 2011 року консалтингова компанія «McKinsey» випустила доповідь «Великі дані: наступний рубіж в інноваціях, конкуренції та продуктивності», в якому оцінила потенційний ринок «великих даних» в мільярди доларів [1]. В тому ж році аналітична компанія «Gartner» відзначає великі дані як тренд номер два в інформаційно-технологічній інфраструктурі, поступаючись лише віртуалізації [3].

У 2012 році адміністрація президента США виділила 200 мільйонів доларів для того, щоб різні американські відомства організовували конкурси з впровадження технологій «великих даних» в життя. Якщо в 2009 році американські венчурні фонди вклали в галузь всього 1,1 мільярда доларів, то в 2012 – вже 4,5 мільярда доларів [1].

У 2015 році аналітична компанія «Gartner» вилучила «великі дані» зі своєї діаграми Gartner Hype Cycle, пояснивши це рішення тим, що ці технології перестали бути «проривними» і стали нормою для корпоративного IT-співтовариства: «сьогодні всі дані – великі» [4].

У 2017 році в Україні з'явився онлайн-курс з «великих даних» на платформі Prometheus [5].

Кінцевою метою обробки інформації є отримання результатів, які легко сприймаються людиною та є ефективними в умовах безперервного росту й розподілення інформації по численних вузлах обчислювальної мережі.

Для характеристики «великих даних» використовують «три v»: їх обсяг (англ. volume), швидкість накопичення нових даних та їх обробки (англ. velocity) та різноманіття типів даних, які можуть оброблятися (англ. variety) [1].

До основних переваг використання технології можна віднести:

– отримання якісно нових знань за рахунок комплексного аналізу усієї інформації у єдиному аналітичному сховищі;

– розширення функціональності існуючих інформаційних систем підтримки бізнесу;

– збільшення ефективності використання апаратних ресурсів серверів;

– забезпечення мінімальної вартості використання всіх видів інформації за рахунок можливості використання ПЗ з відкритим кодом і хмарних технологій.

Водночас, критика «великих даних» пов'язана з тим, що їх зберігання не завжди приводить до отримання швидкої вигоди, а швидкість оновлення даних і «актуальний» часовий інтервал не завжди розумно порівнянні.

Серед відомих випадків застосування «великих даних» можна назвати перемогу Барака Обами на президентських виборах 2012 року. Аналітики виборчого штабу Обами активно використовували BigData для аналізу настроїв виборців та коригування програми кандидата. «Великі дані» також є одним з ключових інструментів роботи Агентства національної безпеки США – у дата-центрі, що знаходиться у штаті Юта аналізуються дані, які АНБ збирає про користувачів в інтернеті [5].

Соціальні мережі та геолокаційні сервіси представляють величезні обсяги інформації, аналіз якої є дуже важливим для прикладних задач містобудування, таких як проектування транспорту, аналіз суспільної думки, виявлення та координація надзвичайних ситуацій тощо [6].

У Великій Британії методи BigData прийняті на озброєння Міністерством охорони здоров'я. Аналізуючи інформацію про те, які рецепти виписують медики, аналітики міністерства намагаються оцінювати потреби британців в ліках та оптимізувати доставки препаратів в різні частини країни [5].

Із поширенням інформаційних технологій у більшості сфер сучасного життя поняття BigData набуває все більшого значення для аналізу відкритої інформації у вигляді статистичних даних. Глибинний аналіз даних здійснюється автоматично шляхом застосування методів математичної статистики, штучних нейронних мереж, теорії нечітких множин або генетичних алгоритмів. Метою аналізу є виявлення правил та закономірностей, наприклад, статистичних подій.

Так, наприклад, можливо виявити зміни у поведінці осіб або груп осіб для регулювання стратегії окремого підприємства, галузі та навіть цілої країни.

Зважаючи та те, що в рамках міжнародної економічної, політичної, ідеологічної, релігійної та соціальної боротьби спецслужби передових країн інтенсивно використовують BigDatay розвідувальних цілях та з метою перешкоджання деструктивної діяльності на шкоду інтересам їх держав, кожна держава має впровадити використання явища BigData для виконання завдань власних спецслужб.

**Література**

1. Великі перспективи індустрії BigData. Український суперкомп'ютерний інтернет-дайджест. 19 лютого 2013.

2. Clifford Lynch (2008). Bigdata: Howdoyourdatagrow? Nature 455 (7209). doi:10.1038/455028a.

3. Gartner's Top 10 IT challen gesincludee xiting babyboomers, BigData. Computerworld (eng). 18 October 2011.

4. Шельпук, Євген (18 лютого 2016). Маленька історія великих даних. TheUkrainians.

5. Золотніков, Ярослав; Бондарев, Олексій (6 січня 2016). Друга нафта. В Україні з'явиться онлайн-курс з Bigdata – найбільш затребуваної в світі IT-професії. Новое Время.

6. Бродецький, Андрій (31 жовтня 2013). Як Foursquare допомагає планувати міста. КПІшник.

*УДК 341.824:338.47 (043.2)*

**Ткаченко О. П.**
Національна Академія СБ України

## ЩОДО ЗАХОДІВ СБ УКРАЇНИ У СФЕРІ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ВІД ТЕРОРИСТИЧНИХ АТАК В КОНТЕКСТІ ВИКОНАННЯ РЕЗОЛЮЦІЇ РАДИ БЕЗПЕКИ ООН

Постійні кібератаки упродовж останніх трьох років перетворили Україну на полігон з випробувань російської кіберзброї, на якому відпра-

цьовуються тактика та нові технології втручання в інформаційні системи, здійснення кібердиверсій та актів тероризму, інформаційно-психологічних операцій. І ми розуміємо чому так: тренувати власні сили на Україні можна не побоюючись бути покараним у юридичному сенсі, бо Кремль вже давно нехтує не лише власним, але й міжнародним законодавством, якщо це відповідає поточній геополітичній ситуації.

Натомість кібератаки наприклад на США, як ми всі мали змогу пересвідчитись під час виборів Президента США у 2016 році, здійснені **більш витончено і технологічно досконало**, ніж відносно «примітивна» атака на ЦВК України під час виборів Президента України у 2014 році.

Саме тому Україною була ініційовано розробка та прийняття першої в історії Ради безпеки ООН (РБ ООН) Резолюції РБ ООН 2341/2017 щодо захисту критичної інфраструктури від терористичних атак. Україна вдячна всім країнам, які підтримали нашу ініціативу та долучилися до розробки цього важливого міжнародного документу.

В контексті імплементації Резолюції 2341/2017 в за ініціативи СБУ вжито наступних заходів:

– у жовтні 2017 року Верховною Радою України прийнято Закон «Про основні засади забезпечення кібербезпеки України», де вперше в українському законодавстві з'явилося визначення поняття «критична інфраструктура» та інші важливі терміни, врегульовано повноваження спецслужб та правоохоронних органів України у сфері захисту критичної інфраструктури від кіберзагроз, зокрема кібератак тощо;

– налагоджено дієве публічно-приватне партнерство державних органів відповідальних за захист критичної інфраструктури із представниками ІТ спільноти.

*Зокрема в рамках відповідного проекту Ради Європи, що реалізується для країн Східного Партнерства Євросоюзу (в т.ч. для України) в Україні заплановано до підписання Меморандум про взаєморозуміння між ІТ бізнесом та спеціальними і правоохоронними органами України у сфері попередження та подолання наслідків атак на критичну інфраструктуру країни. Варто зазначити, що якщо раніше приватний бізнес не мав довіри до держави у цьому контексті, то тепер у разі виникнення масштабного кіберінциденту в інфраструктурі тієї чи іншої компанії, останні за власною ініціативою звертаються по допомогу до СБ України;*

– активізовано співробітництво з відповідними структурами ООН зокрема з Управлінням ООН по боротьбі з наркотиками та злочинністю (УНЗ ООН).

*Представники СБ України регулярно беруть участь в заходах під егідою УНЗ ООН. Так в ході останнього засідання Міжурядової групи експертів з протидії кіберзагрозам, рекомендації українських експертів включені до підсумкового документу вказаного засідання. Крім того за ініціа-*

*тиви СБ України УНЗ ООН наразі опрацьовує питання щодо приєднання України до програми ООН «Global cybersecurity agenda»;*

– за ініціативи та безпосередньої участі СБ України в контексті виконання положень Резолюції ООН 2341/2017 розроблений та направлений до Верховної Ради України законопроект яким передбачено криміналізацію кібератак на об'єкти критичної інфраструктури;

– активізовано двостороннє співробітництво в рамках механізму двосторонніх міжурядових кіберконсультацій із дружніми країнами (проведено подібні заходи із США, Великобританією, ФРН, Сінгапуром, Фінляндією) у сфері попередження та подолання наслідків атак на критичну інфраструктуру.

В умовах що склалися масштабні та систематичні посягання на українську критичну інфраструктуру засвідчили її недостатню, а інколи слабку, захищеність. Це змушує СБ України не лише виконувати власну місію – *протидіяти ворогу та нейтралізувати напади на національні інтереси у кіберсфері*, а й інколи безпосередньо здійснювати невідкладні захисні дії, допомагати у подоланні наслідків, сприяти у банальній організації кібербезпеки державних установ і приватних підприємств, які опинились один на один з професійно підготовленим, добре профінансованим та технічно забезпеченим ворогом.

Протягом останнього часу відчутно *зросла інтенсивність кібератак* на комп'ютерні мережі державних організацій, об'єктів транспорту та енергетики.

Першими наприкінці 2015 року потужних кібератак зазнали **о***б'єкти енергетичного сектору* нашої держави, зокрема, ряд регіональних енергетичних компаній. Широкого міжнародного резонансу зазначені атаки набули через те, що *чи не найперше у світі відбулась компрометація складних систем керування технологічними процесами або SCADA систем.*

Одразу на цей інцидент щиро відгукнулась та надала всебічне сприяння саме американська сторона. Особливо цінною виявилась практична допомога групи фахівців державних та приватних енергокомпаній США, які взяли участь у розслідуванні інцидентів безпосередньо в Україні пліч-о-пліч з працівниками СБУ.

В подальшому Сполучені Штати Америки не залишили Україну сама-на-сам із терористичними діями в мережі Інтернет проти нашої критичної інфраструктури. У вересні минулого року за результатами проведення перших українсько-американських кіберконсультацій урядом США оголошено масштабну програму допомоги у розбудові спроможностей України щодо протидії кіберзагрозам.

Крім того у лютому 2018 року року Палата представників Сполучених Штатів Америки ухвалила законопроект під умовною назвою «Співробітництво США з Україною у сфері кібербезпеки». Вказаний міжнародний нормативно-правовий акт, окрім зазначення найбільших кіберінциде-

нтів, що трапились в Україні та наголошенні на підтримки Сполученими Штатами незалежності та територіальної цілісності України, передбачає можливість надання США сприяння в розбудові дієвої системи кібербезпеки України.

Крім наших американських партнерів необхідно відзначити практичну допомогу представників уряду Великобританії у вигляді професійних тренінгів та високотехнологічного обладнання та програмного забезпечення, що дозволило значно посилити потужності України у сфері захисту національної критичної інфраструктури.

Розслідування вказаних кіберінцидентів показало, що зловмисники діяли свідомо не переймаючись про юридичні наслідки, професійно знищували сліди злочинного діяння, але головне – кібервтручання не мало корисливих чи інших мотивів, які зазвичай характерні криміналітету.

Окремі криміналістичні ознаки переконливо свідчили *про причетність до кібератак спецслужб Російської Федерації*, а постійна оперативна обізнаність проросійських ЗМІ лише утверджує нас у такому висновку.

Кібератаки російських спецслужб та підконтрольних їм хакерських угруповань на державні електронні інформаційні ресурси, об'єкти критичної інформаційної інфраструктури продовжились і дедалі набувають характеру *спланованої глобальної кібероперації, яка є невід'ємною частиною гібридної агресії* РФ як нової форми війни.

Для СБУ такий висновок вже очевидний:

По-перше, після анексії Криму і захоплення частини Донбасу цілком зрозуміло *кому це вигідно і хто фінансує* такі кібердиверсії. Більшість інцидентів, які ми детально розслідували, потребували значного фінансування, але окрім шкоди для України та іміджевих втрат не мали економічної доцільності ані для злочинців, ані для фінансово-промислових груп.

По-друге, практично всі кібератаки так чи інакше *завдавали матеріальних та іміджевих втрат державі*, в тому числі й психологічного тиску на українців. Атаки проводились за однаковими сценаріями, їх метою було блокування роботи інформаційних систем державних інституцій, а головне – досягнення негативного суспільного резонансу. При цьому, можливості зловмисників потенційно давали їм змогу спричинити більш негативні наслідки, водночас *перевага надавалась загостренню соціальних проблем.*

Насамкінець, *політично вмотивований вибір часу здійснення більшості кібератак,* як то – державні свята, значущі соціально-політичні події в Україні або напередодні прийняття на міжнародній арені важливих для українців політичних рішень.

В цьому контексті СБУ наголошує на готовності до співпраці в рамках Контртерористичної стратегіїї ООН та Резолюції РБ ООН 2341/2017 з представниками профільних служб держав членів ООН.

Зокрема в якості потенційних напрямків співробітництва українською стороною пропонуються наступні заходи:

– зняття перепон у напрямку міжнародного розслідування злочинів у кіберсфері, насамперед терористичних/кібератак шляхом налагодження механізму обміну необхідними документами, запитами тощо у режимі реального часу;

– опрацювання питання щодо заснування реально працюючої мережі цілодобових уніфікованих контактних пунктів, через які можна буде передавати не тільки інформацію про кіберзагрози, а й обмінюватися юридично-зобов'язуючими документами;

– доцільність дотримання країнами вже існуючих законодавчих механізмів (таких як наприклад Контртерористична стратегія ООН, Конвенція Ради Європи про кіберзлочинність) замість витрачання фінансових та людських зусиль на розробку нових міжнародних документів;

– проведення компанії підвищення обізнаності громадянського суспільства стосовно впливу терористичних атак на повсякденне життя шляхом створення, за сприяння Контртерористичної групи ООН, в країнах-членах спеціалізованих електронних ресурсів, публічно доступних в мережі Інтернет;

– підвищення освітнього рівня представників державних структур, відповідальних за протидію атакам на критичну інфраструктуру, шляхом створення, за сприяння Контртерористичної групи ООН, в національних освітніх закладах спеціальних навчальних програм підготовки/перекваліфікації фахівців у цій сфері.

**Література**

1) Контртерористична стратегія ООН [Електронний ресурс]. – Режим доступу: http://www.un.org/ru/documents/ods.asp?m=A/RES/60/288.

2) Щодо співробітництва СБ України з ООН у сфері забезпечення кібербезпеки та протидії кіберзагрозам. Доповідна записка., н.с. 130, т. 1, с. 216-218, 2018 р.

3) Резолюція РБ ООН 2341/2017 [Електронний ресурс]. – Режим доступу**:** https://daccess-ods.un.org/TMP/2655444.44322586.html.

*УДК 343.123*

**Ткачук Н. А.**
кандидат юридичних наук,
Національна Академія СБ України

## ПЕРСПЕКТИВИ РОЗВИТКУ НАЦІОНАЛЬНОГО КООРДИНАЦІЙНОГО ЦЕНТРУ КІБЕРБЕЗПЕКИ

2020 рік для України, як і для усього світу, несе нові виклики і загрози у сфері кібербезпеки. Цей рік має стати для нашої держави початком

інтеграції до світової спільноти, що в активному режимі буде працювати над створення колективної системи кібербезпеки світу.

Ключову роль у національній системі кібербезпеки займає Національний координаційний центр при РНБО України(НКЦК) як робочий орган Ради національної безпеки і оборони України.

Відповідно до Указу Президента України від 28 січня 2020 року № 27, внесені зміни в частині граничної чисельності працівників Апарату РНБО України (збільшено на 30 штатних одиниць) та розширені повноваження та завдання Національного координаційного центру кібербезпеки при РНБО України.

Внесення таких змін обумовлено необхідністю посилення спроможностей суб'єктів забезпечення кібербезпеки через координацію та організацію вирішення проблемних завдань.

Вводиться система координат та контролю у сфері забезпечення кібербезпеки.

Національний координаційний центр кібербезпеки бере на себе роль, у подальшому, як основного генеруючого центру ключових напрямів залучення сил та засобів у ході забезпечення національної кібербезпеки. Першим та головним принципом визначається не робота з виявлення, реагування на кібератаки та усунення їх наслідків, а робота на випередження.

Такий підхід передбачає оцінку наявного стану кіберзахисту, вироблення конкретних індивідуальних (для кожного суб'єкта окремо, враховуючи специфіку та наявні можливості) рекомендацій (завдань), усунення недоліків та проведення періодичного аудиту.

При цьому буде застосовуватися ризик-орієнтований підхід, який буде відповідати специфіці об'єкту (галузь, процеси автоматизації, розгалуженість ІТС) та наслідкам які можуть бути спричинені у разі деструктивного впливу на роботу його систем.

НКЦК забезпечує та реалізовує системний підхід до створення сучасного цифрового суспільства, яке не лише користується цифровими послугами, а й усвідомлює елементарні цифрові процеси, в яких воно задіяне. Лише так Україна досягне найвищого ступеню кіберзахисту.

Кібербезпека стає дедалі більш значущою частиною корпоративної і побутової культури, але низький рівень кіберграмотності співробітників державних органів чи підприємств будь якої форми власності визначається ключовим фактором майбутнього ландшафту кіберзагроз (лише 5% користувачів здатні виявити фішинговий електронний лист).

Отже національні програми з комп'ютеної грамотності (кібергігієни) за координації НКЦК повинні стати нормою на національному рівні.

Зловмисники постійно вдосконалюють способи, методи та технології несанкціонованого доступу до активів, що їх цікавлять,спрямовуючи свої дії не безпосередньо на власників активів, а на компанії що їх обслуговують (оператори основних послуг). Основна мета – отримання доступу до

систем оновлення програмного забезпечення активів та систем управління послуг провайдерів (провайдери цифрових послуг) для їх подальшої компрометації та розповсюдження через них ШПЗ.

Для підвищення спроможності кібербезпеки на національному рівні НКЦК прагне до реалізації європейської моделі створеної на основі мережі галузевих (секторальних) центрів (команд) реагування на кіберінциденти (SOC, CSIRT).

Реалізація такої моделі буде мати позитивний вплив та створюватиме сприятливі умови для роботи операторів основних послуг та провайдерів цифрових послуг.

На сьогодні при НКЦК вже створено кілька робочих груп щодо реагування на кіберінциденти до яких входять технічні фахівці державного та приватного секторів, і такий формат вже довів свою ефективність.

У поточному році добігає кінця термін дії чинної Стратегії кібербезпеки України прийнятої у 2016 році. Вона була критично необхідною у зв'язку із зростанням рівня загроз національній безпеці у кіберпросторі, пов'язаним із активним використанням країною-агресором кіберпростору для деструктивного впливу на об'єкти критичної інфраструктури та інформаційного простору України.

Цей документ став першою спробою нагального вирішення питань кібербезпеки під час гібридної агресії і сам факт його прийняття є позитивним та важливим з точки зору накопичення відповідного досвіду.

На сьогодні перед НКЦК стоїть важливе завдання - організація підготовки нової редакції Стратегії кібербезпеки України, що потребує оцінки ефективності вже здійснених заходів та аналізу проблем, які виникли у суб'єктів забезпечення кібербезпекипри реалізації чинної Стратегії.

Наступна Стратегія має стати якісним документом із довгостроковим плануванням та встановленими чіткими критеріями виконання (реалізації) завдань. Її положення будуть враховувати численні рекомендації експертів у сфері кібербезпеки, світові тенденції у напрямі прогнозованих кіберзагроз майбутнього, а також подальший розвиток нормативно-правової бази необхідної для системного і обґрунтованого підходу з вирішення нагальних проблем у сфері кібербезпеки.

**Література**

1. Закон «Про основні засади забезпечення кібербезпеки України» https://zakon.rada.gov.ua/laws/show/2163-19.

2. Рішення РНБО України від 27.01.2016 «Про СтратегіюКібербезпеки України» (введене в дію Указом Президента України від 15.03.2016 № 96) [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/n0003525-16.

3. Указ Президента України «Про Національний координаційний центр кібербезпеки» від 7.06.2016 № 242 [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/242/2016.

4. Указ Президента «Про рішення Ради національної безпеки і оборони України від 7 грудня 2019 року «Про невідкладні заходи з посилення спроможностей держави у сфері кібербезпеки» від 20.12.2019 № 923 [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/923/2019.

5. Указ Президента України»Про внесення змін до Указів Президента України від 27 січня 2015 року № 37 та від 7 червня 2016 року № 242» від 28.01.2020 № 27 [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/27/2020.

*УДК 343.123(477)*

**Ткачук Т. Ю.**
доктор юридичних наук, доцент,
Національна Академія СБ України

## ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ У СИСТЕМІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Нині у глобальному медіапросторі, в публіцистичних і наукових працях, а також у політичних і державних документах багатьох країн широкого вжитку набули терміни «інформаційна війна», «інформаційне протиборство», «інформаційний вплив», «інформаційна зброя» тощо. Інформаційно-комунікаційні технології (ІКТ) відіграють ключову роль у світовій політиці, економіці та системах безпеки. До інформаційних диверсій у кіберпросторі сьогодні вдаються як організовані групи, так і окремі особи. Дедалі важливішою складовою військового потенціалу держав стає інформаційна зброя (ІЗ) як доповнення до власне військового арсеналу. При цьому за своїми наслідками інформаційні війни між державами можуть бути не менш руйнівними і жорстокими, ніж традиційні. Утім, і в давні часи психологічна перевага над ворогом подеколи була важливішою за його фізичне знищення. Так, ще понад дві тисячі років тому згадуваний вище китайський воєначальник, стратег і мислитель Сунь-Цзи наголошував, що «*війна – це шлях обману*», а отже: «…якщо ти й можеш щось, показуй противнику, начебто не можеш; якщо ти й користуєшся чимось, показуй йому, начебто ти цим не користуєшся; хоча б ти і був близько, показуй, начебто ти далеко; хоча б ти і був далеко, показуй, що ти близько» [1, с. 88].

При цьому на міжнародному рівні дотепер відсутні загальноприйняті визначення терміна «інформаційно-комунікаційні технології» і пов’язаних з ним понять. Процес юридичного оформлення понятійного апарату сфери ІКТ у глобальному правовому просторі триває, і, оскільки метою спільних зусиль у зазначеному напрямі є узгодження численних термінологічних суперечностей, важливо простежити розвиток відповідної термінології в національних державних документах.

Розвиток досліджуваних нами питань пов'язаний з іменем професора Мартіна Лібіцкі, фахівця корпорації RAND (американський аналітичний центр, заснований 14 травня 1948 року в Санта-Моніка (Каліфорнія), вважається першим аналітичним центром у світі)[1]. У серпні 1995 року була оприлюднена його стаття «Що таке інформаційна війна?». Вже понад 20 років тому М. Лібіцкі писав, що психологічний вплив на противника під час військових дій використовується з давніх часів, проте у війнах нашої доби технічні методи і психологічні інформаційні операції мають однаково важливе значення й застосовуються в комплексі [2].

Успішне ведення інформаційної війни неможливе без масиву надійних специфічних даних про супротивника, зауважує професор Лібіцкі. Накопичення цих знань включає аналіз ЗМІ противника, оцінку впливу мас-медіа на прийняття рішень на державному рівні, детальне вивчення бюрократичного апарату країни, національної комунікаційної інфраструктури, особливостей програмного забезпечення систем управління і т. ін. У цих умовах ґрунтовна підготовка фахівців для кваліфікованого провадження інформаційних операцій на всіх їхніх етапах набуває винятково важливого значення. Придушення противника не є пріоритетом діяльності таких фахівців – їхня головна мета полягає в забезпеченні інтересів *своєї* держави.

Праці М. Лібіцкі, одного з найвпливовіших американських дослідників і теоретиків в інформаційній сфері, стали базисом для концепцій і стратегій збройних сил Сполучених Штатів, а також відповідних документів Міністерства юстиції США. Його наукові інтереси дотепер охоплюють специфіку застосування ІКТ у системі національної безпеки. Зокрема, цю проблематику Мартін Лібіцкі висвітлює у статті «Криза й ескалація в кіберпросторі», оприлюдненій 2012 року Корпорацією RAND [3].

Сьогодення постає перед Україною з новими викликами та надскладними завданнями. Під час опору різноплановим проявам гібридної війни, розгорнутої Російською Федерацією, стало очевидним, що наразі наша держава стикнулася з життєвою необхідністю захисту фундаментальних національних цінностей – незалежності, територіальної цілісності й суверенітету держави, свободи, прав людини й верховенства права, добробуту, миру й безпеки, – а також у стислі терміни має забезпечити ефективне функціонування сектору безпеки й оборони в умовах обмежених ресурсів. Стаття 17 Конституції України визначає, що «захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу» [4], що свідчить про набуття категорією «інформаційна безпека» в нормативно-правовому аспекті конституційного статусу.

[1] https://www.rand.org/.

**Література**

1. Сунь-цзы: Искусство войны: Древнейший в мире трактат о войне; пер. с кит., коммент., примеч. Л. Джайлса ; 2-е изд. Ростов-на-Дону : Феникс. 2003. 283 с.
2. Martin C. Libicki. Whatis Information Warfare? United States Government Printing, Washington DC, 1995. URL: http://www.dodccrp.org/files/Libicki_What_Is.pdf (дата звернення: 02.03.2020).
3. Martin C. Libicki Crisisand Escalationin Cyberspace. URL: https://www.rand.org/content/dam/rand/pubs/monographs/2012/RAND_MG1215.pdf (дата звернення: 02.03.2020).
4. Конституція України: Основний Закон України від 28.06.1996 № 254к/96-ВР. URL: http://zakon3.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80 (дата звернення: 02.03.2020).

*УДК 378:[001.3+004.72.056.52](477)*

**Уваркіна О. В.**
доктор філософських наук, професор,
**Гангал А. В.**
кандидат філософських наук
ІСЗЗІ Національного технічного
університету України «КПІ імені Ігоря Сікорського»і

## АКТУАЛЬНІ ПРОБЛЕМИ ОСВІТНЬОГО КІБЕРПРОСТОРУ

Сучасна інформатизація українського суспільства суттєво вплинула на всі складові системи вищої освіти, яка активно впроваджує інформаційні технології сучасності в науковий та навчальний процес з метою пошуку нових можливостей використання останніх досягнень у галузі електронних комунікацій для підвищення якості педагогічного процесу. На підвалинах інформатизації в умовах глобалізації у педагогічній науці сформувалось нове поняття «освітній простір», яке має різні смислові характеристики та відрізняється своєю багатомірністю [1, с. 107]. Найбільш розповсюджений серед науковців є територіальний підхід, якій визначає поняття «освітній простір» як єдність, цілісне утворення в галузі освіти, яке має свої межі. Наприклад, глобальний (світовий) освітній простір, міжнародний освітній простір або європейський освітній простір. Така характеристика освітнього простору пов’язана з інтеграційними процесами української освіти та створенням глобальної освіти у майбутньому.

Аналіз педагогічної реальності використання можливостей освітнього простору показує його пряму залежність від сучасних інформаційно-комунікаційних технологій. І якщо формальна вища освіта має ознаки спеціально організованого та захищеного інформаційного педагогічного середовища, то неформальна й інформальна освіта фактично залишаються

беззахисними об'єктами впливу під час використання мережі Інтернет або соціальних мереж і часто-густо потрапляють у пастки кіберзлочинців. На жаль, увага до проблем освітнього кіберпростору не дуже часто стає предметом наукових досліджень і потребує міждисциплінарного аналізу кіберзагроз в освіті.

У Законі України «Про основні засади забезпечення кібербезпеки України» (2017) визначено, що «кіберпростір – це середовище (віртуальний простір), яке надає можливості для здійснення комунікацій або реалізації суспільних відносин, що утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет або інших глобальних мереж передачі даних [2]». Відкритий та вільний віртуальний освітній простір дозволяє освітянам спілкуватися з колегами з різних країн світу, оперативно отримувати інформацію про сучасні наукові дослідження, брати участь у конференціях, симпозіумах на дистанційної основі та публікувати власні наукові досягнення у закордонних електронних періодичних виданнях.

Але віртуальна комунікація має бути захищеною, а робота у мережі Інтернет безпечною. Тому основною метою Стратегії кібербезпеки України, яка була затверджена Указом Президента України у 2016 році, є «створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави [3]».

Для реалізації цієї мети була створена Національна системи кібербезпеки, яка має забезпечити кіберзахист державних електронних інформаційних ресурсів, зокрема освітніх, та захистити інтереси людини у кіберпросторі. Відомо, що науковий потенціал українських науковців визнається та цінується світовими вченими у різних галузях знань, але для захисту національних інтересів держави у наукової галузі потрібно системне удосконалення принципів роботи в віртуальному інформаційному просторі, які б забезпечили захист наукових розробок, інтелектуальної власності на основі кращих світових практик і міжнародних стандартів з питань кібербезпеки та кіберзахисту.

Забезпечення захисту прав освітян, як користувачів комунікаційних систем є також одним із принципів основних засад забезпечення кібербезпеки в Україні. А своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз в українському освітньому кіберпросторі є необхідною умовою для сучасних наукових досліджень та їх реалізації в інтересах держави.

Таким чином, можна зробити висновок, що освітній кіберпростір – це віртуальний простір для здійснення комунікації суб'єктами та об'єктами освіти через систему електронних комунікацій з використанням мережі Інтернет або інших глобальних мереж передачі даних. Для захисту національних інтересів у галузі науки необхідна взаємодія з питань безпечного функціонування освітнього кіберпростору наукових установ, навчальних

закладів, науковці та освітян з Національною системою кібербезпеки. Тільки така взаємодія буде ефективною для розвитку освітнього кіберпростору, забезпечення захисту прав освітян у комукаційних системах та формуванню інформаційної компетентності та культури сучасного науковця.

**Література**

1. Касярум Н. Освітній простір: становлення поняття. *Витоки педагогічної майстерності.* 2013. Вип 12. С. 107-113.

2. Про основні засади забезпечення кібербезпеки України : Закон України від 5.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19.

3. Стратегія кібербезпеки України : Указ Президента України від 15.03.2016 № 96/2016. URL: http:// https://zakon.rada.gov.ua/laws/show/96/2016#n11.

*УДК 34.09+343.342*

**Фурашев В. М.**
кандидат технічних, наук,
старший науковий співробітник,
Національний технічний
університет України «КПІ імені Ігоря Сікорського»і

## ОСНОВНІ ПОКАЗНИКИ ЕФЕКТИВНОСТІ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ

Коли говоримо про управління інформаційною безпекою державою держави, то маємо на увазі створення таких умов, за якими унеможливлюється виникнення обставин, за яких процеси, що відбуваються в інформаційному просторі, не зможуть суттєвим чином впливати до погіршення або неможливості її функціонування і розвитку. Це, по-перше.

По-друге, необхідно постійно мати на увазі, що забезпечення інформаційної безпеки має дві взаємопов'язаних складових – охоронну та захисну.

Охоронна складова забезпечення інформаційної безпеки держави повинна здійснюватися законотворчою, правозастосовною та правоохоронною діяльністю.

З точки зору охоронної складової забезпечення інформаційної безпеки та правового регулювання суспільних відносин в частині поводження з інформацією, з формальних позицій начебто ситуація в країні більшеменше не погана. Є чималий законодавчий фонд правового регулювання суспільних відносин в частині поводження з інформацією, якій зорієнтоване саме на забезпечення інформаційної безпеки держави. Є також низка інших нормативно-правових актів – указів Президента України, постанов Кабінету Міністрів України, наказів центральних органів виконавчої вла-

ди, які спрямовані на вирішення цього питання. Біда лише в одному – всі ці законодавчі та інші регуляторні положення "розмити" по всім цим документам та іноді дублюють один одного, а також не надають цілісного погляду на цю сферу.

Щодо правозастосовної та, як наслідок і це – головне, правоохоронної діяльності у цій сфері ситуація зовсім інша. Можна сказати, що у сфері забезпечення реального втілення у життя суспільства правових норм поводження з інформацією, у переважної більшості, на жаль, не відбувається.

Такий стан можна пояснити лише одним – відсутністю цілісної державної інформаційної політики доступною та зрозумілою для пересічних громадян держави, а не лише для спеціалістів.

У Положенні про Міністерство культури, молоді та спорту України, затвердженим постановою Кабінету Міністрів України від 16 жовтня 2019 р.

№ 885 вказане, що "МКМС є головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику в інформаційній та видавничій сфері, а також забезпечує формування та реалізацію державної політики у сфері телебачення і радіомовлення, у сфері туризму та курортів (крім здійснення державного нагляду (контролю) у сфері туризму та курортів)" [1].

Але як можна зрозуміти та що можна подумати, коли у воюючої країні, причому, центр протиборства знаходиться саме в інформаційної сфері, навіть на формальному рівні відсутній орган центральної виконавчої влади, якій би відповідав за розробку та впровадження державної інформаційної політики або у його назві, хоч би формально, були присутні слово "інформація" або словосполучення "інформаційна політика".

Щодо захисної складової забезпечення інформаційної безпеки держави, яка спрямована на здійснення безпосереднього захисту інформації та інформаційної інфраструктури, то необхідно зауважити, що у даної сфері приділяється значно більше уваги ніж охоронної. Крім того, необхідно також відмітити, що дана складова забезпечення інформаційної безпеки держави значно менше піддається політичному впливу, що дуже суттєвим фактором.

Також необхідно акцентувати увагу на положенні ст. 17 Конституції України: "Захист суверенітету і територіальної цілісності України, *забезпечення* її економічної та *інформаційної безпеки* є найважливішими функціями держави, *справою всього Українського народу*" *(виделено автором)* [2].

Абсолютне вірне положення. Лише організаційно-адміністративними, нормативно-правовими, програмно-технічними та технічними шляхами та засобами, при всій їх важливості та ефективності, проблему ефективного вирішення питань досягнення належного рівня забезпечення інформаційної безпеки не вирішити. Необхідно, починаючи вже зі школи, вивчати основи інформаційної безпеки, а у вищих навчальних закладах це повинно

бути обов`язковою навчальною дисципліною. Це необхідно відобразити у державній інформаційної політиці.

Таким чином можна стверджувати, основними показниками ефективності системи управління інформаційною безпекою держави є:

– наявність цілісної державної інформаційної політики;

– ефективність законотворчої, правозастосовної та, саме головне, правоохоронної діяльності;

– ступеня обізнаності населення у шляхах та засобах забезпечення інформаційної безпеки людини, суспільства, держави.

**Література**

1. Положення про Міністерство культури, молоді та спорту України : Постанова Кабінету Міністрів України. URL: http://zakon2.rada.gov.ua.

2. Конституція України. URL: http://zakon2.rada.gov.ua.

*УДК 34.096 + 342.951*

**Харченко Н. П.**
кандидат юридичних наук,
Національна академія внутрішніх справ

## СТРАТЕГІЧНІ ПРАВОВІ АКТИ У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Національна безпека є важливим предметом дослідження як зарубіжних, так й вітчизняних дослідників. Особливо ця проблематика є важливою нині, що зумовлено довготривалою гібридною війною та затяжними військовими подіями на території України. Не дивно, що нормативно-правове регулювання суспільних відносин у сфері національної безпеки України є наразі доволі динамічним. Адже забезпечення національної безпеки базується на «…визначенні пріоритетів, завдань і заходів із забезпечення національної безпеки України, збалансованого розвитку складових сектору безпеки і оборони на основі оцінки безпекової обстановки та з урахуванням фінансово-економічних можливостей держави» [1].

Вагому роль в упорядкуванні суспільних відносин у сфері національної безпеки здійснюється за допомогою специфічних нормативно-правових актів: стратегій, концепцій, програм, планів тощо. Головною метою цих актів є окреслення концептуальних підходів, напрямів, заходів із забезпечення національної безпеки в конкретний історичний проміжок часу.

Попри актуальність, слід зауважити їх нерозробленість на доктринальному рівні. Адже нині відсутнє нормативне визначення не лише поняття таких актів чи їх особливостей, а й порядок ухвалення та введення в дію [2-3].

Неврегульованість на законодавчому рівні особливостей стратегічних актів призводить часто-густо до того, що одні стратегічні акти затверджуються підзаконними нормативно-правовими актами, інші ж – законами. Отже, юридична сила однакових за назвою правових документів значно різниться.

Навіть ретроспективний аналіз концептуальних нормативно-правових актів у сфері національної безпеки України демонструє неоднозначність розуміння важливості та особливостей тих чи інших стратегічних актів. Так, уперше основи національної безпеки України було урегульовано на рівні Постанови Верховної Ради України «Про Концепцію (основи державної політики) національної безпеки України» та лише у 2003 році на рівні закону.

Однак у жодному з цих актів не унормовувались концептуальні засади розробки, співвідношення, прийняття таких актів як доктрина, стратегія, програма тощо.

Лише нова редакція Закону України «Про національну безпеку України» від 21 червня 2018 року визначає концептуальні засади створення окремих важливих стратегій у сфері національної безпеки, як от: Стратегія національної безпеки України, Стратегія воєнної безпеки України, Стратегія кібербезпеки України, Стратегія громадської безпеки та цивільного захисту України, Стратегія розвитку оборонно-промислового комплексу України.

Визначено, що стратегії затверджуються указами Президента України, а також, що Рада національної безпеки і оборони України, враховуючи зміни в сфері безпеки, затверджує інші проекти стратегій та стратегічних документів [1]. Нині лише Стратегія громадської безпеки та цивільного захисту України не знайшла свого відображення в законодавстві України.

Аналіз змісту вищезазначених стратегій дозволяє дійти висновку, що здебільшого стратегії визначають основні напрями та завдання державної політики в конкретних сферах життєдіяльності суспільства, суб’єктів виконання, їх координацію і контроль. Стратегії також розробляються і затверджуються на чітко визначений проміжок часу. Зміни в державному та суспільному житті спричиняють зміни в цих документах, а тому вони мають доволі динамічний характер. Зокрема, у сфері національної безпеки і оборони України такі документи поділяються на довгострокові, середньострокові і короткострокові залежно від часу, на який ухвалюється конкретна стратегія. Стратегії мають діалектичний характер, оскільки взаємопов’язані з іншими стратегічними нормативно-правовими документами, наприклад, доктриною, концепцією розвитку того чи іншого кола суспільних відносин. Зміни в цих нормативно-правових актах обумовлюють трансформацію положень стратегій. Однак й стратегії також впливають на зміст інших нормативно-правових актів, які приймаються на підставі за-

твердженої стратегії. Стратегії у сфері національної безпеки України мають підзаконний характер, оскільки затверджуються указами Президента України.

Якщо зміст стратегій в сфері національної безпеки більш-менш визначено, то зміст доктрин є абсолютно не визначеним [4, с. 89], не говорячи про програми та плани.

Отже, стратегічні правові акти відіграють значну роль в упорядкуванні суспільних відносин сфері національної безпеки. Саме тому вважаємо за необхідне нормативно визначити співвідношення між різними стратегічними актами, а також особливості їх юридичної природи та змісту.

**Література**

1. Про національну безпеку України : Закон України від 21 червня 2018 року № 2469-VIII. URL : https://zakon.rada.gov.ua/laws/show/2469-19#n355 (дата звернення: 05.03.2020)

2. Харченко Н. П. Стратегические акты Украины: понятие и особенности. Legea Se Viata. 2020. № 3 (339). С. 89–94.

3. Харченко Н. П. Стратегічні правові акти в Україні: плюралізм наукових підходів. Науково-практичний журнал «Прикарпатський юридичний вісник». 2020. Вип. 4. С. 25–28.

4. Харченко Н. П. Доктрина как вид нормативно-правового акта. *Legea Se Viata*. 2019. № 7 (331). С. 89–94.

*УДК 355.40*

**Хоменко Л. В.**
Національний університет оборони України
імені Івана Черняховського

## ПРОБЛЕМИ ВИЯВЛЕННЯ НЕГАТИВНОГО ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ

З кожним днем роль інформації в житті людей стрімко зростає. Посилення ролі інформаційно-психологічного впливу, розширення можливостей використання засобів масової комунікації призводить до наслідків, які вкрай важко прорахувати. Інформаційний вплив на державу, суспільство, громадянина зараз є ефективнішим, ніж політичний, економічний і навіть військовий. Інформація стає реальною, майже фізично відчутною силою [1].

Інформаційно-психологічний вплив, який дедалі посилюється на всіх рівнях і сферах державного та військового управління, дає можливість стверджувати, що на сьогодні питання виявлення та оцінки є не лише актуальними, а й життєво необхідними для забезпечення інформаційної безпеки людини, суспільства та держави.

Проте існує ряд об’єктивних чинників, які впливають на процес виявлення негативного інформаційного впливу. Наприклад, в сучасних умовах інформаційні загрози національним інтересам в усіх сферах діяльності держави постійно кількісно та якісно змінюються. Окрім того, виявлення та оцінка негативного інформаційного впливу визначається багатьма умовами, які впливають на кінцевий результат. Зокрема, значні обсяги інформації про події та явища. Для того, щоб обрати найоптимальніший метод виявлення інформаційного впливу, варто оцінити завдання дослідження, доступні методичні підходи, і, звичайно ж, наявні ресурси та обмеження (час, фінанси, доступність інформації та ін.).

З огляду на значні обсяги інформації про події та явища, які генеруються об’єктами інформаційних відносин, оброблення інформаційних потоків ЗМІ, з метою виявлення ознак інформаційного впливу повинно мати постійний, упорядкований, науково обґрунтований характер, що можливо гарантувати лише за умови розробки методики виявлення ознак інформаційного впливу [2-3].

Сьогодні дослідниками запропоновано чимало методик, призначених оцінити потенційний вплив певної інформації. Накопичений методичний арсенал потребує упорядкування та осмислення, окреслення проблемних зон та перспектив подальших методичних пошуків [4].

Результативна протидія деструктивному інформаційному впливу повинна опиратися на ефективну систему моніторингу зовнішніх і внутрішніх інформаційних загроз, завдання якої – об’єктивно оцінити рівень цих загроз (і, відповідно, інформаційного впливу) для прийняття адекватних рішень щодо підвищення рівня інформаційної безпеки держави.

**Література**

1. Черешкин Д.С. Оружие, которое может быть опаснее ядерного // Независимая газета. – 1995. – № 123 с.

2. Левченко О.В., Косогов О.М. Методика виявлення заходів негативного інформаційного впливу на основі аналізу відкритих джерел // Системи обробки інформації. – 2016. – № 1 (138). – С. 100-102.

3. Сніцаренко П.М., Саричев Ю.О., Михєєв Ю.І., Праута М.В. Методичні основи виявлення та оцінки негативного інформаційно-психологічного впливу на особовий склад військ (сил) // Наука і оборона. – № 3-4. – 2017. – С. 18-25.

4. Фролов П.Д. Інформаційний вплив: теорія і практика прогнозування: монографія / за ред. П. Д. Фролова; Національна акад. пед. наук України, Ін-т соц. та політ. психології. – К.: Міленіум, 2011. – 304 с.

*УДК 004.681:342.742*
**Хорошко В. О.**
доктор технічних наук, професор,
Національний авіаційний університет
**Браіловський М. М.**
кандидат технічних наук, доцент,
Київський національний університет
імені Тараса Шевченка

# МОДЕЛЬ ВИЯВЛЕННЯ ТЕРОРИСТИЧНОЇ ГРУПИ НА ІНФОРМАЦІЙНОМУ ПІДПРИЄМСТВІ

Одним із завдань системи управління інформаційною безпекою є створення оптимальних умов для запобігання або ефективного розслідування посадових злочинів. У таких випадках умисні дії будь-якого з інсайдерів повинні бути однозначно встановлено і доведено [1].

Тому, доповідь присвячена актуальній темі побудови блоків злочинного механізму, розміщення терористичних груп (ТГ), дій ТГ і служби безпеки об'єкта, а також схеми функціонування автоматизованої системи попередження злочинів, як в інформаційному, так і кіберпросторі.

Запропоновані моделі повинні дати можливість аналізувати характер скоєних злочинів і терористичних актів, а також пропонувати реально діючі способи боротьби з витоком конфіденційної інформації.

На початку розглядаються основні складові злочинного механізму, якими є: мотивація, планування і виконання терористичного акту. Кожен з цих блоків механізму злочинної поведінки являє собою складне утворення, що включають різноманітні психічні стани і процеси, вплив зовнішнього середовища, прийняті людиною рішення і зворотні зв'язки.

В якості моделі порушника пропонується розглянути чотири варіанти ТГ, що класифікуються за їх розміщення:

1. ТГ не включає в себе персонал об'єкта.
2. Особи із зовнішнього середовища, пов'язані з персоналом об'єкта (група з боку є ініціатором і впливає на персонал).
3. Персонал об'єкта, пов'язаний з особами із зовнішнього середовища (персонал об'єкта сам виходить на зв'язок).
4. Персонал об'єкта.

У цьому варіанті схему дій ТГ і служби безпеки об'єкта можна представити у вигляді моделі (рис. 1).

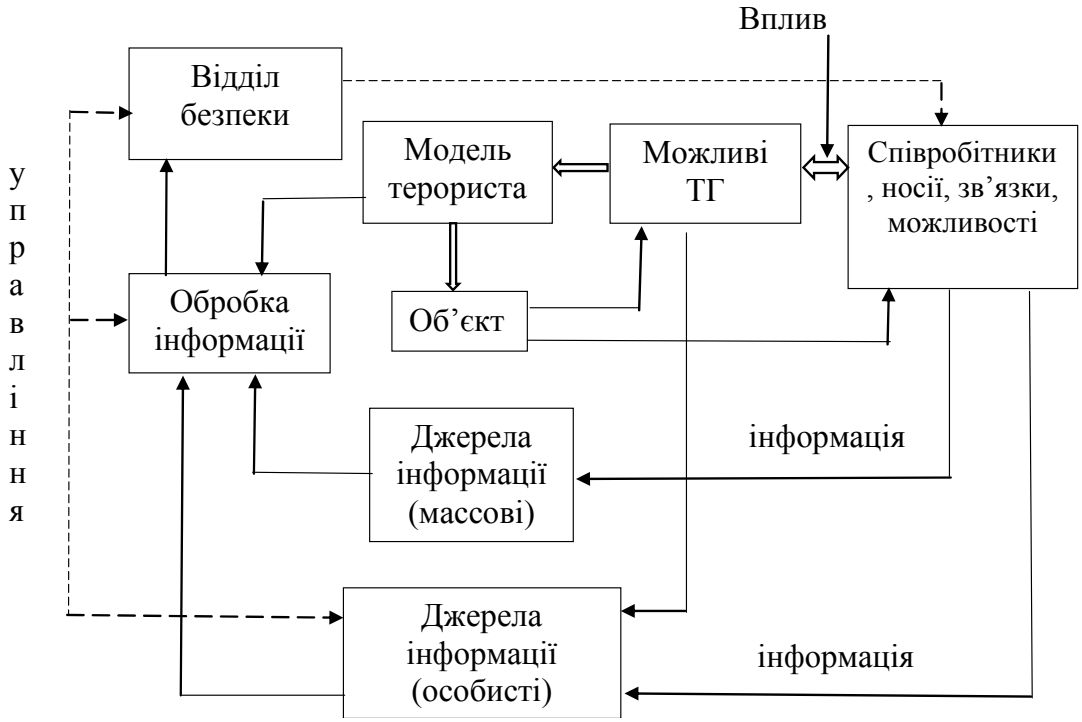


Рис. 1. Модель дії ТГ і служби безпеки об'єкта

Для реалізації описаної моделі дій ТГ і служби безпеки об'єкту пропонується схема функціонування автоматизованої системи попередження злочинів, яка дозволяє описати і проаналізувати розвиток можливих ТГ (рис. 2). Причому можливо розглянути динаміку розвитку групи і залучення в неї співробітників об'єкта для збільшення її професійної підготовки до вчинення злочину. Можливість залучення визначається ступенем взаємної зв'язку члена ТГ і співробітника об'єкта, можливістю впливу на нього і необхідності знань і умінь даного співробітника залучення в групу.

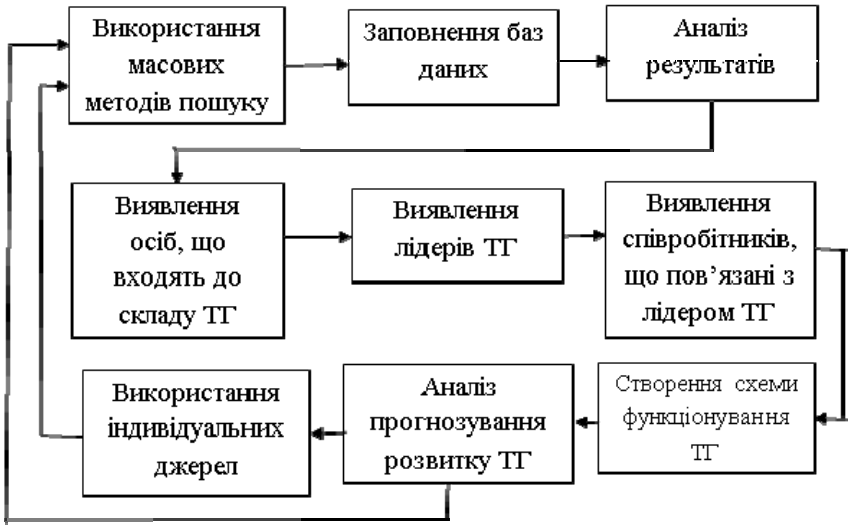


Рис. 2. Схема функціонування автоматизованої системи попередження злочинів

У разі залучення до групи нового члена, який необхідний ТГ для здійснення можливого злочину (терористичного акту), це є сигналом службі безпеки про можливе формування ТГ.

Пропоновані моделі дозволяють виявити терористичну групу, а також попередити злочин і зберегти інформацію.

**Література**

1. Кобозева А.А., Хорошко В.А. Анализ информационной безопасности. – Л.: Изд. ГУИКТ, 2009. – 251 с.

*УДК 004[056.53+413.4]*

**Цуркан В. В.**
кандидат технічних наук, доцент,
ІСЗЗІ Національного технічного
університету України «КПІ імені Ігоря Сікорського»і

## СПЕЦИФІКАЦІЯ ВИМОГ ДО СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Система управління інформаційною безпекою розробляється за встановленими вимогами забезпечення конфіденційності, цілісності та доступності інформації в організації [1]. Їх формалізоване описання представляється як специфікація. Для її відображення використовується діаграма вимог у графічній нотації SysML [2].

Цією діаграмою відображаються вимоги забезпечення інформаційної безпеки та співвідношення між ними. Насамперед [2], отримання, відновлення, задоволення, перевіряння, уточнення, копіювання, відстеження. Завдяки цьому встановлюється відповідність з елементами описання архітектури системи управління інформаційною безпекою. Як наслідок [1], враховуються інтереси зацікавлених сторін стосовно належності обробляння ризиків в організації.

Отже, специфікування вимог до системи управління інформаційною безпекою у графічній нотації SysML дозволяє, по-перше, встановити відповідність між ними і елементами описання архітектури означеної системи; по-друге, врахувати інтереси зацікавлених сторін.

**Література**

1. ДП “УкрНДНЦ”. (2015, Груд. 18). ДСТУ ISO/IEC 27001, Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT). Київ, 2016, 29 с.

2. SysML Open Source Project. URL: https://sysml.org/ (accessed on: 09.03.2020).

*УДК 355.40: 356.35*
**Цурко Ю. В.**
Національний університет оборони України
імені Івана Черняховського

# ОСОБЛИВОСТІ ВИЗНАЧЕННЯ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ОРГАНІВ ВІЙСЬКОВОГО УПРАВЛІННЯ

Через нерозвиненість нормативної бази в Україні існують суттєві розбіжності щодо розуміння різними суб'єктами поняття "загроза інформаційній безпеці".

У практиці збройних сил країн-членів НАТО поняття "інформаційна безпека" означає "захист інформації та інформаційних систем від несанкціонованого доступу, використання, розкриття, переривання (порушення цілісності), модифікації (зміни) або пошкодження (знищення) з метою забезпечення: а) цілісності, що означає захист від невідповідної зміни або пошкодження (знищення) та включає забезпечення повноти та достовірності (автентичності) інформації; б) конфіденційності, що означає захист санкціонованих (визначених) обмежень щодо доступу та розкриття інформації, включаючи заходи із захисту інформації про персональні дані та права власності; в) доступності, що означає забезпечення своєчасного та надійного доступу до інформації та її використання" [1, с. 94-95].

Загрози інформаційній безпеці, відповідно, полягають у можливості реалізації різного роду порушень, втручання або здійснення іншого негативного впливу на зазначені вище три елементи – цілісність, конфіденційність, доступність, які пропонується обрати у якості показників ефективності забезпечення інформаційної безпеки.

Крім того, існують три базові рівні інформаційної безпеки: рівень особи, суспільний рівень та державний (організаційний) рівень [2, p. 3], які відрізняються за своїм змістом та обсягом заходів із забезпечення безпеки.

Об'єднавши показники ефективності та базові рівні забезпечення інформаційної безпеки в єдиній матриці (табл. 1), стає можливим сформувати рамки, у межах яких проводити визначення загроз інформаційній безпеці, а у подальшому – оцінювати ефективність комплексу заходів з протидії цим загрозам.

Таблиця 1

Показники оцінювання ефективності та базові рівні забезпечення інформаційної безпеки

| | **Особа** | **Суспільство** | **Держава (організація)** |
|---|---|---|---|
| **Цілісність** | формування стійкості (критичного мислення) | боротьба з пропагандою; забезпечення свободи слова та плюралізму думок; формування сприятливого інформаційного простору | боротьба з пропагандою; формування сприятливого інформаційного простору |
| **Конфіденційність** | виховання інформаційної гігієни | | захист інформації з обмеженим доступом; протидія правопорушенням в інформаційній сфері |
| **Доступність** | | створення якісного інформаційного контенту; багатоканальність отримання інформації; незалежні ЗМІ | інформаційне забезпечення внутрішньої та зовнішньої політики |

Загальний порядок визначення загроз інформаційній безпеці органів військового управління Збройних Сил України наведено на рис. 1.

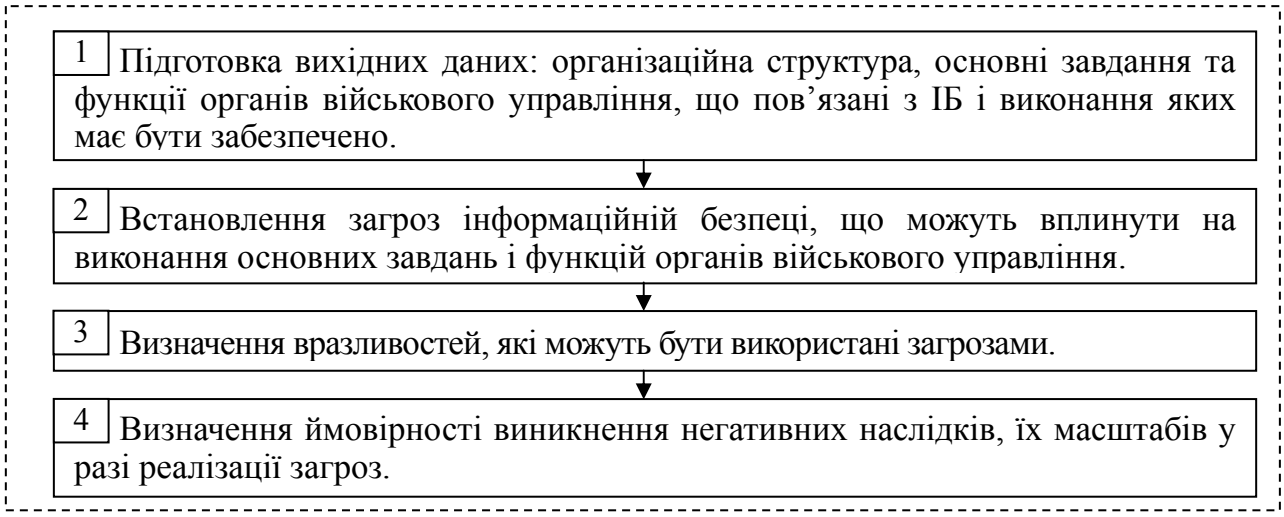


Рис 1. Порядок визначення загроз інформаційній безпеці органів військового управління ЗС України

На першому етапі за результатами оцінки умов обстановки, противника та своїх військ (сил) встановлюються та пріоритезуються загрози в інформаційній сфері. При цьому вихідними даними (блок 1) являються: політичні та військові цілі противника; загрози національній безпеці та похідні від них загрози в інформаційній сфері; сценарії, способи і форми реалізації загроз; спроможності противника, що він може використати для досягнення своїх цілей та реалізації загроз; організаційна структура органів військового управління; їх основні завдання та функції, що пов'язані із

забезпеченням інформаційної безпеки і успішне виконання яких має бути забезпечено.

На основі вихідних даних у блоці 2 встановлюються ймовірні загрози, які можуть вплинути на виконання органами військового управління критично важливих завдань і функцій. Для визначення характеру загроз використовується метод сценаріїв. Формулювання загроз має відповідати таким вимогам: бути конкретним; таким, що дозволяє виявлення, вимірювання та відслідковування їхніх проявів та змін.

У блоці 3 встановлюються вразливості, які можуть бути використані для здійснення впливу на функціонування органів військового управління у разі реалізації загроз.

У блоці 4 визначаються ймовірність виникнення та обсяги (масштаби) негативних наслідків у разі реалізації загроз інформаційній безпеці та проводиться відповідна пріоритетзація цих наслідків та пов'язаних з ними загроз. Кінцеві результати роботи заносяться до табл. 2.

Таблиця 2

Ймовірність виникнення та обсяги (масштаби) негативних наслідків у разі реалізації загроз інформаційній безпеці

| Загрози ІБ | Складові ІБ | Рівні ІБ | Органи військового управління | | | Оцінка ймовірності настання негативних наслідків | | Оцінка масштабів негативних наслідків | | Рейтинг негативних наслідків |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Назва | Основні характеристики впливу | Вразливості, що можуть бути використані | Характеристика | Оцінка | Характеристика | Оцінка | |
| (1) | (2) | (3) | (4) | (5) | (6) | (7) | (8) | (9) | (10) | (11) |

Для оцінки ймовірності та масштабів негативних наслідків розробляються оціночні шкали від 1 до 5, де 1 означає низьку ймовірність та відсутність негативних наслідків, а 5 – дуже високу ймовірність та масштабні наслідки. Для подальшої роботи обираються загрози, що мають найвищий рейтинг.

**Література**

1. NISTIR 7298, Revision 2, Glossary of Key Information Security Terms, Richard Kissel, URL: http://dx.doi.org/10.6028/NIST.IR.7298r2.

2. Указ Президента України Про рішення Ради національної безпеки і оборони України від 29.12.2016 №47/2017 "Про Доктрину інформаційної безпеки України".

*УДК 346.346.5.346.57*
**Чередниченко О. Ю.**
кандидат економічних наук, доцент,
Інститут підготовки юридичних
кадрів для Служби безпеки України
Національного юридичного
університету імені Ярослава Мудрого
**Козлова А. О.**
кандидат економічних наук,
Харківський національний університет міського господарства
імені Олексія Бекетова

# КАТЕГОРІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА КАТЕГОРІЇ «ІНФОРМАЦІЙНОЇ СИСТЕМИ» В СИСТЕМІ КОРПОРАТИВНОГО УПРАВЛІННЯ ПІДПРИЄМСТВ, ОРГАНІЗАЦІЙ ТА УСТАНОВ

Інформація є важливою складовою, предметом та продуктом діяльності сучасного суспільства. Загрози інформаційній безпеці стають все серйознішими і вагомішими, а засоби збереження, використання, передачі інформації стрімко змінюються. Захист ділової, фінансової, технологічної та іншої інформації від несанкціонованого використання, її зміни чи знищення набуває важливого значення серед вітчизняних підприємств, організацій та установ в період загострення конкурентної боротьби та нової хвилі світової фінансової кризи. Концептуальні та науково-методологічні основи інформаційної безпеки остаточно ще не розроблені. Тому для здійснення ефективного захисту «інформації» необхідно поділити «інформаційну безпеку» на категорії згідно яких впроваджувати певні засоби безпеки інформації.

З погляду інформаційної безпеки в науковій літературі виділяють 4 категорії інформаційної безпеки: конфіденційність, цілісність, автентичність, апелюємість. Але на нашу думку категорії інформаційної безпеки мають бути доповнені наступними категоріями: підзвітність та достовірність (рис. 1.1.)

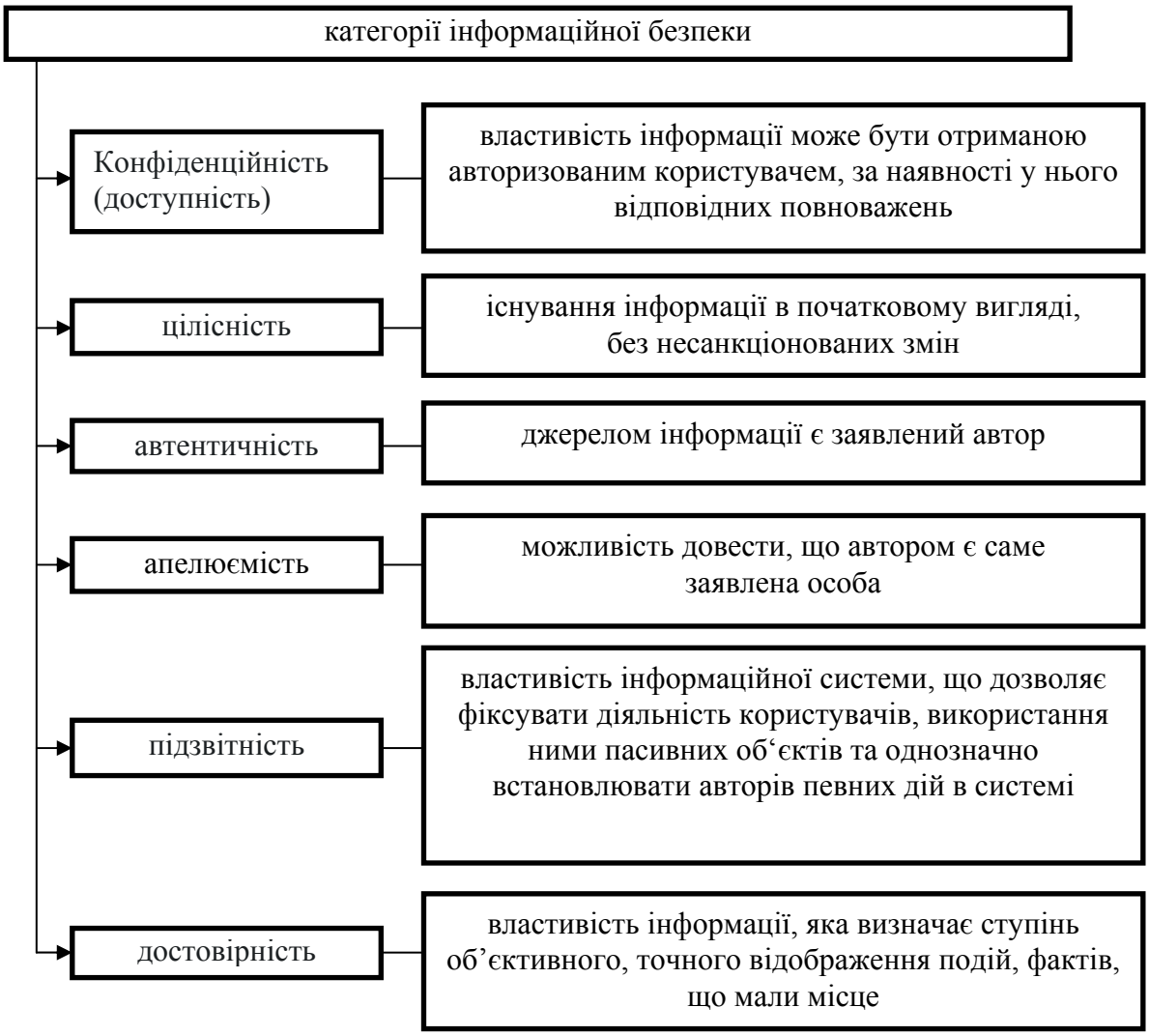


Рис. 1.1. Категорії інформаційної безпеки

Взаємозв’язок даних категорії дає змогу всебічно попереджувати витік інформації з підприємства чи організації, установи.

Для ефективного використання та захисту інформації вона має бути систематизована та пов’язана між собою. Як система управління інформаційна система, тісно пов’язується з системами збереження, видачі та обміну інформації в процесі управління. Вона охоплює сукупність засобів та методів, що дозволяють користувачу збирати, зберігати, передавати і обробляти відібрану інформацію. Інформаційні системи на підприємстві необхідні для організації інформації та ефективного управління всіма ресурсами, створення інформаційного та технічного середовища для управління діяльністю на підприємстві.

Будь-яка інформаційна система має відповідати наступним категоріям, які наведені у рис. 1.2.

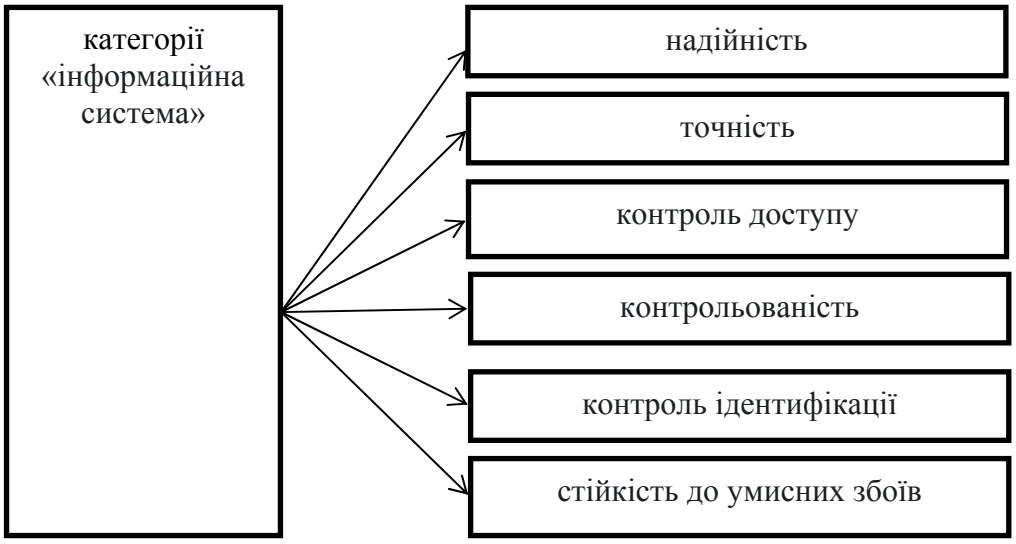


Рис. 1.2. Категорії «інформаційна система»

Таким чином, з урахуванням визначених категорій інформаційна безпека організації це цілеспрямована діяльність її органів та посадових осіб з використанням дозволених сил і засобів по досягненню стану захищеності інформаційного середовища організації, що забезпечує її нормальне функціонування і динамічний розвиток. Також, система заходів забезпечення безпеки підприємства має включати сукупність державно-правових, адміністративних, режимних заходів, організацію попереджувально-профілактичної роботи з персоналом, фізичну охорону об'єктів і працівників підприємства, впровадження технічних засобів захисту від промислового і комерційного шпигунства.

*УДК 316.625*
**Шемаєв В. М.**
доктор військових наук, професор,
Національної академії СБ України

## МОДЕЛЬ РЕФЛЕКСИВНОГО УПРАВЛІННЯ У МЕТОДАХ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА

Людина в будь-який ситуації зазнає впливу зовнішнього світу, який вона сприймає органами почуттів, відчуваючи його як реальність, що є об'єктом рефлексивних досліджень, що відображені у роботах А. Раппопорта, К. Поппера, Ю. Шрейдера, Дж. Адамса-Веббера, Л. Міллера, В. Лефевра. 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 безпеки набуває для України наукової та практичної актуальності.

Сприйняття реальності суб'єктом включає три рівні: неусвідомлюваний тиск зовнішнього світу (позначимо його змінною $a_1$), очікуваний тиск (сформований минулим досвідом, позначимо його змінною $a_{2,}$ ) а також інтенції суб'єкта у сформованій ситуації (позначимо змінною $a_{3)}$. Другий і третій рівні представляють суб'єктивне сприйняття самого себе в даній ситуації. Тому в сукупності ці два рівні характеризують самооцінку суб'єкта – "образ себе" у даній ситуації, який складається з психологічної настанови й інтенцій суб'єкта.

Учасники ситуації є активними суб'єктами, тобто досліджується суб'єкт–суб'єктна взаємодія (взаємне управління), але для визначеності вважаємо, суб'єкта ситуації, який здійснює управління – суб'єктом управління, суб'єкта ситуації, на якого спрямоване управління – об'єктом управління.

Готовність *i*-го суб'єкта ситуації до вибору типу поведінки при впливі на нього *j*-го суб'єкта може бути формалізованою за допомогою функції $A_{ij} = f(a_1, a_2, a_3)$, де всі змінні визначені на інтервалі [0,1]. Орган інформаційного управління має власний еталон поведінки об'єктів управління – вектор $\overline{A}$, при цьому основною керуючою змінною є $a_1$. Відповідні верхній та нижній "пороги тиску" визначимо $\breve{a}_1$ і $\hat{a}_1$.

Формальне завдання рефлексивного управління на даному етапі полягає у пошуку рішень задачі:

$$\rho(A - \overline{A}) \to \min,$$

де $A$ – вектор реальної готовності до вибору поведінки *i*-х об'єктів управління під впливом *j*-го суб'єкта управління, $i = 1, 2, 3, \ldots, n$;

$\overline{A}$ – вектор бажаної готовності до вибору поведінки *i*-х об'єктів управління під впливом *j*-го суб'єкта (еталон поведінки об'єктів управління з точки зору суб'єкта управління), $i = 1, 2, 3, \ldots, n$;

$\rho$ – норма збіжності між реальною і бажаною готовністю до вибору поведінки об'єктами управління, при обмеженнях: $0 \le \breve{a}_1 \le a_1 \le \hat{a}_1 \le 1;\ 0 \le \rho \le 1$.

Враховуючи суб'єктивність та приблизний характер даних, як метрики для розрахунку норми збіжності, можна обрати евклідову норму, тобто $\rho\left(A - \overline{A}\right) = \left\| A - \overline{A} \right\|_E = \frac{1}{n}\sqrt{\sum_{s=1}^{n}\left(a_i - \overline{a}_i\right)^2}$, використання більш точних метрик не є обґрунтовано.

Вирішення цього завдання на основі загальної формальної моделі рефлексивної взаємодії, яка включає обох суб'єктів з їх власними характери-

тиками, детально розглянуте у працях науковців. Підсумовуючи зазначено, систематизуємо вимоги до умов, за яких рефлексивне управління об'єктом буде дієвим:

1. У процесі прямої взаємодії з партнером необхідно дотримуватись толерантного стилю поведінки, виявляти готовність до компромісу, підтри-муючи у суб'єкта *A* завищені уявлення про ситуацію (вибір операції диз'юнкції).

2. Варто дотримуватись стратегії пошуку і задоволення загальних інтересів, а у випадку їх розбіжності дотримуватись стратегії зміни цільових настанов суб'єкта *A* и маскування власних цілей (вибір операції кон'юнкції).

Висновки, отримані формальним шляхом з аналізу моделі рефлексивного вибору, збігаються з принципами рефлексивного управління, які використовуються у військовій справі, політиці тощо. Це слугує підтвердженням правильності опису рефлексивних процесів запропонованими математичними моделями, що дозволяє використовувати їх у системах підтримки прийняття рішень у методах інформаційного протиборства.

Перспективою подальшого розвитку у даному напрямі є поєднання зазначеного підходу з механізмом цілепокладання, розроблення моделей вибору в умовах використання розгорнутої та швидкої форм рефлексії та дослідження можливостей щодо рефлексивного управління та програмування, коли вибір суб'єкта підпорядковується зовнішньому тиску, та моделей, які враховують образ іншого суб'єкта.

*УДК 351.86(477)*

**Шиповський В. В.**
Національний університет оборони України
імені Івана Черняховського

## ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ДІЙ У КІБЕРПРОСТОРІ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

Штучний інтелект (далі – AI (artificial intelligence)) як унікальний продукт технічного прогресу, через алгоритми програмного забезпечення надає змогу машинам вчитися, аналізуючи людський і власний досвід, пристосовуватися до нових умов в рамках свого застосування, виконувати різнопланові завдання, які тривалий час були під силу лише людині, прогнозувати події й оптимізувати ресурси різного характеру. Використання AI, відомі сьогодні охопило майже усі виробничі та невиробничі галузі діяльності людини – від комп'ютерів, що грають у логічні ігри, до автономних роботизованих систем, які застосовують провідні армії світу [1].

AI, який забезпечує захист мереж збирає у кілька разів більше інформації про мережевий трафік, звичайні протоколи протоколи (NetFlow, IPFIX). Інтерфейс веб-користувача надає всебічні дані та трафік в мережі. Для пошуку підозрілих подій в мережі у інтерфейсі представляються дані про з'єднання мереж, підмереж, користувачів та програм, рівні, індивідуальні потоки та їх зміст. Використовуючи передові методи штучного інтелекту, виявлення шкідливого програмного забезпечення не обмежується відомими загрозами, виявляючи ознаки шкідливої поведінки на найглибшому рівні. Шкідливі програми ідентифікуються на ранніх стадіях, зменшуючи час реагування на інциденти та запобігаючи подальшому заподіянню шкоди, а також зменшуючи загальний ризик. Щодо інтернету речей (IoT), AI самостійно перевіряє широкий перелік даних про мережеві потоки також на пристроях IoT і здатний ідентифікувати не тільки трафік на вході і виході з мережі, а також потоки зав'язків між пристроями всередині мережі; може виявляти такі типи аномалій, як аномальні пристрої, надмірний зв'язок одного пристрою з іншим або вузлом поза мережею, періодичну комунікацію, типову для сучасних постійних загроз. Замість застосування більш старого та обмеженого механізму опитування AI використовує перевірку на основі потоку та вмісту. Моніторинг на основі потоку забезпечує огляд в режимі реального часу (інтервали – 1 хвилина) статистики мережі та інших загальних та деталізованих питань. Глибокий огляд вмісту (DCI) розширює цю інформацію за допомогою комплексних контекстуальних метаданих у режимі реального часу (наприклад, ідентифікатора користувача, додатку) [2]. Генерація метаданих зав'язків мережі, забезпечує повне знання контексту – наприклад, призначення та джерела, ідентифікатора користувача та протоколу додатка. На відміну від технологій, заснованих на повному охопленні пакетів, це дозволяє зберігати метадані в мережевому трафіку значно довше із низькими вимогами щодо кількості місця для зберігання, що забезпечує потужну експертизу.

Отже, використання AI надає можливості виявлення загроз на основі сигнатур та здійснювати глибокий огляд пакетів, аналізувати поведінку мережі, спеціалізовані алгоритми, здійснювати моніторинг продуктивності мережі та моніторинг продуктивності додатків, забезпечуючи високий рівень кіберзахисту.

**Література**

1. Штучний інтелект: що це таке і чому це важливо? [Электронний ресурс]. Режим доступу:https://www.everest.ua/ai-platform/analytics/shtuchnij-intelekt-ai-shho.

2. Аналіз трафіку мережі [Электронний ресурс]. – Режим доступу: https://eset.ua.

*УДК 343.13*
**Школьніков В. І.**
Національна академія внутрішніх справ

# ІМПЛЕМЕНТАЦІЯ КОНВЕНЦІЇ ПРО КІБЕРЗЛОЧИННІСТЬ В УКРАЇНСЬКЕ ЗАКОНОДАВСТВО

Питання боротьби з кіберзлочинністю в Україні є одним із актуальних викликів, що стоїть перед нашою державою. За даними компанії Cisco у період з 2013 по 2018 роки світовий об'єм мобільного трафіку зріс майже в 11 раз та на сьогодні складає 15,9 ексабайтів. Окрім того, кількість підключених пристроїв до мережі Інтернет вже у 3,47 рази перевищує кількість населення світу, а у 2020 році прогнозується перевищення у 6,58 рази [1]. В даному контексті очевидним є збільшення кількості вчинення кіберзлочинів особами, для яких не існує територіальних обмежень в цифровому середовищі.

Верховна Рада України 7 вересня 2005 року ратифікувала Конвенцію про кіберзлочинність 2001 року [2]. Учасниками Конвенції є 44 європейських держави – членів Ради Європи та 20 держав, які не є членами Ради.

Згідно з положеннями Конвенції, Сторони надають одна іншій взаємну допомогу з метою розслідування або переслідування кримінальних правопорушень, пов'язаних із комп'ютерними системами і даними, або з метою збирання доказів у електронній формі.

Сторона може запитати іншу Сторону видати ордер чи іншим чином провести термінове збереження комп'ютерних даних, які зберігаються за допомогою комп'ютерної системи, яка знаходиться на території такої іншої Сторони, і відносно якої Сторона, яка запитує, має намір надіслати запит про взаємну допомогу щодо обшуку чи подібного доступу, арешту чи подібних дій або розголошення таких даних.

Закон України № 2824-IV від 07.09.2005 року «Про ратифікацію Конвенції про кіберзлочинність» набув чинності 01.07.2006 року, але станом на початок 2020 року кримінальне процесуальне законодавство України ще не відповідає положенням Конвенції про кіберзлочинність. В свою чергу, це ускладнює переслідування злочинців, державно-приватне співробітництво та міжнародну співпрацю під час боротьби з кіберзлочинністю.

З огляду на викладене, необхідно розробити відповідні зміни в чинне українське законодавство України. 11 грудня 2019 року при Комітеті Верховної Ради України з питань правоохоронної діяльності була утворена робоча група з метою підвищення ефективності досудового розслідування кіберзлочинів та використання електронних доказів. До складу робочої групи увійшли народні депутати України, представники Апарату Верховної Ради України, Ради Європи, Консультативної місії Європейського Союзу, аналітичного центру «Український інститут майбутнього», Офісу Генерального прокурора, Служби безпеки України, Національної поліції

України, Національної академії внутрішніх справ, Київського національного університету імені Тараса Шевченка, Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при РНБО України, приватного навчального закладу «Міжнародна кіберакадемія», Crime Stoppers NGO.

За результатами роботи було розроблено відповідні зміни в Кримінальний процесуальний кодекс України, Кримінальний кодекс України, Закони України «Про оперативно-розшукову діяльність», «Про телекомунікації», які стосуються:

1) надання можливості правоохоронним органам здійснювати термінове збереження інформації, що значно підвищить ефективність відслідковування та попередження вірусних атак на кшталт Not.Petya, WannaCry, кібератак на енергетичні компанії України (23.12.2015, 18.12.2016) із використанням троянської програми BlackEnergy тощо (імплементація статті 16 Конвенції про кіберзлочинність);

2) можливості у виняткових невідкладних випадках здійснювати тимчасовий доступ до інформації, яка знаходиться в операторів та провайдерів телекомунікацій, до постановлення ухвали слідчого судді, суду (імплементація статті 17 Конвенції про кіберзлочинність);

3) можливості під час проведення обшуку законним чином отримувати доступ до комп'ютерних систем, які фізично розташовані за межами місця проведення обшуку, долати системи логічного захисту, отримувати інформацію про особливості функціонування комп'ютерних систем та застосовані щодо них заходи захисту (імплементація статті 19 Конвенції про кіберзлочинність);

4) вдосконалення державно-приватної взаємодії правоохоронних органів та операторів телекомунікації під час проведення оперативно-розшукових заходів, негласних слідчих (розшукових) дій та тимчасового доступу до речей і документів;

5) посилення відповідальності за злочини у сфері авторського права та суміжних прав, злочини, визначені розділом XVI Особливої частини Кримінального кодексу України, а також за незаконні дії з платіжними документами, електронними грошима, у тому числі із віртуальними активами.

Імплементації Конвенції про кіберзлочинність в українське законодавство є важливим кроком, що сприятиме підвищенню ефективності боротьби з кіберзлочинністю, наслідком чого стане мінімізації негативного впливу цього явища на процеси, що відбуваються в суспільстві.

**Література**

1. Організована злочинність і правоохоронна система України. Резонанс: веб-сайт. URL: http://resonance.ua/organizovana-zlochinnist-i-pravookho / (дата звернення: 09.03.2020).

2. Про ратифікацію Конвенції про кіберзлочинність: Закон України № 2824-IV від 07.09.2005. Офіційний вісник України. 2005. 14 жовт.

# НАУКОВЕ МАЙБУТТЯ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ ОЧИМА МОЛОДИХ ВЧЕНИХ І СТУДЕНТІВ, КУРСАНТІВ

*УДК 35.355/359*

**Аметов Е. А.**
**Шемаєв В.М.,**
доктор військових наук, професор,
Національна академія СБ України

## МІФ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ ПРО ВИСОКУ ЕФЕКТИВНІСТЬ ЇХ ПРИВАТНИХ ВІЙСЬКОВИХ КОМПАНІЙ

В умовах сучасної інформаційної глобалізації дуже актуальним є питання впливу на свідомість людини шляхом розповсюдження фейкової інформації, іншими словами – розповсюдження міфів. Одним з таких є міф Росії про високу ефективність її приватних військових компаній.

Задля розгляду питання про міф РФ щодо високої ефективності власних приватних військових компаній, необхідно визначитись насамперед з тим, що таке приватна військова компанія (ПВК).

Під цим поняттям слід розуміти комерційне підприємство, яке пропонує спеціалізовані послуги, пов’язані з охороною, захистом (обороною) когось або чогось, нерідко це передбачає участь у військових конфліктах, а також збір розвідувальної інформації, стратегічне планування, логістику і консультування.

З’явилося це поняття приблизно у 1967 році у зв’язку із створенням першої у світі приватної військової компанії, що мала назву Wach Guard International засновником якої був полковник британської армії Девід Стерлінг.

До складу першої ПВК увійшли відставні офіцери і солдати зі спецвійськ Британії. З такою ж ініціативою виступили американці, після чого вже і російські колишні військовослужбовці.

Від початку створення і до теперішнього часу ПВК наймаються різними державами світу і організаціями для вирішення внутрішніх і зовнішніх проблем, які неможливо усунути власними силами з певних політичних, економічних або інших не менш важливих причин.

На сьогодні ми маємо рейтинг найпопулярніших ПВК світу, до яких входять американські: Academy (Blackwater), FDGCorp, DynCorp, MPRI; англійські: G4S, AegisDefenceService, ErinysInternational ті інші.

У зв’язку із відсутністю в таких списках Росії, її ЗМІ розповсюджують фейкову інформацію щодо власних ПВК, відносячи їх до самих ефек-

тивних і професійних компаній на ринку, з метою підвищення попиту та отримання авторитету.

У зв'язку з тим, що для існування приватних військових компаній відсутнє будь-яке правове забезпечення окрім проекту закону РФ «про оборону», якій в більшій мірі може в майбутньому застосовуватись лише з метою відвернення покарання для «нужних людей», політичні керівники та інші впливові фігури верхівки влади не мають можливості публічно вихвалювати власні ПВК із за незаконності їх існування і заперечують будь які зв'язки з ними, особливо питання щодо фінансування діяльності цих організацій.

Але для штучного підвищення популярності, своїх рейтингів і ринкової конкурентоспроможності, управлінська ланка використовує ЗМІ (телебачення, мережу інтернет, соціальні мережі), де розповсюджує фейкову інформацію про професіоналізм російських приватних військових компаній.

Основною інформацією виступають новини про нібито вдалі операції ПВК в Сирії, Африці та інших територіях, але це не є достовірною інформацією. Досліджуючи це питання, було з'ясовано, що в ході операцій в Сирії, російські ПВК незграбно втратили велику кількість співробітників,що повністю заперечує їх характеристиці як «непереможних».

Російські ЗМІ, шляхом проведення спеціальних інформаційних операцій, тобто комплексу заходів інформаційно-психологічного впливу на свідомість населення власної та інших країн формує в них позитивну думку про ПВК Росії та їх безмежну силу.

Також, не беручи до уваги принципи людськості, засоби масової інформації, нехтуючи правами людей, здійснюють для досягнення поставленої мети, маніпулятивний вплив, наслідком чого створюється бажання співпраці з самим ПВК або здійсненні іншої корисної для організації дії.

Виходячи з вище перерахованого можна дійти висновку, що весь авторитет приватних військових компаній Росії отримується лише за допомогою розповсюдження міфу про їх ефективність.

**Література**

1. fontanka.ru [Електронний ресурс]. – Режим доступу: https://m.fontanka.ru/2017/08/18/075/.

2. novayagazeta.ru. [Електронний ресурс]. – Режим доступу: https://novayagazeta.ru/articles/2019/07/28/81406-bez-schita.

3. regnum.ru [Електронний ресурс]. – Режим доступу: https://regnum.ru/news/polit/2736843.html.

4. lenta.ru [Електронний ресурс]. – Режим доступу: https://m.lenta.ru/news/2020/02/03/four/.

5. техэкспегт [Електронний ресурс]. – Режим доступу: http://docs.cntd.ru/document/9020348.

*УДК 35.078*
**Андросюк А. С.**
Національна академія СБ України

# РОЛЬ МАС-МЕДІА В ГІБРИДНІЙ ВІЙНІ ПРОТИ УКРАЇНИ

Нинішня війна Росії проти України, супроводжується широким спектром сил та засобів, що не притаманні класичній війні. Важливе місце у цій війні відводиться інформаційному протиборству. З'явилася нова назва «гібридна війна», в якій мас-медіа стали потужною зброєю у формуванні суспільної думки, що призводить до відчутних суспільних наслідків.

Варто зазначити, що перманентного інформаційного впливу в російських та проросійських ЗМІ Україна зазнавала задовго до подій 2014 року. Ще з 90-х років російські спецслужби інтенсивно вели «інформаційні війни» проти України. Україна зіткнулася з проблемою домінування російського капіталу в українських сферах телекомунікацій та інформатизації. Половина інтернет-ресурсів в Україні була під контролем росіян. Серед них мережі «Vkontakte» та «Одноклассники», які входять до складу «mail.ru», що безпосередньо пов'язані з ФСБ РФ. Крім цього, інтернет-ресурси «Правда.Ру» та «Российский диалог» поширювали фейки та певні стереотипи про Україну, на кшталт таким, як:

1. Україна – це частина Росії, і вона не може існувати без Росії. Українці є регіональною групою росіян, що має свій говір і територіальні особливості.

2. Української мови не існує. Чимало росіян вважають, що українська мова – це діалект, який утворився з російської.

3. Західна Україна – це «бандерівці», «укрофашисти», Львів – їх столиця.

4. Майдан – вияв агресії проти Росії. Повідомлялося, що у Києві, на Майдані, за гроші стоять «бандерівці» та «Правий сектор» з метою вбити якомога більше росіян та організувати повстання проти російського народу.

5. Української культури не існує. Окрім вишиванок, народних пісень і кількох письменників в українському культурному середовищі нічого немає. Іншими культурними надбаннями Україна має завдячувати СРСР.

6. Крим – це Росія. Проте Крим став частиною Росії лише у XVIII ст. У XIX ст. Росія програла війну за Крим Британії, Франції та Османській імперії, але Крим залишили у її складі за певні поступки. У 1954 році Крим увійшов до складу УРСР.

7. Українська армія вбиває мирне населення на сході України. Російські ЗМІ фальсифікують інформацію про Україну. Мешканці окупованих територій дезорієнтовані, відтак, спостерігається підтримка російської армії жителями сходу України. У багатьох росіян сформувалось вороже ставлення до українців.

8. Україна потерпає від кризи, тому жителі її тимчасово окупованих територій просять притулку в Росії. Пропагандисти активно поширюють інформацію про високу якість життя в Росії.

9. На півдні та сході України відбуваються масові напади української армії на церкви та синагоги. Цій пропаганді сприяють виступи у мас-медіа тих, хто творить і впливає на громадську думку: зірки естради та кінематографу (більшість з них знаходяться у переліку осіб, які створюють загрозу національній безпеці України, опублікованому Міністерством культури України), бізнесмени, чиновники та інші [2].

Уміло маніпулюючи українською аудиторією, російські мас-медіа дезорієнтують суспільство, висвітлюючи події в Україні так, як це вигідно Кремлю, ігноруючи етичні засади журналістики, застосовуючи дезінформацію.

Обмеженість населення сходу нашої держави у виборі вітчизняних мас-медіа призводить до сприйняття ними інформації, яку нав'язують їм «пропутінські» ЗМІ. При цьому піддаються пропаганді, оскільки, не маючи достовірної інформації, не можуть критично аналізувати ситуацію.

Мобілізувавши ЗМІ та проросійські медіа, країна-агресор активно спрямована на забезпечення влади президента В. Путіна й посилює вплив на своїх громадян та інформаційний простір України. Вони переконують наших громадян у необхідності дружби, співробітництва та стратегічного партнерства двох країн. А при здійсненні інформаційного впливу на своїх громадян російські спецслужби цілеспрямовано формують думку про недієздатність української держави, підігріваючи антиукраїнські настрої в російському суспільстві [3].

Внаслідок негативного інформаційного впливу Росії із застосуванням усього арсеналу мас-медіа Україна зазнає суттєвої шкоди інформаційній безпеці людини, суспільства та держави.

Серед цих негативних наслідків: 1) зростання кількості колабораціоністів; 2) неможливість забезпечення єдиного інформаційного простору України; 3) підрив іміджу нашої держави на міжнародній арені; 4) поширення сепаратистських настроїв.

Отже, назріла нагальна необхідність ведення виваженої інформаційної політики України щодо ефективної та проактивної протидії деструктивному інформаційному впливу агресора. З цією метою вітчизняні мас-медіа мають подавати правдиву, достовірну інформацію, зображаючи обидві сторони конфлікту, залучати своїх та іноземних експертів і фахівців для висвітлення реальних подій та виявлення маніпулятивних намірів агресора, підкріплювати інформацію перевіреними фактами, висвітлювати реальну мирну політику України та формувати її позитивний імідж на міжнародній арені.

**Література**

1. Ожеван М. Інформаційні війни: курс онлайн лекцій [Електронний ресурс] // Prometheus. – 2015. – Режим доступу: http://courses.prometheus.org.ua/courses/KNU/102/2015_T2/about.

2. Еляшевська Н. Ф. Вразливість України до інформаційної війни / Н. Ф. Еляшевська // Теле- та радіожурналістика. – Львів, 2015. – Вип. 14. – С. 165–168.

3. Будур І. М., Ракитянський С. В. Особливості інформаційної війни Російської Федерації проти України / І. М. Будур, С. В. Ракитянський. // «Науковий семінар ХНУ ПС ім. І. Кожедуба, 25.10.2018». – 2018. – С. 68-71.

*УДК 342.721*

**Білоус І. А.**
**Третяк Д. В.**
**Меленті Є. О.**
кандидат технічних наук,
Інститут підготовки юридичних
кадрів для Служби безпеки України
Національного юридичного
університету імені Ярослава Мудрого

## ОСОБЛИВОСТІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ СПІВРОБІТНИКІВ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

Глобальна мережа стала невід'ємною складовою сучасного суспільства. Сьогодні не можливо уявити повсякденне життя людини без використання глобальної мережі Інтернет, використання месенджерів, інформаційних технологій. Діджиталізація охопила майже всі сфери державного управління, надання соціальних послуг, фінансових операцій, медичного обслуговування та медійного контенту. Таким чином, в мережі Інтернет здійснюється збір, обробка, зберігання та цифрової інформації великих об'ємів. Проте поміж переваг створюються й передумови до збільшення кількості кіберінцидентів, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, зростає імовірність порушення штатного режиму функціонування об'єктів критичної інформаційної інфраструктури. Як визначено в [1], кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору. В умовах активної розвідувально-підривної діяльності спеціальних служб іноземних держав проти України постає питання з захисту персональних даних військовослужбовців і співробітників сектору безпеки та оборони, підвищення рівня підго-

товки зазначеної категорії осіб щодо кіберзахисту своєї персональної інформації.

Отже розробка практичних рекомендацій для співробітників Служби безпеки України щодо захисту персональних даних в мережі Інтернет є актуальним завданням.

В роботі представлено класифікацію кібератак, які здійснюються по відношенню до засобів електронних комунікацій (персональних комп'ютерів, ноутбуків, смартфонів). З метою збереження цілісності, конфіденційності й доступності персональної інформації співробітник має дотримуватись певних заходів безпеки при роботі з власними персональними даними. Наведено способи проникнення кіберзлочинця в мережі до персональних даних й наслідки таких зловмисних дій [2]. В доповіді наведені практичні поради щодо захисту засобів електронних комунікацій, створенню надійних паролів, особливості використання бездротової мережі WiFi. Розглянуті питання щодо надійного збереження даних, створення резервних копій та безповоротного їх видалення. Також вбачається доцільним поводити тренінги (курси) з основ кіберзахисту для військовослужбовців (співробітників) сектору безпеки та оборони України особливо перед виконанням службово-бойових завдань в районі проведення бойових дій.

**Література**

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовтня 2017 р. 2163-VIII / Верховна Рада України. URL: http://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 19.03.2020).

2. Академия Cisco. Введение в кибербезопасность. URL: http://685059869.netacad.com/courses/974895.

*УДК 342.1*

**Бова І. В.**
Національна академія СБ України

## СУДОВА ПРАКТИКА РОЗГЛЯДУ СПРАВ ЩОДО КРИПТОВАЛЮТИ

Нині існує понад тисячу різних криптовалют. Обіг цифрових валют неконтролюють ні уряди держав, ні банківські установи. Принципи,на основі яких функціонує криптовалюта, дають змогу здійснювати децентралізовані, безпечні й анонімні транзакції через мережу.

У 2015 році в Європі починає формуватися судова практика з питань правового режиму криптовалют. Так, Європейський суд справедливості в

результаті розгляду звернення в спорі між Девідом Хедквістом та податковою службою Швеції ухвалив рішення в справі С-264/14 від 22 жовтня 2015 року, у якому йшлося, що біткоін, найпоширеніша криптовалюта у світі, є не товаром, а виключно валютою – платіжним засобом. Рішення, яке схвалив суд, слід вважати революційним, адже воно стало першим кроком у забезпеченні цій криптовалюті майбутнього як альтернативи національним валютам. У судовому порядку криптовалюту біткоін було визнано повноцінним платіжним засобом, операції з яким не підлягають оподаткуванню. Отже, Європейський суд як вища судова інстанція ЄС уперше в історії існування європейського співтовариства своїм рішенням визначив біткоін на одному рівні з традиційними валютами. Таким чином, саме це прогресивне рішення посилило позиції криптовалюти, усунувши загрозу надмірного його оподаткування. Це слугувало вихідною позицією у вирішенні питання щодо правового режиму криптовалют у ЄС.

Відповідно до чинного законодавства України, поняття «криптовалюта» і регулювання операцій з нею не підпадають під режим регулювання обігу грошових коштів. Оскільки криптовалюта не існує в формі банкнот, монет, записів на рахунках в банках, вона не може бути визнана грошима в розумінні українського законодавства. Крім того, крипто валюта не є видом валютних цінностей в трактуванні валютного законодавства України. Криптовалюта і операції з нею не підпадають під режим регулювання обігу електронних грошей оскільки не випускається банком. Криптовалюта не може бути кваліфікована ані як гроші, ані як інші речі, ані навіть як майнове право вимоги, оскільки, по-перше, не є платіжним засобом і не імітується НБУ, по-друге, не має матеріального вираження, по-третє, не породжує права вимоги.

Судова практика в Україні з даного питання складалась дуже цікаво та неоднозначно. 30.01.2015 року в одній із своїх ухвал про тимчасовий доступ до речей Деснянський районний суд м. Чернігова, поміж іншого, зазначив, що випуск та обіг криптовалюти біткоін на території України заборонений.

13.10.2016 року, в Харківському окружному адміністративному суді розглядалась справа про скасування податкової консультації, згідно з якою операції з криптовалютою В рішенні суд встановив, що операції з обміну традиційних валют на біткоіни повинні бути вільні від податку на додану вартість. При цьому суд послався на те саме рішення Суду справедливості ЄС «Хедквіст проти Швеції» від 22.10.2015 року (ототожнивши цей суд із ЄСПЛ). В подальшому апеляційна інстанція підтвердила таку позицію та залишила рішення в силі.

На сьогодні, схожих рішень є велика кількість, судова практика у них є різноманітною та вбачається відсутність єдності судів не лише у підходах до оподаткування криптовалюти, а й до визначення її правового статусу.

Неможливо не звернути увагу на одну із справ слідчих Державної фіскальної служби, які намагалися «притиснути зловмисників», і вимагали від Солом'янського райсуду Києва надати тимчасовий доступ до документів громадської організації «Біткоіни Фундація України», яка, на їхню думку, нібито зберігає дані про клієнтів «грошової системи» біткоіни, а саме: ПІБ користувачів, адресні дані, контактні телефони, паспортні або інші персональні дані, договори, заяви на підключення.

Досудове розслідування проводилося за фактом фіктивного підприємництва та сприяння в ухиленні від сплати податків в особливо великих розмірах (ч. 5 ст. 27 ч. 3 ст. 212, ч. 2 ст. 205 КК України). «Зловмисники» використовували реквізити та поточні рахунки фіктивних підприємств, чим сприяли діючим суб'єктам підприємницької діяльності в умисному ухиленні від сплати податків. Підприємства, що мають ознаки фіктивності, з метою прикриття своєї незаконної діяльності використовували, як зазначає слідчий, електронну грошову систему «Біткоін», а саме електронний гаманець. Висновок про те, що громадська організація «Біткоін Фундація України» є офіційним представником біткоіну, слідчі зробили з «загальнодоступної інформації, що міститься в мережі Інтернет».Цікаво, що рішення суду з дозволом на обшук було вмотивоване тим, що правила випуску даної валюти не погоджені з НБУ і це порушує порядок використання електронних грошей на території України.

Негативне ставлення державних органів до криптовалюти має свої причини. Так, основна частина судових справ, де фігурує біткоін як спосіб платежу, стосуються продажу наркотиків, вимагання, заволодіння коштами з чужих платіжних карток, діяльності конвертаційних центрів, організації DDOS-атак і ін.

Наприклад, криптовалюта Біткоін використовувалася групою осіб з числа громадян України, Португалії та Швейцарії в міжнародній фінансовій схемі, спрямованої на заволодіння коштами українців. Зловмисники зареєстрували на території Великобританії підприємство Planet business management ltd, яке нібито розробило програмний продукт «Кайрос», і привернули велику кількість інвесторів (громадян України та іноземців), обіцяючи їм отримання надприбутків. В результаті велика частина коштів була виведена за кордон з використанням біткоінів.

Фігурує криптовалюта і в цивільних справах. Причому, як показала одна із судових справ, при виконанні роботи, що оплачується криптовалютою, навіть при підписанні договіру і акту, у разі виникнення спору щодо несплати за виконану роботу претензії залишаться без відповіді. Адже криптовалюта, на думку суду, не має ознак матеріального світу, тому не може бути об'єктом судового захисту. Так, 24 березня 2016 р Дарницький районний суд м. Києва розглянув справу, що стосується оплати біткоінами роботи програміста. Між Н. і Л. був укладений договір обміну

товару на роботи, згідно з яким Н. зобов'язався виконати роботи по розробці і створенню програмного забезпечення з передачею їх результатів Л., а Л. – передати йому за цю роботу визначену договором кількість цифрової продукції Bitcoin (товару) на загальну суму 10 тис. грн. Н. виконав умови договору – розробив і створив програмне забезпечення відповідно до технічного завдання, що підтверджується актом прийому-передачі виконаних робіт, однак відповідач біткоіни йому не передав.

Суд не погодився з позицією позивача про те, що до даних правовідносин застосовуються положення договору підряду, оскільки суб'єктний склад сторін не відповідає умовам зазначеного виду договору. На думку суду, до спірних правовідносин застосовуються положення договору міни (бартеру). Згідно з укладеним між Н. і Л. договором, товар – визначену договором кількість цифрової продукції Bitcoin, яка є предметом господарського обороту, вироблена в процесі майнінгу і об'єктивно виражена за допомогою комп'ютерного програмування у формі цифрових записів, облік якої ведеться колективно в публічній базі Blockchain невизначеною кількістю учасників по чітко заданому алгоритму. Як висновок, суд підкреслив, що відповідач не може передати позивачу те, що не має ознак матеріального світу, з цією позицією також погодився Апеляційний суд м. Києва.

Незважаючи на окремі рішення, в більшості рішень криптовалюта розцінюється українськими судами не як платіжний засіб, а як актив, а договір купівлі-продажу або поставки, де засобом платежу за товари (роботи, послуги) сторонами визначається криптовалюта розцінюються судами як договори міни. При цьому судами робиться акцент на тому, що Bitcoin не є річчю в розумінні ст. 179 Цивільного кодексу України та не має ознак матеріального світу, не є продукцією, не є майновими правами, не має індивідуальних ознак. А оскільки такий предмет договору не можна ідентифікувати, визначити його ознаки матеріального світу, суд приходить до висновку, що такий предмет не може бути об'єктом судового захисту. Таким прикладом може бути Рішення Дарницького районного суду м. Києва у справі № 753/599/16-ц від 24.03.16. При цьому суд посилається на Лист НБУ від 08.12.2014 № 29-208/72889, який був відізваний НБУ та приходить до висновку, що "Bitcoin є грошовим сурогатом, який не має забезпечення реальної вартості.

Майнінг в Україні правоохоронці прирівнюють до фіктивного підприємництва, а за наявності угоди купівлі-продажу криптовалюти долучають ще одну статтю Кримінального Кодексу України – легалізація доходів, отриманих злочинним шляхом.

Суди перебувають в стадії осмислення проблем, пов'язаних з використанням віртуальних валют (активів). На сьогодні в Верховній Раді зареєстровано 3 законопроекти, що передбачають визначення правового статусу

криптовалют та особливостей оподаткування з нею. Проте жодний проект на ставився у порядок денний на голосування.

Отже, чинне законодавство не дає можливості в повній мірі врегулювати усі правовідносини, які виникають. Таким чином, майнери та особи, які здійснюють купівлю/продаж чи обмін криптовалюти та бажають працювати в правовому полі не мають такої змоги та змушені на власний ризик керуватись загальними положеннями і необов'язковими рекомендаціями та роз'ясненнями. Судова практика показує, що законотворча діяльність в даній сфері є незавершеною та потребує невідкладного вдосконалення, що буде кроком назустріч покращенню інвестиційного клімату України та врегулюванню однієї із найбільш іноваційних сфер нашого життя.

*УДК: 35.355/359*
**Боярський М. О.**
**Воскобойніков С. О.**
кандидат педагогічних наук,
Національна академія СБ України

## СИТУАЦІЯ В АЗОВСЬКОМУ МОРІ В КОНТЕКСТІ ЗАГРОЗ НАЦІОНАЛЬНИМ ІНТЕРЕСАМ УКРАЇНИ

Вільний доступ у Азовське море та свобода пересування ними важливі для української економіки та безпеки. Сьогодні можливості України користуватися своїм правом на ресурси Чорного та Азовського морів, а також правом свободи навігації і пересування у власних морських водах є обмеженими. Регіон двох морів перетворився на простір домінування військової сили, нестабільності, занепаду регіонального економічного співробітництва та збільшення ролі співпраці у сфері безпеки. Становище України ускладнилося з появою низки нових загроз, пов'язаних з російською агресією, окупацією та мілітаризацією Криму. За цих умов не менш загрозливою для України стає відсутність комплексної морської політики, яка поєднувала б військову і цивільну складову.

Азовський регіон сьогодні став простором домінування сили. За другорядної ролі міжнародного права як гарантії безпеки лише держави з високою безпековою спроможністю (військова міць, без пекові союзи) здатні захистити власні інтереси. Такий стан речей цілком відповідає інтересам Росії. А оскільки саме Москва в даному випадку є провокатором хаотизації регіону, то стабілізації ситуації та повернення до відносин, що базуються на міжнародному праві не варто чекати у найближчому та середньостроковому періоді. До зміни політичної ситуації будь-які загальнорегіональні формати співпраці в економічній, гуманітарній сфері або в час-

тині захисту довкілля є безперспективними, оскільки не матимуть в своїй основі спільного інтересу. Натомість високий запит регіональних країн на безпеку змушує їх активно групуватися у безпекові альянси згідно спільного інтересу, а там де це тимчасово неможливо – розвивати двостороннє безпекове співробітництво.

Головною загрозою для України в Чорному морі сьогодні є агресивні наміри та дії Росії з подальшої дестабілізації південних регіонів України, початковим етапом чого може бути встановлення російського контролю за судноплавством. Додаткові ризики для України створює певна готовність країн ЄС до компромісу з Росією за рахунок інтересів України та міжнародна інституційна неспроможність в контексті конфлікту між Росією та Україною. Крим перетворився на "сіру зону", територію, на яку міжнародні організації (ООН, ОБСЄ тощо) не можуть потрапити, навіть маючи відповідний мандат. В умовах воєнного конфлікту з Росією Україна має завдання зі створення максимально сприятливого для себе клімату міжнародних відносин з іншими чорноморськими країнами як через двосторонні відносини, так і через багатосторонню співпрацю у різних форматах.

При цьому слід враховувати, пріоритет регіональної взаємодії та інтерес у чорноморських країн знаходиться сьогодні переважно у безпековій сфері. Україні в цьому контексті варто приєднуватися як до тих, які вже оформилися, так і пропонувати нові ініціативи. Також необхідно забезпечити належне правове і дипломатичне реагування на усі випадки правопорушень Росії в Азовському морі, включно з екологічними правопорушеннями (незаконна діяльність в Каркінітській затоці в порушення Рамсарської Конвенції 1971 р.) та з правопорушеннями в сфері Глобальної навігаційної супутникової системи. Україні також варто розглянути можливість ініціювання питання перегляду правил судноплавства по р. Дунай для військових суден не дунайських держав. В цьому контексті потребує перегляду статусу Росії як єдиної не дунайської країни-учасниці Дунайської комісії.

Враховуючи те, що силовий чинник має пріоритетний вплив на формування міжнародного порядку денного в Азовському регіоні, перед Україною стоїть завдання посилення своїх військово-морських спроможностей та збільшення військової присутності своїх союзників – НАТО та окремо США, Великобританії, Канади. Для руху на цьому напрямку необхідно з одного боку переконувати держави-члени НАТО у необхідності створення флотилії НАТО у Азовському морі, а з іншого – сприяти правовому режиму максимальної відкритості Азовського моря для військових кораблів нечорноморських держав.

Захист національних інтересів у Азовському морі потребує від України вирішення завдання із забезпечення безпеки морських шляхів, що ве-

дуть до українських чорноморських портів та реалізації своїх прав на освоєння чорноморського шельфу. В умовах воєнного конфлікту з Росією Україна має завдання зі створення максимального сприятливого для себе клімату міжнародних відносин з іншими чорноморськими країнами як через двосторонні відносини, так і через багатосторонню співпрацю у різних форматах. При цьому слід враховувати, що пріоритет регіональної взаємодії та інтересу чорноморських країн знаходиться сьогодні переважно у безпековій сфері. Україні в цьому контексті варто приєднуватися як до тих, які вже оформилися, так і пропонувати нові ініціативи.

**Література**

1. Переговори російського командування з екіпажами прикордонних кораблів РФ. 25 11 2018 : [аудіозапис, стенограма] // Генеральний штаб ЗСУ : офіційний канал на YouTube. – 26.11.2018.

2. Комітет ВР з нацбезпеки підтримав уведення воєнного стану // Цензор.нет. – 26.11.2018.

УДК 351.865

**Василишин В. Ю.**
Національна академія СБ України

## ОХОРОНА ДЕРЖАВНОЇ ТАЄМНИЦІ ЯК ОДИН З ПРІОРИТЕТІВ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Характерними рисами здійснення безпосередньої демократії є прозорість та вільний доступ суспільства до інформації. Однак законодавством передбачено, що не вся інформація може перебувати у вільному доступі, тому існують правові режими, що здійснюють захист відомостей розголошення яких може завдати шкоди національним інтересам держави. Одним з таких правових режимів є охорона державної таємниці.

Відповідно до Закону України «Про державну таємницю» [1] під поняттям «охорона державної таємниці» слід розуміти комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів, спрямованих на запобігання розголошенню секретної інформації та втратам її матеріальних носіїв. Законом також передбачено, що уповноваженим суб’єктом у сфері охорони державної таємниці є Служба безпеки України.

З початком анексії Криму та військових дій на сході України цінність інформації зросла в декілька разів. Різного роду пропагандистські кампанії та спеціальні інформаційні операції збоку РФ становлять серйозну за-

грозу національній безпеці України, тому інформаційна зброя є одним з чинників через який може здійснюватись несанкціонований витік таємної інформації. Наприклад, в грудні 2019 року СБУ блокувала витік таємної інформації з військової частини через програмне забезпечення на якому зберігалися матеріальні носії секретної інформації. Така інформація свідчить про те, що захист інформаційно-телекомунікаційних систем державних органів є досить уразливим від загроз та потребує подальшого вдосконалення на законодавчому та технічному рівнях.

Важливим елементом забезпечення охорони державної таємниці є налагодження міждержавних відносин з метою створення належної правової бази для взаємного захисту інформації, як такої доступ до якої обмежено. Міжнародне співробітництво надає змогу створити сучасну систему захисту державних секретів, яка відповідає найкращим світовим практикам та стандартам НАТО, постійно підписуються меморандуми, конвенції, тощо.

За статистикою органів СБУ станом на 2019 р. Україною підписано більше 50 міжнародних договорів у сфері захисту ІзОД та денонсовано одну угоду з Словацькою республікою у 2008 році та з Російською Федерацією у 2015 році.

Ще одним фактором, який впливає на стан забезпечення державної таємниці є питання допуску. Адже допуск громадян до цих відомостей передбачає низку обмежувальних заходів передбачених законодавством, що в свою чергу забезпечує відповідальність громадян-секретоносіїв з метою недопущення розголошення державної таємниці. Але зважаючи на це загроза розголошення державної таємниці існує постійно. Таким чином підрозділи Служби безпеки України, як спеціально уповноважені суб'єкти несуть відповідальність за стан функціонування державної таємниці в Україні, але належне функціонування неможливе без відповідального відношення інших суб'єктів, що провадять діяльність пов'язану з державною таємницею.

Отже, в Україні діє механізм охорони державної таємниці, який має на меті унеможливити витік державних секретів, забезпечити нормативне регулювання чинного законодавства та налагодження міжнародного співробітництва з країнами-партнерами. Нормативно-правовими актами визначено правовий статус державної таємниці та визначено перелік відомостей, що становлять державну таємницю. Проте, питання охорони державної таємниці в Україні досі залишається відкритим. Оскільки аналізуючи геополітичні події в нашій державі, що відбуваються впродовж останніх років, – захист державної таємниці є одним з ключових завдань забезпечення національної безпеки.

На нашу думку правовий режим державної таємниці в Україні в повній мірі забезпечує захист секретної інформації в різних сферах суспільс-

тва, однак постійно потрібно впроваджувати сучасні методи, які необхідні для належного захисту ІзОД, що в свою чергу слугуватиме зміцненню національної безпеки України.

**Література**

1. Про державну таємницю [Електронний ресурс]: Закон України № 3855-XII від 21.01.1994 р. - Режим доступу: https://zakon.rada.gov.ua/laws/show/3855-12.

*УДК 32.019.5*

**Веприк Ю. А.**
**Гринь А. К.**
кандидат технічних наук,
Національної академії СБ України

## ІНФОРМАЦІЙНІ ПРИЙОМИ ЩОДО ПРОПАГАНДИ «РУСЬКОГО МИРУ» НА ТИМЧАСОВО НЕКОНТРОЛЬОВАНІЙ УКРАЇНОЮ ЧАСТИНІ ТЕРИТОРІЇ ДОНБАСУ

У Росії є ціла низка інформаційних прийомів для зміщення уваги з війни – тобто, життєво-небезпечної проблеми, – на другорядні. А отже, запущені в український інформаційний простір, ці прийоми працюють і на зниження мобілізаційно-оборонної спроможності українців.

Як і дотепер, росіянам і далі свідомо чи несвідомо допомагатимуть окремі політологи, експерти, активісти, журналісти та інші агенти впливу. Ті, що свідомо, – за гроші чи ідею «руського миру».

Проаналізуємо відносно нові російські інформаційні розробки, які зараз або тільки починають обкатуватись, або ж запустять у найближчому майбутньому:

– вживання якнайчастіше у публічному дискурсі слова «мир» (хто проти миру, той за війну). Тут замовчуватиметься, який саме «мир» бачать. ЗМІ РФ постійно наголошуватимуть, що від війни страждають мирні люди, замовчуючи, безумовно, чому саме розпочалась війна, і хто саме її розпочав та постійно підживлює. Метою цього є зміна контексту сприйняття з необхідності тотальної оборонної війни до так званого миру;

– створення громадських «переселенських» організацій, щоб сформувати так званий «голос Донбасу». Вони масовано заходитимуть у громадські ради відповідних міністерств (як, наприклад, зараз у ситуації з Міністерством тимчасово окупованих територій, де до громадської ради увійшла низка дуже сумнівних громадських організацій, які або з’явились нещодавно, або взагалі не мають відношення до проблематики Донеччини та Луганщини).Такий «голос» також важливий і для ймовірного залучення й

перерозподілу європейських коштів на відновлення Донбасу. Контрольований із Росії «голос Донбасу» відрізнятиметься від справжнього голосу українського Донбасу, який сформувався і викристалізувався на Донецькому й Луганському ЄвроМайданах, і який виніс основний тягар мітингів за Україну на початку російської окупації. Мета цього – зробити окрему ідентифікацію «переселенців» для того, щоб ті, хто переїхав, не розчинялись у загальноукраїнському контексті. Посіяти сумнів: «можливо, Україна реально когось на Донбасі дискримінувала?», сіяти протистояння між Заходом і Сходом;

– наголошення на стандартах ВВС в Україні (це коли медіа, яке їх застосовує, бере участь у російській інформаційній кампанії, давати місце в українському медіа-просторі відкритій російській пропаганді (згадаймо ефіри про «секретні тюрми СБУ»). ЗМІ РФ постійно наголошуватимуть на так званій небезпеці (чому?) мілітаризації суспільства. У закликах до українізації почнуть наголошувати на радикалізмі. Мета цього – зробити російську пропаганду цілком легальною в українському інформаційному просторі, посіяти сумніви у журналістів: «а чи не забагато ми показуємо військових?...»;

– окремо слід виділити протидію зовнішньому та показному патріотизму, який зріс після Революції Гідності. Власне, на будь-який показний елемент патріотизму, наприклад, на вимогу спілкуватись українською у закладах харчування, навішуватимуть ярлики. Мета цього – показати патріотів як неадекватних осіб, які «неконструктивні» і лише зациклені на національних чи патріотичних питаннях;

– створення недостовірних соціологічних опитувань, де «правильно» поставлені питання даватимуть заздалегідь визначений результат. Так, нещодавно одна з громадських організацій зі Сходу України опублікувала дослідження, де респондентів запитували, чи погоджуються вони, що в разі повернення до України окупованих територій вчителям треба зберегти їхні робочі місця. Мета цього – метод легітимізації необхідних РФ тез, що буде легітимізувати тези й надавати в ефірах модних політичних токшоу «беззаперечний» доказ того, що так нібито думають українці;

– при обговоренні покарання для російських колабораціоністів, це буде подаватиметься як бажання помститись, що це радянська практика», «у них не було вибору, і тому вони працювали на росіян». Метою є: сприяння тому, щоб громадяни України сумнівались у необхідності не допуску до державних та державотворчих посад людей, які працювали на РФ;

– розмови про необхідність поступок для миру. По Мінських домовленостях – треба провести на окупованій території вибори (...бо це, принесе «мир»). І, відповідно, у разі можливої реінтеграції чи то визволення окупованих Росією територій, треба зберегти частину управлінців на місцях. Мета цього – легітимізувати й просунути в державні органи українсь-

кої влади на звільнених територіях людей, які працювали на російський окупаційний режим. Ці місцеві управлінці-колабораціоністи, насаджені російською зброєю, повинні стати узаконеними керівниками Донеччини та Луганщини після війни.

Очевидно, наведеними вище прикладами і ймовірними сценаріями росіяни не обмежаться. Вони будуть долучати нові можливості й нові сили у своєму бажанні скорити Україну. Арсенал росіяни постійно оновлюватимуть і трансформовуватимуть.

**Література**

1. Віталій Овчаренко, публікація від 2018-09-19.

2. Володимир В'ятрович. https://blogs.pravda.com.ua/authors/viatrovych/5c77ed7f557c8/.

3. Український Інститут Національної Пам'яті. Стаття від 27.02.2019 https://uinp.gov.ua/informaciyni-materialy/viyskovym/do-5-richchya-vid-pochatku-zbroynoyi-agresiyi-rosiyskoyi-federaciyi-proty-ukrayiny.

*УДК: 35.355/359*

**Гончаров П. О.**
**Сидоренко С. М.**
Національна академія СБ України

## МІФ РОСІЙСЬКОЇ ВЛАДИ ПРО НЕПРИЧЕТНІСТЬ ДО ТРАГЕДІЇ ЗІ ЗБИТИМ МАЛАЙЗІЙСЬКИМ ЛІТАКОМ «БОЇНГ-MG17»

Катастрофа, яка сталася 17 липня 2014 року на сході Донецької області (Україна), в районі збройного протистояння між урядовими силами і формуваннями невизнаних Донецької і Луганської Народних Республік за кількістю загиблих стала найбільшою в історії авіації за період з 11 вересня 2001 року і увійшла в десятку найбільших авіакатастроф за всю історію (9-е місце). Вона стала найбільшою авіакатастрофою XXI століття і на пострадянському просторі. Ця подія стала однією із основних тем, яка обговорювалася в соціальних мережах і ЗМІ. Версій винних у скоєнні цього діяння було дві – Україна і Росія. Остання, у свою чергу, незалежно від існуючих фактичних обставин, почала вводити в оману всю міжнародну спільноту.

9 вересня 2014 року опубліковано перший попередній звіт міжнародної комісії з розслідування авіакатастрофи. Остаточні результати розслідування причин аварії літака Boeing 777 під Донецьком очікувалися в другій половині 2015 року.

5 березня 2015 року низка українських ЗМІ, посилаючись на Генпрокуратуру Нідерландів, опублікували інформацію про те, що літак рейсу MH17 був збитий ракетою «Бук», запущеної з російською установки, і, швидше за все, російським екіпажем. Першоджерелом інформації виявилося голландське видання NOS, яке оповідало про хід розслідування. У звіті Bellingcat, організації, яка займається розслідуваннями військової тематики за відкритими джерелами, говорилося, що 17 липня 2014 року ракетну установку «Бук» з російської 53-ї зенітно-ракетної бригади, що базується під Курськом, провезли за маршрутом Донецьк-Сніжне. Потім вона була вивантажена з трейлера і доїхала своїм ходом до поля на південь від Сніжного, де приблизно о 16:20 вечора випустила ракету «земля-повітря», що збила рейс 17 Малайзійських Авіаліній. Вранці 18 липня ракетну установку «Бук» провезли по Луганську і далі через кордон з Україною.

Альтернативні сценарії, представлені Міністерством оборони Російської Федерації і концерном «Алмаз-Антей» являють собою навмисні спроби ввести громадськість в оману за допомогою сфабрикованих доказів.

23 лютого 2016 року група Bellingcat опублікувала нову доповідь, в якій назвала підозрюваних в атаці на MH-17. Зокрема, група заявляла, що «Бук», який збив літак MH-17, доставили до українського кордону бійці другого дивізіону 53-ї зенітно-ракетної бригади з Курська; до катастрофи були причетні близько 20 російських військових. Також Bellingcat спростувала російську версію катастрофи MH17.

23 лютого 2016 року група Bellingcat оприлюднила результати розслідування, в якому показано командну вертикаль – імена командирів, відповідальних за збиття пасажирського лайнера від президента РФ Володимира Путіна до командувача 53-ї зенітно-ракетної бригади Сергія Мучкаєва. Окрім них, було встановлено коло військовослужбовців бригади, що могли брати безпосередню участь у виконанні наказу: командир 2-го батальйону, 3 командири батарей та 10 командирів установок «Бук».

19 червня 2019 року прокуратура Нідерландів на основі розлідування Об’єднаної слідчої групи (JIT) пред’явила звинувачення у справі про збиття літака рейсу MH17 на Донбасі в 2014 році чотирьом підозрюваним терористам: росіянам Ігорю Гіркину (Стрєлкову), Сергію Дубінському, Олегу Пулатову і громадянину України Леоніду Харченку. Українські спецслужби внаслідок операції на території «ДНР» затримали підозрюваного Володимира Цемаха, колишнього «командира ППО» міста Сніжне, який може фігурувати у справі по катастрофі MH17 на Донбасі. Нідерланди визнали Цемаха підозрюваним у катастрофі MH17.

16 липня 2019 року Верховний представник Ради Європи від імені Європейського Союзу закликав Росію визнати відповідальність за катастрофу малайзійського «Боїнга» над Донбасом влітку 2014 року, співпрацю-

вати з проведеним розслідуванням а також висловив свою повну впевненість в незалежності і професіоналізмі правових процедур».

Уповноважена міжнародна слідча група досягла успішного розслідування, полагаючись на фактичні данні, які вказали на причетність РФ до цієї катастрофи.

Отже, за результатами проведеного дослідження здійснена спроба щодо розвіювання міфу РФ про непричетність до трагедії зі збитим Боїнгом МН17 на підставі фактів розслідування різних міжнародних уповноважених органів, не зважаючи на вплив на свідомість та підсвідомість суспільства з боку РФ за допомогою різних засобів ЗМІ.

**Література**

1. https://ru.wikipedia.org/wiki/Катастрофа_Boeing_777_в_Донецкой_области.
2. https://news.liga.net/incidents/news/delo-mn17-chto-izvestno-o-tragedii-chetyre-goda-spustya.
3. https://tsn.ua/special-projects/mh17/.
4. https://www.radiosvoboda.org/a/28025471.html.

*УДК 327.316*

**Гордієнко Л. О.**
Воєнно-дипломатична академія
імені Євгенія Березняка

## СПІВРОБІТНИЦТВО УКРАЇНИ ТА ВЕЛИКОБРИТАНІЇ У СФЕРІ ІНФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ

Співробітництво в галузі інформаційної безпеки – невід'ємна складова політичної, військової, економічної, культурної та інших видів взаємодії України та Великобританії.

Сполучене королівство є одним з ключових суб'єктів міжнародної інформаційної безпеки та має значний потенціал у цій сфері. Ще у 2010 році тодішній британський міністр оборони Нік Харві наголошував на зростаючій актуальності кіберзагроз та закликав уряди всього світу розробити закони, що регулюють використання кіберпростору. Виступаючи в Королівському інституті міжнародних відносин, він зазначив, що питанням часу залишається систематичне використання терористами кіберпростору не тільки як засобу комунікації для своїх власних організацій, але і як методу атак [1].

У листопаді 2011 року британський уряд опублікував першу Національну стратегію кібербезпеки [2]. З 2016 року в Сполученому Королівстві діє оновлена п'ятирічна стратегія, в якій кібератаки визнані найбільшою загрозою національній безпеці в усіх її сферах, включаючи економіку [3].

В урядовому документі сформульована амбітна мета – зробити Великобританію невразливою до сучасних загроз в цифровому середовищі, а британські ініціативи – моделлю для глобальних зусиль кіберзахисту. В рамках нової стратегії у 2016 році був створений Національний центр кібербезпеки (National Cyber Security Centre), в завдання якого увійшла реалізація програми "Активний кіберзахист" (Active Cyber Defence) [4].

Згідно з даними міжнародного Індексу кібербезпеки за 2018 р Великобританія зайняла перше місце в рейтингу з 193 країн світу, які роблять найбільш ефективні заходи інтернет-захисту [5].

Сполучене Королівство надає суттєву пряму та опосередковану підтримку Україні у боротьбі з російською агресією. Британський уряд неодноразово звертав увагу міжнародного співтовариства на агресивні дії в кіберпросторі з боку РФ, в тому числі на причетність російських спецслужб до "справи Скрипалів". В рамках розслідування цієї справи, у жовтні 2018 року Національним центром кібербезпеки Великобританії представлено дані про те що атаки здійснені з метою завдати шкоди як звичайним громадянам, так і державним структурам і міжнародним організаціям. Зазначається, що Росія демонструє своє небажання слідувати нормам міжнародного права, а за допомогою незаконної діяльності в інтернеті прагне впливати на політичні процеси в інших державах [6].

У серпні 2019 року в британських ЗМІ оприлюднені дані про створення спеціального підрозділу британської армії, в завдання якого увійшла боротьба з гібридними загрозами і кібератаками з боку РФ та різних терористичних угрупувань [7].

Україна проводить активне співробітництво та постійні консультації з урядом Великобританії у сфері протидії кіберзагрозам [8].

За ініціативи Лондона протидія інформаційним і кібератакам – одна з провідних тем у двосторонньому діалозі не тільки з Україною, але й з іншими країнами Східної Європи. Співробітництво з Великобританією у сфері інформаційної та кібербезпеки відкриває для України широкі можливості для забезпечення національної безпеки та використання переваг політичної підтримки за рахунок британської санкційної політики.

**Література**

1. Defence minister Nick Harvey to detail UK cyber battle plans. URL: https://www.infosecurity-magazine.com/news/defence-minister-nick-harvey-to-detail-uk-cyber/.

2. UK Cyber Security Strategy 2011. URL: https://www.gov.uk/government/publications/cyber-security-strategy.

3. UK National Cyber Security Strategy 2016 to 2021. URL: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021.

4. Active Cyber Defence. URL: https://www.ncsc.gov.uk/blog-post/active-cyber-defence-tackling-cyber-attacks-uk.

5. Global Cybersecurity Index (GCI) 2018. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf. P. 62.

6. UK exposes Russian cyber-attacks. URL: https://www.gov.uk/government/news/uk-exposes-russian-cyber-attacks.

7. Cyber Warfare: Army Deploys Social Media Warfare Division To Fight Russia. URL: https://www.forbes.com/sites/zakdoffman/2019/08/01/social-media-warfare-new-military-cyber-unit-will-fight-russias-dark-arts/#252850a64f6e.

8. Україна і Великобританія посилять співпрацю в області кібербезпеки. 19.03.2018. URL: https://www.ukrinform.ua/rubric-technology/2424940-ukraina-i-velikobritania-posilat-spivpracu-v-oblasti-kiberbezpeki.html/.

*УДК 351.746.1 + 004.9*

**Горьовий Д. В.**
Національна академія СБ України

## КІБЕРВІЙНА – КОМП'ЮТЕРНЕ ПРОТИСТОЯННЯ У ПРОСТОРІ ІНТЕРНЕТУ

У добу новітніх інформаційних технологій кіберпростір стає середовищем, в якому все частіше відбувається протиборство між суб'єктами міжнародних відносин. Термін «кібервійна» широко використовується в повсякденному житті, але сьогодні не існує загальноприйнятого й вичерпного визначення цього поняття. Відправною точкою для визначення терміну «кібервійна» доцільно вважати трактування війни у класичному розумінні цього слова. З огляду на це, кібервійну можна визначити як комплекс ретельно спланованих і скоординованих суб'єктами міжнародних відносин кібератак деструктивного характеру на (критичну) інформаційну інфраструктуру супротивника, з метою послаблення позицій об'єкта впливу та досягнення політичних, економічних та військових цілей.

Так, основні напрями. Спрямована передусім на дестабілізацію комп'ютерних систем і доступу до інтернету державних установ, фінансових та ділових центрів і створення безладу та хаосу в житті країн, які покладаються на інтернет у повсякденному житті. Міждержавні стосунки і політичне протистояння часто знаходить продовження в інтернеті у вигляді кібервійни: вандалізмі,пропаганді, шпигунстві, та безпосередніх атаках на комп'ютерні системи та сервери.

Український професор міжнародного права О. О. Мережко визначає кібервійну так: «кібервійна» – використання Інтернету й пов'язаних з ним технологічних і інформаційних засобів однією державою з метою заподі-

яння шкоди військовій, технологічній, економічній, політичній та інформаційній безпеці та суверенітету іншої держави.

Як визначив експерт з безпеки уряду США Річард А. Кларк, в своїй книзі «Кібервійна» (англ. CyberWarfare)[3] (вийшла в травні 2010) «кібервійна – дії однієї національної держави з проникнення в комп'ютери або мережі іншої національної держави для досягнення цілей нанесення збитку або руйнування». Американський журнал Економіст (англ. The Economist) описує кібервійну як «п'яту область війни, після землі, моря, повітря і космосу».Про важливість готовності до ведення військових дій в кіберпросторі свідчить факт створення в США цілого військового підрозділу – Кіберкомандування США.До кінця 2011 р 12 держав світу офіційно заявили про існування у них IT-служб, призначених для ведення не тільки оборонною, а й наступальної кібернетичної війни

На тлі Російсько-української кібервійни Президент України указом № 242 від 7 червня 2016 року створив Національний координаційний центр кібербезпеки. На центр покладена відповідальність за аналіз стану кібербезпеки, готовності до протидії кіберзагрозам, фінансового й організаційного забезпечення програм і заходів із забезпечення кібербезпеки, прогнозування й виявлення потенційних і реальних погроз у сфері кібербезпеки, участь в організації й проведення міжнаціональних і міжвідомчих кібернавчань і тренінгів

Основні види кібервійн: наступальна та захисна.

Спеціалісти виділяють такі види атак в інтернеті: вандалізм – використання хакерами інтернету для паплюження інтернет сторінок, заміни змісту образливими чи пропагандистськими зображеннями; пропаганда – розсилка звернень пропагандистського характеру, або вставка пропаганди в зміст інших інтернет сторінок; збір інформації – зламування приватних сторінок чи серверів для збору секретної інформації чи її заміни на фальшиву, корисну іншій державі; відмова сервісу – атаки з різних комп'ютерів для унеможливлення функціонування сайтів чи комп'ютерних систем; втручання в роботу обладнання – атаки на комп'ютери, які займаються контролем над роботою цивільного чи військового обладнання, що призводить до його відключення чи поломки; атаки на об'єкти критичної інфраструктури – атаки на комп'ютери, які забезпечують життєдіяльність міст, їх інфраструктури, таких як телефонні системи, водопостачання, електроенергії, пожежної охорони, транспорту тощо.

Прикладом кібератаки на об'єкти критичної інфраструктури можна назвати російську кібератаку на енергетичні компанії України в грудні 2015 року. Оскільки на той час тривала Російсько-українська війна, а метою кібератаки було саме виведення енергетичної системи з ладу, а не шпигунство чи викрадення грошей, деякі дослідники, такі як Мікко Хіпонен з фірми F-Secure вважають даний випадок першим справжнім прикладом кібервійни.

Характерні риси. З поширенням комп'ютерних технологій та інтернету багато громадян, підприємств і державних установ почали залежати від інтернетного зв'язку у повсякденному житті. Використання інтернету для атак комп'ютерних систем іншої держави може завдати значної шкоди її економіці і створити розлад у повсякденному житті країни. На відміну від кібератак минулого зараз кібервійна являє собою загрозу для національної безпеки країн і сприймається багатьма як серйозна загроза безпеці держави.

Крім того, розвідувальні організації багатьох країн займаються шпигунством використовуючи інтернет: збирають інформацію, зламують комп'ютерні системи інших держав, займаються диверсійною діяльністю та економічним шпигунством. За визнанням спеціалістів, лідерами у веденні кібервійни зараз є Китай та Росія. Зокрема Китай звинувачували у організації атак на сайти Сполучених Штатів, Німеччини, Індії. Росія використовує інтернет не тільки для збору інформації, але й для організації масованих атак на недружні країни. Росія, як і Китай, однак заперечують причетність державних установ до організації атак.

Під час російсько-української війни, що розпочалась з анексії Криму в 2014 році, інформаційно-обчислювальні системи України ставали об'єктами атак з боку Росії.

Під час президентських виборів в Україні 2014 фахівцями Ситуаційного центру забезпечення кібербезпеки СБУ спільно з CERT-UA було знешкоджено атаки на автоматизовану систему «Вибори». За декілька днів до проведення виборів ця система була повністю виведена з ладу. Відповідальність за це взяла на себе проросійська група хакерів Cyber-Berkut. Згодом СБУ отримала дані що до цього причетна група хакерів відома як APT-28, яка використовувала шкідливе програмне забезпечення SOFACY. Декілька діб із залученням фахівців приватної компанії Датагруп тривала напружена робота з відновлення повністю виведеної з ладу системи. З метою демонстрації світу причетності до цього втручання саме спецслужб Росії, фахівці СБУ залишили один з виявлених «сюрпризів», попередньо його знешкодивши. І ця пастка, але вже для російських спецслужб спрацювала. Увечері 25 травня було отримано інформацію про те, що на російських телеканалах анонсували новину про нібито виграш Дмитра Яроша на «президентських перегонах». З метою підтвердження цієї інформації на російському ТБ була продемонстровано картинку, яку в мережі вже назвали як «Картинка Яроша». 25 травня, о 20:16:56 було зафіксоване перше звернення до веб-сайту ЦВК виключно за IP-адресою внутрішнього веб-сервера з вказівкою в GET-запиті повного шляху до картинки «result.jpg» з IP-адреси 195.230.85.129. Ця адреса входить до діапазону IP-адрес телеканалу ОРТ.

23 грудня 2015 року сталась перша у світі підтверджена атака, спрямована на виведення з ладу енергосистеми: російським зловмисникам вдалось успішно атакувати комп'ютерні системи управління в диспетчер-

ській «Прикарпаттяобленерго», було вимкнено близько 30 підстанцій, близько 230 тисяч мешканців залишались без світла протягом однієї-шести годин. Атака відбувалась із використанням троянської програми BlackEnergy.

16 березня 2016 Президент України підписав указ, яким увів в дію рішення Ради національної безпеки і оборони України від 27 січня «Про Стратегію кібербезпеки України». У концепції зазначається: «Економічна, науково-технічна, інформаційна сфера, сфера державного управління, оборонно-промисловий і транспортний комплекси, інфраструктура електронних комунікацій, сектор безпеки і оборони України стають все більш уразливими для розвідувально-підривної діяльності іноземних спецслужб у кіберпросторі. Цьому сприяє широка, подекуди домінуюча, присутність в інформаційній інфраструктурі України організацій, груп, осіб, які прямо чи опосередковано пов'язані з Російською Федерацією».ізму на Говерлі, сайти Євразійського союзу молоді, який взяв відповідальність за їхнє проведення, були атаковані з України.

У зв'язку з розвитком нових технологій рівень кібервійни постійно вдосконалюється. Деякі держави починають приділяти захистові від кібервійни належну увагу – виділяють необхідні кошти для організації систем захисту і підтримують спеціальні підрозділи, основною задачею яких є вдосконалення інтернетної безпеки країни та захисту від нападів.

*УДК 351.746*

**Гребенюк В. М.**
доктор юридичних наук
**Данилків Д. Я.**
Національна академія СБ України

## ГІБРИДНА ВІЙНА РОСІЙСЬКОЇ ФЕДЕРАЦІЇ ПРОТИ РЕСПУБЛІКИ КАЗАХСТАН: ОСОБЛИВОСТІ ІНФОРМАЦІЙНОЇ КОМПОНЕНТИ

Республіка Казахстан – країна зі значним ресурсним потенціалом, вигідним геополітичним положенням табагатовекторною зовнішньополітичною стратегією. На жаль, вказані потенціал та положення керівництво Російської Федерації в їх інформаційних кампаніях схильне розглядати окремо від самої країни. Вони представляють для Кремля об'єкт для завоювання та включення в підконтрольну систему сил та засобів,необхідну для неоімперського реваншу. Зрозуміло, що за таких умов самостійність та багатовекторність казахстанців лише заважає, а тому підлягають інформаційним дискредитації та нівелюванню.

На цьому тлі особливо актуальним стає розвиток українсько-казахстанських стосунків, обмін досвідом та знаннями про те, як не допу-

стити повторення апробованих країною-агресором сценаріїв гібридної війни, керованого хаосу, агресивних інформаційно-пропагандистських операцій, які ведуть до сепаратизму, коштують багатьох життів та політично-економічної стабільності. Справа у тім, що ті ж вихідні умови, які «дратують» Кремль та «штовхають» його до вторгнення в межі суверенної держави, притаманні й Україні …

Російська Федерація у таких випадках традиційно обирає деструктивний шлях«очорнення» країни-жертви, нарощування військової присутності й «захисту російськомовного населення». Що стосується РК, то РФ не влаштовує зміна парадигми в геостратегічному середовищі Казахстану в Центральноазійському регіональному вимірі. Реакцією Москви, як і у випадку з Україною та іншими країнами, що обрали шлях незалежності, залишається формування комплексу викликів та загроз національній безпеці в умовах штучно провокованої геополітичної нестабільності.

Така політика РФ щодо наших країн – справа не одного десятиріччя. Зокрема, вироблення необхідної ідеології для казахстанського народу охоплює тривалий період, який можна умовно розбити на етапи: російська експансія в Казахстані (1465-1731 рр.);приєднання Казахстану до Росії та його подальша інкорпорація (1731 р. – середина XIX ст.); удосконалення ідеологічної основи російської експансії в Казахстані (XX ст.).

Як результат, сьогодні казахи (за аналогією з українцями) вважаються російським науково-експертним середовищем «відсталим народом», приреченим на архаїзацію у випадку розриву стосунків з «русским миром», а їх території нібито є «исконнорусскими».

Проте, уточнює ці судження геополітичне значення Республіки Казахстан, сформоване для Російської Федерації, яке заперечує «переживання» росіян з приводу можливого занепаду казахів. Повторимося нагадавши, що РК представляє для цієї країни всього лише: потенціал та ресурси, необхідні для включення в імперський арсенал боротьби за світове лідерство; транзитний шлях, призначений для транспортування товарів РФ; південні кордони новоявленої Російської імперії. А от якщо казахстанська держава не погодиться з цим, то опиниться в «дузі глобальної нестабільності», яку сам Кремль, мабуть, і створить.

«Незгода» Казахстану з російським диктатом вже фіксується вченими та політиками РФ на рівні зближення цього лідера Центральної Азії з Китайською Народною Республікою, Сполученими Штатами Америки, Тюркським союзом, а також в площині розвитку патріотичного вектору розвитку РК.

Як і у випадку з Україною, яка теж обрала багатовекторність як основний принцип зовнішньої політики, пішла на зближення з Європейським Союзом, у Казахстані розвивається військова присутність Російської Федерації. Як правило, військові бази РФ на території інших держав (не лише України, алей, для прикладу, країн Балкан) використовуються для деструктивної діяльності, розпалювання осередків нестабільності, нанесення

шкоди національним інтересам країн-жертв в інтересах російської експансії. У такий спосіб військова компонента доповнює інформаційну, а остання формує базу для першої.

При цьому представники науково-експертного середовища РФ прямо заявляють про необхідність від'єднання територій Казахстану, включаючись у потужну інформаційну кампанію, що корелюється з посилами, які поширювалися про Україну, а потім результували у анексії Криму та дестабілізації Донбасу.

Що у цьому випадку робити Республіці Казахстан?

Наведемо, відповідаючи на це питання, слова казахстанця Н. Тureханова:

«*Когда они пришли за молдаванами, я молчал – я не был молдаванином. Когда они пришли за грузинами, я молчал – я не был грузином. Когда они пришли за украинцами, я молчал – я не был украинцем. Когда они придут за мной – уже некому будет заступиться за меня*».

Потрібно розуміти, що проблема гібридної війни Російської Федерації стосується не окремої країни, а світового правопорядку. Відповідно, й боротися треба спільно …

*УДК 343.321.2*

**Гринчешен М. А.**
**Тугарова О. К.**
кандидат юридичних наук, доцент,
Національна академія СБ України

## КЛАСИФІКАЦІЯ ТА ЗАСЕКРЕЧУВАННЯ СЕКРЕТНОЇ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ РЕСПУБЛІКИ КАЗАХСТАН

Система охорони державної таємниці в Республіці Казахстан регулюється законом Республіки Казахстан «О государственных секретах». Закон визначає правові основи і єдину систему захисту державних секретів у інтересах забезпечення національної безпеки Республіки Казахстан, регулює суспільні відносини, що виникають у зв'язку з віднесенням інформації до державних секретів, їх засекречуванням, розпорядженням, захистом і розсекречення.

Особливістю системи охорони державної таємниці, є те, що законодавством передбачено точне розділення державну таємницю та службову таємницю, які в комплексі складають секретну інформацію. Показово, що в порівнянні з вітчизняним законом «Про державну таємницю» інформація ступеню секретності «для службового користування» в документі Республіки Казахстан є секретною і до неї використовується режим такий же як і для секретної.

Закон складається з 7 глав та 38 статей, і був підписаний 15 березня 1999 року. Документ містить наступні глави : Загальні положення, Повноваження Президента Республіки Казахстан, Парламенту; Уряду, державних органів і організацій Республіки Казахстан в області захисту державних секретів; Відомості, що відносяться до державних секретів Республіки Казахстан; Засекречування відомостей і їх носіїв, що становлять державні секрети Республіки Казахстан; Розсекречення відомостей і їх носіїв; Розпорядження відомостями, що становлять державні секрети Республіки Казахстан; Захист державних секретів.

Важливою складовою цього закону, є визначення, які дає цей закон, зокрема, йдеться про пояснення, що є державним секретом, державною таємницею, та службовою таємницею.

Так, державний секретом є захищені державою відомості, які складають державну і службову таємницю, поширення яких обмежується державою з метою реалізації ефективної діяльності, яка не протирічить міжнародним правовим актам.

Державною таємницею, власне, є свідчення військового, економічного, політичного та іншого характеру розголошення або втрата котрих наносить або може нанести шкоду національній безпеці Республіки Казахстан.

«Государственные секреты – защищаемые государством сведения, составляющие государственную и служебную тайны, распространение которых ограничивается государством с целью осуществления эффективной военной, экономической, научно-технической, внешнеэкономической, внешнеполитической, разведывательной, контрразведывательной, оперативно-розыскной и иной деятельности, не вступающей в противоречие с общепринятыми нормами международного права; Служебная тайна – сведения, имеющие характер отдельных данных, которые могут входить в состав государственной тайны, разглашение или утрата которых может нанести ущерб национальным интересам государства, интересам государственных органов и организаций Республики Казахстан» [1; с. 2].

Стаття 18, Закону Казахстану «О государственных секретах» регламентує ступені секретності і головний критерій за яким інформація має бути віднесена до державної таємниці. Згідно з законом виділяють 3 ступені секретної інформації і відповідні грифи до них «особливої важливості», «цілком таємно» , «таємно», однак для надання ступеню секретності державній таємниці використовується лише ступені «цілком таємно» та «особливої важливості». Для службової ж інформації використовується ступінь і гриф відповідно «секретна». Крім того, забороняється присвоювати грифи інформації, що не є державним секретом.

Закон також передбачає значну кількість відомостей, категорій, які мають бути засекреченими, вони деталізовані в Главі 3 Закону «О госу-

дарственных секретах». Згідно Глави 3, відомості які є секретною інформацією в Республіці Казахстан є відомості що стосуються військової галузі, економіки освіти й науки і техніки, зовнішньої політики та зовнішньоекономічної діяльності, розвідувальної, контррозвідувальної та оперативно – розшукової діяльності.

Деталізація цих категорій, присутня в Законі Республіки Казахстан в Главі 3, статтях 11 – 14. Для прикладу можна представити уривок зі статті 13 Закону Республіки Казахстан «О государственных секретах».

«Статья 13. Сведения во внешнеполитической и внешнеэкономической области, относимые к государственным секретам Республики Казахстан

К государственным секретам во внешнеполитической и внешнеэкономической области относятся:

1) сведения по вопросам внешней политики, внешней торговли, научно-технических связей, раскрывающие стратегию и тактику внешней политики Республики Казахстан, преждевременное распространение которых может нанести ущерб интересам государства;

2) сведения по политическим, военным, научно-техническим или экономическим вопросам в отношении одного или ряда иностранных государств, полученные в доверительном порядке, если их разглашение может привести к выявлению источника;

3) сведения о переговорах между представителями Правительства Республики Казахстан и представителями других государств о выработке единой принципиальной позиции в международных отношениях, если, по мнению участников переговоров, разглашение этих сведений может повлечь для одной из сторон дипломатические осложнения;

4) сведения о подготовке, заключении, подготовке к денонсации, содержании или выполнении международных договоров, преждевременное распространение которых может нанести ущерб обороноспособности, безопасности, политическим или экономическим интересам Республики Казахстан;

5) сведения об экспорте и импорте вооружения, военной техники или снаряжения, а также сведения об оказании технического содействия иностранным государствам в создании вооружения, военной техники и военных объектов, в том числе безвозмездно, с указанием стран-получателей, если разглашение этих сведений может повлечь для одной из сторон дипломатические осложнения [1; с. 12–13]».

**Література**

1.О государственных секретах. Закон Республіки Казахстан від 15 березня 1999 року. URL: https://zakon.uchet.kz/rus/docs/Z990000349_ (дата звернення 4.03.2020).

*УДК 316.625*
**Гришина О. Г.**
Національна академія СБ України

# ТРОЛІНГ ЯК ЧИННИК ВПЛИВУ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ

Інтернет – тролінг все частіше використовується для підтримання військових дії. Недавні конфлікти показали, як державні, так і недержавні суб'єкти ефективно використовують тролінг, щоб отримати підтримку за свої дії, залучати нових членів, обдурити і залякати противника, і навіть використовувати його для традиційних військових дій – такі як розвідувальний збір, залякування і контроль.

Інтернет – це територія свободи, в тому числі й свободи слова. Хто завгодно може сказати кому завгодно, що завгодно, і в більшості випадків нічого йому за це не буде. У певному сенсі це добре – це дозволяє дізнаватися багато неофіційних новин, отримувати найбільш повну інформацію про людей, компанії, політику тощо.

Але, з іншого боку, ця свобода слова може стати джерелом негативу. Адже анонімність багатьом розв'язує язик (або точніше – пальці), і якщо в звичайному житті більшість все ж намагається стримувати агресію, не лаятися матом і взагалі вести себе пристойно, то, спілкуючись в Інтернеті, ті ж самі люди перетворюються на справжнісіньких «тролів».

Тролінг використовується для того, щоб викликати конфлікт, спровокувати учасників на взаємні образи, лайки і т. п. При цьому мотиви, що спонукали людину зайнятися такого роду хуліганством, можуть бути абсолютно різними: від бажання поставити експеримент над живими користувачами до спроби самоствердитися.

Метою даної статті є проведення системного аналізу тролінгу в контексті впливу на інформаційну безпеку.

У результаті контент-аналізу Інтернет – комунікацій я виділила міжкультурні, технічні і універсальні чинники , що вплинули на появу тролінгу в комунікативному просторі Інтернет:

а) Міжкультурні – це тролінг, пов'язаний з розвитком демократичних прав і свобод.

б) Технічні – це наявність вільного, комфортного, високошвидкісного доступу в Інтернет ; розвиток нових засобів і способів передачі інформації – безпровідних телекомунікаційних засобів, такі як мобільні телефони, планшети тощо, і різних безпровідних технологій , способів входу в Інтернет.

в) Універсальні: віртуальна комунікація надзвичайно популярна, тому що вона порівняно не дорога, зручна та проста у використанні, та сприяє швидкому обміну інформацією між користувачами, незалежно від відстані та місця розташування абонентів.

В Україні як ніколи активізувалась проблема тролів і ботів та існування відповідних бот-мереж, які несуть загрозу інформаційному середовищу. Як відомо, інформаційні війни – це дії, розпочаті для досягнення інформаційної переваги шляхом завдання шкоди інформації та процесам, що базуються на інформації та інформаційних системах ворога при одночасному захисті власної інформації та процесів, що базуються на інформації та інформаційних системах. Найбільш поширеним видом таких дій є тролінг, який застосовується в інформаційних мережах, соціальних середовищах та платформах.

На тему «тролінг» написано безліч навчальних, публіцистичних статей та книжок. Це явище досліджувала достатньо велика кількість науковців, такі як: М. Акулич, Р. Внебрачних, І. Ксенофонтова, Дж. Хірш, А. Галінський, Дж Маккі та інші. Не дивлячись на це, понятійний апарат залишається неупорядкованим.

Тому, на мою думку, тролінг – це вид мережевого спілкування, який направлений на навмисне створення провокаційних повідомлень, що породжують агресивну поведінку учасників (учасника) обговорення, та призводять до конфліктів.

Основна задача тролінгу полягає в маніпулюванні масовою свідомістю з такими цілями, як, наприклад:

– внесення в суспільну свідомість і свідомість окремих людей визначених ідей та поглядів;

– дезорієнтація людей та їхня дезінформація;

– ослаблення визначених переконань людей, основ суспільства;

– залякування мас.

Причинами появи і розвитку тролінгу в мережі Інтернет можуть служити інтерес, цікавість, бажання самоствердитися, посперечатися, проявити дотепність, розважитися, бажання проявити агресію і негативні емоції.

Виходячи з наведеного, можна зробити висновок, що протидія інформаційній війні є одним з напрямів забезпечення інформаційної безпеки як складової частини національної безпеки держави. Механізми протидії зазначеним загрозам мають бути високотехнологічними та мати системний характер. Що потрібно здійснити терміново? По-перше, слід нарешті не декларувати, а почати створювати систему кібербезпеки, а також забезпечити функціонування центру реагування та проведення спеціальних операцій з метою нейтралізації інформаційних загроз.

По друге, доцільно впровадити в освітній процес, починаючи зі старших класів школи, хоча б факультативні заняття з «Основ інформаційної безпеки». Третім кроком має бути підтримка держави в ініціюванні та проведенні наукових пошуків проблем інформаційного протиборства та вироблення захисних механізмів. З цією метою мають бути залучені спеціалісти у багатьох сферах знань: медичних, технічних, психологічних,

юридичних тощо. Вказані заходи є далеко невичерпними, але мають бути вжиті одночасно у якомога коротший термін.

**Література**

1. Зеленін В. В. По той бік правди: нейролінгвістичне програмування як зброя інформаційно-пропагандиської війни / В.В. Зеленін. – Вінниця: Віндрук, 2014. – 384 с.

2. Курбан О. В. PR у маркетингових комунікаціях : навч. посіб. / О.В. Курбан. – Київ : Кондор-Видавництво, 2014. – 246 с.

3. Судариков Виктор. Троллинг: анализ явления. Православие и мир (19 февраля 2013) // URL: http://www.pravmir.ru/trolling-analiz-yavleniya/ (дата обращения:16.09.2015).

4. Внебрачных Р. А. Троллинг как форма социальной агрессии в виртуальных сообществах / Р. А. Внебрачных // Вестн. Удмурт. ун-та. – Серия 3: Философия. Социология. Психология. Педагогика. – 2012. – Вып. 1. – С. 48-51.

*УДК 004.056*

**Гуліватий Д. М.**
Національна академія СБ України
**Жевелєва І. С.**
Національна академія СБ України

## ГІБРИДНІ ЗАГРОЗИ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ ДЕРЖАВИ В КОНТЕКСТІ МІЖДЕРЖАВНОЇ КОМУНІКАЦІЇ

Кожне суспільство в сучасних умовах перебуває в спілкуванні з іншими соціумами і зацікавлене у збереженні своєї мовної та культурної самобутності, що в умовах глобального інформаційного простору і легкості транскордонних впливів є досить важким завданням [1]. Під впливом інформаційно-комунікаційних технологій змінюється і співвідношення компонентів традиційної могутності держав, яка визначається на основі володіння інформаційно-комунікаційними технологіями і позиції у сучасному інформаційному просторі. Така ситуація призводить до виникнення нового міжнародного протистояння, коли прагнення однієї держави домінувати у глобальному інформаційному просторі породжує опір і протидію інших.

Виклики міжнародним відносинам, що виникли 2014 року, породили також нові явища і ситуації, які можна охарактеризувати як незрозумілі, непередбачувані та нестандартні [2, с. 127]. У медійному, а згодом і науковому середовищі вони отримали характеристику «гібридних». Зокрема про гібридний характер загроз міжнародній безпеці говорить Р. Сіле, наголошуючи, що саме 2014 рік позначив парадигму змін у світі, а українсько-російський конфлікт показав, що у Європу повернулося використання

державними акторами військової сили та насильства заради досягнення політичних цілей

Зважаючи на складну політичну ситуацію, яка склалася на Україні за останній час, соціологи стверджують про явні ознаки гібридної загрози і гібридної війни. Так гібридні загрози об'єднують широкий діапазон штучно створених ворожих дій і намірів, таких як кібервійна, інформаційна війна, сценарії асиметричних військово-силових конфліктів низької інтенсивності, цілеспрямована організація терористичних актів і піратства на морі, підтримка і стимулювання незаконної міграції, роздування етнічних і релігійних конфліктів.

Звичайно, критерієм концептуального розмежування гібридної загрози від гібридної війни є факт порушення суверенітету держави, перетин збройними формуваннями кордону, захоплення стратегічно важливих об'єктів [3]. Ключовою рисою підходу, який виник для протидії багатовимірному характеру гібридних загроз, є його всеосяжність, адже передбачає скоординоване застосування всього спектру наявних ресурсів, зокрема дипломатичні, військові, розвідувальні та економічні. Важливо зазначити, що гібридні атаки не є виключно інструментом асиметричних чи недержавних акторів, до них можуть вдаватися як недержавні, так і державні суб'єкти. Гібридні загрози навіть не прив'язані територіально, і можуть проявлятися в будь-якій операційній зоні, включаючи кіберпростір.

Смертельні та руйнівні атаки можуть бути розпочаті і здійснені миттєво з віддалених місць, не залишаючи слідів для визначення їхнього походження. Ефективна відповідь подібним атакам потребує єдності зусиль. У доктрині збройних сил США зазначено, що існуюча гібридна загроза побудована на діях Москви у Східній Європі, які створюють прецедент на майбутнє: вона використовує значну кількість гібридних способів і засобів проти слабкої або ослабленої держави (України), щоб примусити її підкорятися своїй волі.

Традиційні гібридні загрози зосереджені на змішуванні різних можливостей на тактичному та операційному рівнях війни. Однак Російська Федерація сьогодні використовує не лише військовий інструментарій, а й економічні, інформаційні та дипломатичні засоби, конструюючи гібридну загрозу для подальшого загострення проблеми [4, с. 39]. «Суть гібридної війни в тому, що ворог постійно випереджає і постійно використовує свої ресурси на тих фронтах і ділянках, де його не чекають, або не мають можливості відповісти». Український досвід засвідчує, що гібридні загрози найактивніше проявляються у попередньо створеній паралельній реальності [5].

Гібридні загрози знаходиться між конфліктами, в яких рушійною силою є держава, і конфліктами, в яких рушійною силою є недержавний суб'єкт. Саме тому питання про роль мови в захисті від гібридних загроз

набуло особливого звучання. Оскільки історично склалося, що на території України українсько-російська двомовність у суспільстві зумовлена функціонально-стилістичним, територіальним, віковим, конфесійним, соціальним чинниками, то держава турбується про розвиток україномовних форм культурного життя. Але, розуміючи важливість багатомовності, Україна гарантує вільне використання регіональних мов та забезпечує реалізацію прав і культурних інтересів усіх мовних груп, не перешкоджаючи ретрансляції передач із сусідніх країн.

Але при визначенні функцій державної мови влада повинна чітко окреслювати сфери обов'язкового застосування мови. У такому випадку мова стає інструментом для захисту національних інтересів і політичної думки. Відсутність чіткої концепції що до розвитку державної мови призводить до підсилення впливу потенційного агресора [6, с. 11].

Отже, перед владними структурами постає завдання зберегти національну ідентичність країни шляхом введення української мови у всі сфери життєдіяльності суспільства, з умовою врахування багатомовної реальності. Крім цього, в умовах тісної міждержавної комунікації, забезпечити захист свого населення, адже протидія гібридним загрозам стає пріоритетом, оскільки вони розмивають чітку межу між війною та миром, поєднуючи військові можливості з політичними, дипломатичними, економічними, кібер-безпековими та дезінформаційними заходами. Для нейтралізації таких загроз потрібні не лише нові спроможності, але й нові партнери, нові процеси і, перш за все, нове мислення.

**Література**

1. Горбулін В. Російська гібридна війна змінює світо устрій. URL: https: // zbruc. eu / node / 63861 (дата звернення 13.02.2020).

2. Стратегія національної безпеки України (альтернативна). Луцьк: МКФ, 2016. С. 127.

3. Про засади державної мовної політики: Закон України. URL: http: // zakon. rada. gov. ua / laws / show / 5029–17 (дата звернення 13.02.2020).

4. Doctrine for the Armed Forces of the United States // Department of Defense, Joint Publication (JP) 1, Washington D. C.: Department of Defense, 2013. P. 39

5. Вите С. Типология вооруженных конфликтов в международном гуманитарном праве: правовые концепции и реальные ситуации URL: https: // www. icrc. org / rus / assets / files / other / vite. pdf (дата звернення 13.02.2020).

6. Пожуєв В. І. Формування інформаційного суспільства в умовах глобалізації. Гуманітарний вісник *ЗДІА*, 2009. Вип. № 36. С. 11.

*УДК 327.5:316.776.23*
**Даценко А. Ю.**
Національний інститут стратегічних досліджень

# АКТУАЛЬНІ ШЛЯХИ ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ В УМОВАХ ІНФОРМАЦІЙНОЇ ВІЙНИ

За оцінками фахівців у інформаційній сфері, кількість інформації на нашій планеті останнім часом подвоюється кожні два роки. Зокрема, кожну хвилину на YouTube переглядають майже п'ять мільйонів роликів, щохвилини користувачі Інтернет завантажують 375 тисяч додатків і надсилають один одному 18 мільйонів текстових повідомлень. У такому потоці просто немає ніяких бар'єрів для тих, хто хоче ввести нас в оману, обдурити чи використати [4].

Разом із глобальним розширенням використання соціальних мереж, яке різко збільшило швидкість та обсяг потоку всієї інформації, різко збільшились й відмінності між поширенням суб'єктивних думок та констатацією фактів. Тим більше в умовах інформаційної війни поширення вигідної суб'єктивної інформації, фейків, перекручених фактів або маніпуляцій (навіть з достовірною інформацією) стає основним інструментарієм в інформаційному протиборстві.

Виходячи з цього, питання експертної оцінки ефективності заходів з протидії дезінформації набуває першочергової актуальності в середовищі фахівців безпекового сектору, у тому числі й за кордоном. Зокрема, Європейський аналітичний центр European Values у рамках спеціальної стратегічної програми Kremlin Watch провів дослідження [3], в якому був зроблений аналіз різних заходів боротьби нашої країни із російською дезінформацією та дана оцінка її ефективності.

Результатом аналізу стали наступні висновки:

– боротьбу з дезінформацією необхідно кодифікувати. Дезінформація з боку Росії є частиною її гібридних атак проти іноземних країн, цю загрозу слід сприймати відповідним чином у рамках національної безпеки та розробляти й ухвалювати спеціальні закони для боротьби з дезінформацією;

– для боротьби з дезінформацією дуже важлива координація зусиль між державними інститутами, а також між державою та громадянським суспільством. За час неоголошеної війни в Україні багато неурядових організацій були створені саме для підвищення спротиву дезінформаційним зусиллям Кремля: StopFake, Informnapalm, Euromaidan Press, тощо. Саме зусилля неурядових організацій стали провідними у боротьбі з російською дезінформацією, і державі слід більше їх підтримувати та координувати з ними свої зусилля. У деяких випадках неурядові організації навіть краще

реагують на інформаційні загрози, ніж уряд: вони більш гнучкі та менш забюрократизовані. Зокрема, співпраця з Українським кризовим медіа-центром, була найкращим кроком уряду для зміцнення комунікаційних можливостей України;

– оскільки телебачення залишається основним джерелом інформування певної категорії населення, то заборона телеканалів, які розповсюджують дезінформацію, є ефективним методом боротьби з фейками. Згідно із опитуваннями громадської думки, рішення заборонити розповсюдження в українському інформаційному просторі російських каналів було ефективним: наразі не більше 6% українців дивляться російські новини, і здатність російських ЗМІ впливати на людей стала дійсно нижчою;

– запобігання завжди краще, ніж реагування. Постійно відбиватися від фейків російського походження – це кропітка робота, дуже витратна за часом та фінансово, причому у багатьох випадках не дуже ефективна [1]. Адже здебільшого такі фейки мають на меті відвернути увагу від чогось більш суттєвого. Тому усі зусилля, спрямовані на їх спростування, ще більше привертають до них увагу. Виходячи з цього, як засіб протидії дезінформації рекомендується постійно та своєчасно підвищувати довіру громадян до ключових державних інституцій, на дискредитацію авторитету яких у переважній більшості спрямовується ворожа дезінформація, а особливо до тих, що відповідають за безпеку і оборону нашої держави;

– поінформоване про тактики ведення інформаційної війни населення менш вразливе до загроз та дезінформації, пов’язаних з цими війнами. В Україні підвищення громадської обізнаності здійснюється на декількох рівнях: обмін досвідом у боротьбі з дезінформацією між журналістами, державними службовцями та неурядовими організаціями. Однак державі рекомендується надавати більше підтримки громадським проектам медіа-освіти в їхніх спробах підвищувати обізнаність населення.

Найбільш ефективним засобом боротьби з дезінформацію є розвиток критичного ставлення населення до будь-якої інформації через впровадження державою масштабної програми, спрямованої на підвищення в суспільстві рівня медіаграмотності. Експерти наголошують на необхідності приділити особливу увагу в медіа-освіті таким питанням:

– оскільки медіа-освітні програми орієнтовані переважно на реалізацію в середніх й вищих навчальних закладах та впроваджуються за підтримки держави на постійній основі, поза увагою залишилось підвищення медіаграмотності окремих категорій громадян, зокрема, літніх людей, які найбільше підпадають під вплив російської дезінформації через телебачення [2];

– при формуванні медіа-освітніх програм для учнів та студентів із врахуванням результатів дослідження новинної грамотності молоді слід

брати до уваги, що ця категорія громадян легко піддається «обдурюванню» під час користування онлайновою інформацією, і як наслідок, «саме за участі молоді фальшиві чутки подорожують мережею набагато швидше, довше і глибше, ніж правдиві історії» [4].

**Література**

1. Біла книга спеціальних інформаційних операцій проти України 2014-2018 / Д.Ю. Золотухін. – К., 2018. – 384 с., іл. [Електронний ресурс]. Режим доступу: https://mip.gov.ua/files/pdf/white_book_2018_mip.pdf (дата звернення 1.03.2020).

2. Черненко Т.В. Міжнародний досвід впровадження медіаграмотності для окремих цільових груп: можливості для України [Електронний ресурс]. Режим доступу: https://niss.gov.ua/doslidzhennya/informaciyni-strategii/mizhnarodniy-dosvid-vprovadzhennya-mediagramotnosti-dlya (дата звернення 1.03.2020).

3. Analyzing the Ground Zero. What Western Countries can Learn From Ukrainian Experience of Combating Russian Disinformation [Електронний ресурс]. Режим доступу: https://www.europeanvalues.net/wp-content/uploads/2017/12/Analyzing-the-Ground-Zero..pdf (дата звернення 1.03.2020).

4. «All information is not created equal». Вісім думок людини, яка десять років розвиває медіаграмотність в США [Електронний ресурс]. Режим доступу: https://www.radiosvoboda.org/a/fake-news-propaganda-usa-miller/30208392.html (дата звернення 1.03.2020).

*УДК: 342.951*

**Дворник В. Т.**
Інститут підготовки юридичних
кадрів для Служби безпеки України
Національного юридичного
університету імені Ярослава Мудрого

## ДО ПИТАННЯ ВИЗНАЧЕННЯ ТА НАПРЯМІВ ПРОТИДІЇ КІБЕРТЕРОРИЗМУ

В умовах сучасних військових загроз та політичної ситуації держави на міжнародній арені, ми неодмінно стикаємося з проблемами забезпечення інформаційної безпеки, що пов’язані з трансформацією інформаційних ресурсів. Стрімкий розвиток технологій в XXI столітті спонукає держави та їх громадян підпорядковуватися новим умовам життєдіяльності, що в свою чергу, змушує людей шукати і нові шляхи для захисту особистих даних. Свою діяльність, на жаль, удосконалюють і терористичні угрупуван-

ня, почавши використовувати кібертехнології задля задоволення власних потреб, що спричиняють порушення громадської безпеки, залякування населення та негативно впливають на прийняття рішень органами влади.

Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р., дає визначення поняттю «кібертероризм», під яким розуміється терористична діяльність, що здійснюється у кіберпросторі або з його використанням [1].

Визначення «кібертероризму» на нашу думку, дуже влучно сформулювали в The National Conference of State Legislatures (USA), створеній для вироблення узгодженої політики з питань економіки і внутрішньої безпеки в США, яка визначає кібертероризм як – використання інформаційних технологій терористичними групами і терористами-одинаками для досягнення своїх цілей, що може включати використання інформаційних технологій для організації та виконання атак проти телекомунікаційних мереж, інформаційних систем і комунікаційної інфраструктури, або обмін інформацією, а також загрози з використанням засобів електрозв'язку [2].

Серед злочинів, які відносимо до кібертероризму, можна вказати такі як: злом інформаційних систем, внесення вірусів у вразливі мережі, дефейс веб-сайтів (тип хакерської атаки, при якій сторінка веб-сайту замінюється на іншу), DoS-атаки (напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними користувачам, для яких комп'ютерна система була призначена) та ін.

Враховуючи зазначене, а також те, що серед сучасних реформаційних нововведень є перехід роботи органів державної влади та місцевого самоврядування в електронний режим – вся інформація, яка буде реєструватись там (не дивлячись на форму доступу), буде під ризиком розголошення, чим кібертерористи та агенти іноземних спецслужб можуть скористатись. Для прикладу, в Україні найбільшою атакою на комп'ютерні засоби органів влади був вірус PETYA у 2017 році, який шифрував файли та знищував цілі файлові системи.

У зв'язку з цим, свою діяльність спрямували на недопущення таких загроз як правоохоронні органи, так і органи державної влади, зокрема Служба безпеки України, Міністерство внутрішніх справ, Державна служба спеціального зв'язку та захисту інформації України,Міністерство інформаційної політики, Державний комітет з питань телебачення й радіомовлення та ін.

Так, згідно з Законом України «Про Службу безпеки України» протидія кіберзлочинності в цілому і кібертероризму, зокрема, покладена на Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки, який здійснює запобігання, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі [2, ст. 8]. Крім того, для узгодженої протидії кіберзагрозам, на

базі Служби безпеки України створено ситуаційний центр, основним завданням якого є моніторинг масової інформації та мережі Інтернет з метою виявлення загроз національній безпеці України в інформаційній сфері.

Для удосконалення протидії кібертероризму в Україні, вбачається логічним вивчати досвід іноземних держав у даній сфері, які мають в ній позитивні напрацювання. Так, однією з провідних країн світу, яка на високому рівні забезпечує інформаційну безпеку держави та своїх громадян – є США. Американський досвід державної політики у сфері інформаційної безпеки може бути актуальним для багатьох питань української зовнішньої та внутрішньої політики. Насамперед, необхідно звернути увагу на такі аспекти американського досвіду в сфері забезпечення інформаційної безпеки, як: виокремлення найбільш ефективних підходів до регулювання ринку інформаційних технологій; спеціально створений орган National Cyber Security Division (Національне управління кібербезпеки), що діє на базі Міністерства внутрішніх справ; структурована нормативно-правова база, що регламентує цю діяльність, де основні: Кіберстратегія Міністерства оборони від квітня 2015 року; Міжвідомчий план дій з кібербезпеки систем управління; План дій з посилення кібербезпеки найважливіших об'єктів інфраструктури (2014) [4].

Отже, підсумуємо, що Україна має певний потенціал для того, щоб протидіяти такому сучасному виду загроз, як кібертероризм, проте, враховуючи стрімкість технологічних змін і звертаючи увагу на досвід США та інших країн, можемо констатувати тенденції постійного розвитку системи забезпечення національної безпеки у сфері інформаційного захисту на прикладі США, які можуть слугувати напрямом покращення стану протидії кібертероризму в нашій країні.

**Література**

1. Закон України « Про основні засади забезпечення кібербезпеки України» від 05.10.2017 року. // Офіційний веб-портал Законодавство України. – Електронний ресурс. URL: https://zakon.rada.gov.ua/laws/show/2163-19.

2. Defining cyber terrorism: веб-сайт. URL: https://www.i-policy.org/2009/07/defining-cyber-terrorism.html.

3. Official website of the Department of Homeland Security. // Офіційний веб-сайт Департаменту внутрішньої безпеки. – Електронний ресурс. URL: https://www.cisa.gov/cybersecurity-division.

*УДК 342.15*
**Дячук Л. М.**
**Козюра В. Д.**
кандидат технічних наук, доцент,
Національна академія СБ України

# МІФИ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ ПРО ПРИНАЛЕЖНІСТЬ КРИМУ ДО РОСІЇ

Станом на сьогодні, територія Криму, яка є невід'ємною частиною України, знаходиться під окупацією Російської Федерації внаслідок збройного захоплення АРК на початку 2014 року та проведення 16 березня 2014 року нелегітимного референдуму щодо приєднання Криму до Росії, реальні результати якого встановити неможливо.

По суті, ще задовго до фактичної окупації Криму, РФ здійснювала інформаційно-психологічний та інформаційно-технічний вплив, особливо активно поширювалась пропаганда, внаслідок цього настрої населення півострова були штучно змінені за допомогою активного застосування дезінформації, маніпулювання свідомістю, створення негативного іміджу України. Це посприяло втраті національної ідентичності кримчан, толерантного ставлення до інших народів, зумовило посилення антиукраїнських настроїв та категоричного несприйняття європейського вектору розвитку України.

Окрім цього, РФ активно підключала ЗМІ та ЗМК з метою доведення до власних громадян, українців та жителів інших країн позиції РФ щодо Криму та збільшення підтримки населення. Президент РФ В. Путін протягом так званої «Кримської промови» наголошував, що у Криму буквально все пронизане нашою спільною історією й гордістю, а всі ці роки і громадяни, і багато громадських діячів неодноразово порушували цю тему, казали, що Крим – це споконвічно російська земля, а Севастополь – російське місто.

Але крім цієї промови В. Путіна були й зовсім протилежні. Наприклад, після грузинської війни 2008 року, він заявляв: «Росія не претендує на півострів, а Крим не є ніякою спірною територією, там не було ніякого етнічного конфлікту, РФ вже давно визнала кордони сьогоднішньої України. А питання про якісь подібні цілі Росії віддає провокаційним сенсом. Там всередині суспільства в Криму відбуваються складні процеси – проблеми кримських татар, українського населення, росіян – але це вже внутрішньополітичні проблеми самої України».

Водночас, як у міжнародних, так і в національних нормативно-правових актах чітко закріплена приналежність Криму до України. Так, в Угоді про створення Співдружності Незалежних Держав від 8 грудня 1991 року зазначено про визнання та повагу взаємної територіальної цілі-

сності та недоторканності існуючих кордонів у межах Співдружності, у Алма-Атинській декларації від 21 грудня 1991 року вказано теж саме, а Статут СНД від 22 січня 1993 року, що закріплював серед взаємопов'язаних і рівноцінних принципів відносин усередині СНД визнання та непорушність існуючих державних кордонів, відмову від протиправних територіальних надбань, а також територіальну цілісність держав і недопущення будь-яких дій, спрямованих на розчленування чужої території. Основним міжнародним нормативно-правовим актом вважається Договір про нерозповсюдження ядерної зброї, підписаний Україною, РФ, Великою Британією та США, учасники якого підтвердили зобов'язання утримуватися від загрози силою або її застосування проти територіальної цілісності та незалежності України.

Беручи до уваги внутрішнє законодавство України, треба зазначити, що в ньому легітимно закріплений статус Криму як частини України. Наприклад, відповідно до ст. 133, 134 Конституції України, АРК і м. Севастополь є невід'ємною частиною України, і згідно із ст. 14 ЗУ «Про всеукраїнський референдум», референдум щодо зміни території України призначається виключно Верховною Радою України, тобто Російська Федерація порушила не тільки українські, а й міжнародні нормативно-правові акти.

Протягом 2014 року нелегітимний парламент Криму та Державна Дума РФ ухвалили цілу низку нормативно-правових актів. Кримським парламентом була ухвалена постанова щодо проведення так званого «загальнокримського референдуму». Факт даного порушення був встановлений Конституційним Судом України, який у своєму рішенні від 14 березня 2014 року вказав на те, що ця постанова суперечить Конституції України, визнав її неконституційною і зобов'язав органи АРК припинити будь-яку діяльність з підготовки до референдуму. 15 березня 2014 року Верховна Рада України постановила достроково припинити повноваження Верховної Ради АРК, внаслідок чого остання втратила будь-яку легітимність. Але 17 березня 2014 р. ВР АРК приймає Постанову про незалежність Криму та проголошення незалежної суверенної держави – Республіки Крим, а 18 березня 2014 р. укладено Договір між РФ і Республікою Крим про прийняття в РФ Республіки Крим та утворення у складі РФ нових суб'єктів, що був ратифікований Державною Думою РФ 20 березня 2014 року та в ряду з іншими нормативно-правовими актами нелегітимного парламенту Криму та Державної Думи РФ, прямо суперечить чинному українському та міжнародному законодавству.

Отже, Російська Федерація здійснювала деструктивний вплив на жителів Криму ще задовго до здійснення окупації АРК. Такий інформаційно-психологічний та інформаційно-технічний вплив поширювався, здебільшого, за допомогою пропаганди, значною частиною якої були офіційні виступи В. Путіна, в яких він зазначав про «приналежність Криму до Ро-

сії», хоча ще в 2008 році, він заявляв, що РФ не претендує на півострів і Крим не є спірною територією. Здійснивши окупацію АРК, російська сторона порушила українське та міжнародне законодавство, зокрема положення Договору про нерозповсюдження ядерної зброї, яким заборонено загрозу силою або її застосування проти територіальної цілісності та незалежності України (а Російська Федерація взагалі, виступає тут гарантом), а також Конституцію України, в якій зазначено, що АРК та місто Севастополь є невід'ємною частиною України та інші нормативно-правові акти.

**Література**

1. Конституція України [Електронний ресурс] / Режим доступу: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.

2. Договір про нерозповсюдження ядерної зброї [Електронний ресурс] / Режим доступу: https://zakon.rada.gov.ua/laws/show/995_098.

3. ДоговормеждуРоссийскойФедерациейи Республикой Крымо принятии в Российскую ФедерациюРеспубликиКрыми образовании в составе РоссийскойФедерациииновыхсубъектов [Електронний ресурс] / Режим доступу: http://www.kremlin.ru/events/president/news/20605.

4. Права людини в Україні 2014. Доповідь правозахисних організацій [Електронний ресурс] / Режим доступу: http://khpg.org/index.php?id=1432190917.

5. КрымНаш. Історія російського міфу / С. В. Громенко. – К., 2017 [Електронний ресурс] / Режим доступу: http://shron1.chtyvo.org.ua/Hromenko_Serhii/KrmNash_Istoriia_rosiiskoho_mifu.pdf.

*УДК 39.394*

**Жуков Є. М.**
**Тиква В.Л.**
Національна академія СБ України

## ДОКАЗИ З ІФОРМАЦІЙНИХ ДЖЕРЕЛ ПРО ПРИЧЕТНІСТЬ РФ ДО ТРАГЕДІЇ ЗІ ЗБИТИМ МАЛАЙЗІЙСЬКИМ ЛІТАКОМ "БОЇНГ МН-17"

Вся світова спільнота пам'ятає трагедію 17 липня 2014 року, коли був збитий Боїнг Малайзійських авіаліній у повітряному просторі тимчасово окупованих територій України, який виконував рейс МН-17 зі Амстердама до Куала-Лумпур. На жаль, загинуло 298 чоловік. Після цієї трагедії було сформовано Міжнародну слідчу групу з метою об'єктивного розслідування та визначення винних у катастрофі.

Безпосередньо одразу після трагедії до-сьогодні можна спостерігати, що влада та ЗМІ Російської Федерації, а також підконтрольні їм "керівники" невизнаних "ДНР" та "ЛНР", у тому числі їх ЗМІ стверджують, що

вони не причетні до трагедії та навіть перекладають вину, вигадуючи різні версії трагедії.

Але члени Міжнародної слідчої групи, що розслідує причини катастрофи рейсу МН-17, яка сталася 17 липня 2014 року, переконані, що мають у своєму розпорядженні незаперечні докази того, що лайнер був збитий зенітною ракетою серії 9М38 зенітно-ракетного комплексу «Бук». Крім того, в розпорядженні слідства є докази, які дозволяють стверджувати, що місцем запуску ракети було поле в районі смт Первомайське, яке на той час перебувало під контролем проросійських бойовиків. Про це було оголошено в ході презентації для родичів загиблих у катастрофі. Держави, що входять у Міжнародну слідчу групу (Австралія, Бельгія, Малайзія, Нідерланди і Україна), ведуть спільне кримінальне розслідування причин катастрофи авіалайнера [1].

18 жовтня 2014 року видання «DeutscheWelle» із посиланням на «Шпіґель» повідомило: «Катастрофу малайзійського літака Boeingрейсу МН-17 у небі над Східною Україною спричинили проросійські сепаратисти – такого висновку дійшла німецька розвідка. Президент Федеральної розвідувальної служби Німеччини Гергард Шиндлер, за інформацією журналу, розповів про це членам парламентського контрольного органу Бундестагу ФРН ще 8 жовтня, представивши ґрунтовні докази» [2].

Розслідування, проведене групою журналістських розслідувань встановило, що пасажирський Боїнг малайзійських авіаліній був збитий проросійськими бойовиками пострілом зенітно-ракетного комплексу «Бук М1», якій був доставлений з російського Курська.

Експерти з Варшави, Лондона і Мюнхена, досліджуючи фрагменти збитого літака, встановили, що МН-17 був збитий саме з «Бука». В обломках малайзійського літака знайдено уламки ракети ЗРК «Бук» [3].

Використовуючи записи радіопереговорів між сепаратистами, СБУ встановила, що співробітник Державного розвідувального управління Росії причетний до катастрофи малайзійського Boeing-777 рейсу МН17, збитого над Донецькою областю.

Розслідування журналістської організації Bellingcat встановило, що в ході прес-конференції в липні 2014 року Міністерство оборони РФ надало підроблені супутникові зображення, щоб звинуватити Україну в катастрофі Боїнга МН-17.

Американський телеканал CNN, який посилався на власні джерела у Пентагоні, повідомив, що за даними супутникового спостереження, ракету, яка вразила пасажирський «Боїнг» випущено з території Росії [4].

Отже, Міжнародна слідча група на підставі доказів знайшла злочинця – РФ, яка без законних підстав задіяла свої збройні сили та вчинила злочин, в результаті якого загинуло 298 осіб. При цьому РФ порушила не тільки ж власну Конституцію та закони, а ще й міжнародне законодавство,

застосовуючи при цьому власну деструктивну пропаганду та вигадування різних версій події, які не співпадають з дійсністю.

**Література**


1. ssu.gov.ua/ua/news/1/category/21/view/1954#.nW6Tya6V.dpbs.
2. archive.vn/20141019091348/http://www.ukrinform.ua/ukr/news/nimetska_rozvidka_vstanovila_shcho_boiing_zbili_separatisti_1982615.
3. www.pravda.com.ua/news/2015/03/19/7062082/.
4. zaxid.net/teroristi_zbili_pasazhirskiy_boeing_777_n1315384.



*УДК 304.5*



**Загребельний В. С.**
**Клочкова В. В.**
**Шемаєв В. М.**
доктор військових наук, професор,
Національна академія СБ України


## МІФИ РОСІЙСЬКОЇ ПРОПАГАНДИ ПРО ТЕ, ЩО РІВЕНЬ ЖИТТЯ В РОСІЇ ВИЩИЙ НІЖ РІВЕНЬ ЖИТТЯ В ЄС

На сьогоднішній день рівень життя характеризує добробут населення держави поряд з доходами і витратами, демонструє ступінь розвитку та задоволення потреб людей. Варто зазначити, що він відображає умови праці й побуту, елементи робочого та вільного часу, показники культурного та освітнього рівня суспільства, а також здоров'я, екологічну та демографічну ситуацію. Відповідно до Рекомендацій ООН, рівень життя – це сукупність таких показників, як: здоров'я, зокрема демографічні умови, їжа, одяг, фонди споживання і нагромадження, умови праці, зайнятість, організація праці, освіта, зокрема письменність, житло та його благоустрій, соціальне забезпечення [1].

Коли говорять про багатство країни як єдине ціле, зазвичай використовують показник внутрішнього валового продукту (ВВП – це ринкова вартість усіх товарів і послуг, вироблених на території держави для споживання, накопичення або на експорт за певний період, частіше за рік). Простіше кажучи, ВВП показує, скільки коштує все, що виробила країна. Неважко передбачити, що в такому переліку на високих місцях будуть високорозвинені держави з великою кількістю населення [3].

Уже тривалий час лобісти євразійської інтеграції та різних «возз'єднань» із Росією активно використовують міф про вищий рівень життя в РФ порівняно з Європейським Союзом. Проте глибокий аналіз засвідчує, що ці твердження не відповідають дійсності, що виявляє значно нижчу соціальну ефективність путінської авторитарної моделі держави [2].

Так, у більшості регіонів РФ через великі диспропорції між різними суб'єктами Федерації та їх розвитком, реальна купівельна спроможність середньої заробітної плати суттєво відрізняється від європейської, та в більшості випадків заробітна плата в Європейському Союзі є значно вищою, ніж в Росії [2-4].

Процес, який почався в жовтні 2014 року на тлі санкцій Заходу і падіння нафтових доходів, за декілька років спустошила гаманці громадян Російської Федерації більше ніж на 11%, а на регіональному рівні спад рівня життя перевищує середній як по країні, так і по ЄС [2].

Однак поліпшення свого матеріального становища бачать лише 10% населення, 31% скаржаться, що їх фінансова ситуація продовжує погіршуватися, а більше третини населення (38%) – незадоволені відсутністю грошей навіть на необхідне, з них 9% заявили, що їм не вистачає на їжу, а 28% – не можуть придбати собі одяг [4].

Кожен десятий російський працівник – людина в працездатному віці і офіційно зайнятий не може забезпечити себе і свою сім'ю, адже його доходи нижче прожиткового мінімуму, якщо враховувати, що витрачати отримане доводиться не тільки на себе, а й на своїх близьких родичів [4].

На основі даних сайту Numbeo, що становить окремий рейтинг країн за рівнем життя обчислюється загальний індекс рівня життя, який використовують в якості джерела великі ЗМІ і видання: Forbes, Business Insider, Time, The Economist, BBC, The New York Times [3]. Цей сайт оцінює 71 державу, і ось як виглядає перша п'ятірка за рівнем життя станом на січень 2019 року: Данія; Швейцарія; Фінляндія; Австралія; Австрія.

Посилаючись на інформацію, отриману з цього рейтингу, можемо зробити висновок, що перші місця очолюють, в основному, країни ЄС [3].

Беручи до уваги вищезазначене, можна сказати, що рівень життя в Російській Федерації насправді є набагато нижчим ніж в країнах Європейського Союзу, а Росія намагається активно просувати даний міф, не обґрунтовуючи його вагомими фактами, вводячи в оману не тільки власне населення, а й увесь світ.

**Література**

1. Рівень життя населення України [Електронний ресурс]. – Режим доступу: https://xreferat.com/113/3859-1-r-ven-zhittya-naselennya-ukra-ni.html.

2. Росія: багата країна - бідні громадяни [Електронний ресурс]. – Режим доступу: https://tyzhden.ua/World/101261.

3. Рейтинг стран по уровню жизни в 2019 – самые богатые и самые бедные страны мира / Migronis [Електронний ресурс]. – Режим доступу: https://migronis.com/blog/rejting-stran-po-urovnju-zhizni-v-2019-samye-bogatye-i-samye-bednye-strany-mira.

4. Росстат: Уровень жизни россиян продолжает снижаться [Електронний ресурс]. – Режим доступу: https://eadaily.com/ru/news/2017/12/20/rosstat-uroven-zhizni-rossiyan-prodolzhaet-snizhatsya.

*УДК 340.134 (477+061.1 ЄС): 351.822.009.6*
**Залевський В. В.**
**Пивовар П. Є.**
Національний технічний університет України
«КПІ імені Ігоря Сікорського»і

# ЗАГАЛЬНИЙ РЕГЛАМЕНТ ПРО ЗАХИСТ ДАНИХ ЄС (GDPR): КОНЦЕПТУАЛЬНІ ЗАСАДИ ТА ПЕРСПЕКТИВИ ВИКОРИСТАННЯ В УКРАЇНІ

Україна зараз знаходиться в активному процесі «діджиталізації» та впровадження програми «Держава в смартфоні», а тому захист персональних даних користувачів електронних систем набуває в Україні особливого значення. Слід зауважити, що нині не лише держави збирають персональні дані, але й компанії як міжнародні (наприклад, Google, Facebook, Amazon та ін.), так і українські (наприклад, Rozetka, Citrus, Нова Пошта та ін.), що також мають доступ до персональних даних своїх користувачів, у тому числі й з України. Не можна забувати і про велику кількість кібератак в Україні за останні роки, що ставить під загрозу інформаційну безпеку держави в цілому та окремих громадян. Отже, виникає потреба в ухваленні спеціального законодавства, яке забезпечувало б правові механізми регулювання процесів збереження та обробки персональних даних користувачів. Враховуючи підписання Угоди про асоціацію між Україною та Європейським Союзом (далі – ЄС) та бажання України в майбутньому стати членом ЄС, доцільним є вивчення досвіду ЄС щодо захисту персональних даних на прикладі Регламенту Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 р. про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних (Загальний регламент про захист даних)» (англ. General Data Protection Regulation) (далі – GDPR) [1].

Насамперед, одним з основних принципів GDPR є принцип підзвітності, який полягає в тому, що будь-які організації, а також посередники, що допомагають їм в обробці даних повинні бути здатні продемонструвати відповідність своєї діяльності до принципів захисту даних [1, ст. 5]. Іншим важливим принципом є можливість для користувачів вирішувати чи давати згоду на обробку власних даних [1, ст. 7]. У разі втрати даних організація зобов'язана сповістити уповноважені органи захисту інформації. Для досягнення консистентності було створено спеціальний механізм (англ. One-Stop-Shop & Consistency Mechanism), який стосується організацій, що мають представництва в декількох державах ЄС. Всю відповідальність за впровадження засобів захисту даних має бути покладена на головну уста-

нову з організації в одній країні. У разі порушення правил Регламенту або за втрату даних ЄС на організацію накладається штраф. Дані користувачів також підлягають захисту й за межами самого ЄС [1, ст. 3].

Згідно зі ст. 12 GDPR, користувачам надаються також певні права. По-перше, користувач має право вимагати від організації отримати свої дані в зручному, загальновживаному форматі для поширення. По-друге, користувачі мають право відмовитись від обробки власних даних, крім випадків, коли ці дані необхідні за законом чи контрактом. По-третє, особа має право на видалення особистих даних, що були зібрані організацією.

Організації, що обробляють персональні дані, зобов'язуються захищати дані за замовчуванням (privacy by default) та за дизайном (privacy by design). Конфіденційність за дизайном означає, що інформаційні та комунікаційні системи повинні бути побудовані таким чином, щоби принципи захисту інформації були не порушені.

Українським компаніям в частині захисту персональних даних потрібно звернути увагу на ч. 2 ст. 3 GDPR, яка передбачає екстратериторіальну дію закону. Вона встановлює, що правила регламенту застосовуються до обробки персональних даних контролером або обробником, який перебуває поза межами ЄС, якщо він здійснює обробку, збір, використання чи зберігання персональних даних суб'єктів із ЄС. Для пояснення конкретних пунктів щодо екстратериторіальної дії GDPR Європейська рада із захисту даних (англ. European Data Protection Board) також випустила роз'яснення щодо територіальної дії GDPR (Guidelines 3/2018 on the territorial scope of the GDPR) від 16 листопада 2018 р. [2]. Згідно з ними GDPR може застосовуватись до іноземних компаній, якщо: їх веб-сайт або додаток доступний мовою країни члена ЄС; компанія має домен, що зареєстрованим у зоні ЄС; компанія пропонує доставку чи надання послуг на території ЄС; приймає оплату в євро.

Тому GDPR є важливим документом, що захищає права користувачів, норми якого необхідно враховувати компаніям що працюють (або лише планують працювати) на ринку ЄС, якщо вони хочуть уникнути проблем з їх роботою на території ЄС. Серед нових норм, які запроваджені GDPR, і які відсутні, або потребують актуалізації в чинному законодавстві України, можна виділити: збільшення штрафів за неправомірну обробку чи збереження персональних даних до 2-4% загального річного обороту або 10-20 млн. євро в залежності від порушених правил і типу даних тощо [1, ч. 4 ст. 84]; надання права суб'єктам персональних даних обмежувати їх використання або обмежувати персональні дані які роботодавець має право робити публічним тощо [1, ст. 13]; запровадження чіткого механізму «надання згоди» на обробку персональних даних, за яким мовчання чи бездіяльність знаком згоди не вважаються, і згода має бути виражена у

формі ствердних, активних дій користувача тощо [1, ст. 7]; необхідність призначення відповідальної за захист персональних даних особи (англ. – Data Protection Officer, DPO), яка забезпечуватиме та матиме право перевіряти якість та законність обробки даних у конкретній компанії, якщо вона працює з великими обсягами чутливих даних, наприклад, медичними записами або відомостями про судимість [1, ст. 37]; право суб'єкта даних на отримання його або її персональних даних, які він надав контролеру, в структурованому, загальноприйнятому форматі, що легко зчитується машиною, та право на передавання таких даних іншому контролеру без перешкод від контролера, якому було надано персональні дані [1, ст. 20]. Додатково на компанії покладається обов'язок впроваджувати надійні механізми для забезпечення безпеки персональних даних – псевдонімізацію, шифрування, забезпечення обмеженого доступу до місць зберігання інформації [1, ст. 32].

Таким чином, існує необхідність в адаптації законодавства України сфері захисту персональних даних до права ЄС, особливо в частині штрафів, регулюючих органів та прав користувачів на обмеження доступу до приватних даних, і поки цей процес відбувається, українським компаніям, незалежно від того, розповсюджуються на них норми GDPR чи ні, бажано вже почати процес переходу на них. Для цього потрібно систематизувати наявні в них дані, почати належним чином вести їх облік та обробку, а також потрібно впевнитись у свідомій згоді користувачів щодо обробки їх персональних даних, та реальних обсягах їх збереження.

**Література**

1. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 р. про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних (Загальний регламент про захист даних). URL: https://zakon.rada.gov.ua/laws/file/text/63/f474904n8.pdf (дата звернення: 08.03.2020).

2. Adopted Guidelines 3 / 2018 On the territorial scope of the GDPR (Article 3) Version for public consultation. URL: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_3_2018_territorial_scope_en.pdf (дата звернення: 08.03.2020).

*УДК 343.321.2*
**Зейкан К. Т.**
**Тугарова О. К.**
кандидат юридичних наук, доцент,
Національна академія СБ України

# КЛАСИФІКАЦІЯ ТА ЗАСЕКРЕЧУВАННЯ СЕКРЕТНОЇ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ЕСТОНСЬКОЇ РЕСПУБЛІКИ

Сутність державної таємниці в Республіці Естонія описано в законі «про державну таємницю» Естонії, від 22 жовтня 1997 року. Цей закон встановляє підвалини та порядок віднесення інформації до державної таємниці в інтересах забезпечення безпеки Естонської Республіки, її засекречення, а також підстав для допуску до державної таємниці та порядку її захисту.

Згідно з законом Республіки Естонія «Про державну таємницю» державною таємницею є інформація, яка в інтересах забезпечення державної безпеки потребує захисту від розголошення, є об'єктом власності Естонської Республіки або знаходиться під її контролем або розроблена нею або для неї, якщо ця інформація віднесена до державної таємниці і засекречена на передбачених законом підставах і в порядку. Інформація, стан якої задовольняє вищезгадані умови може бути державною таємницею незалежно від виду її носія. Не може бути державною таємницею згідно законодавства службова інформація.

Крім того, в законі зазначаються категорії відомостей, які відносяться до державної таємниці. Згідно з законом, до державної таємниці відносяться відомості пов'язані з державною безпекою. Деталізація цього в статті 3.1) До державної таємниці може бути віднесена інформація, яка стосується:

1. планів, озброєння, постачання, резервів або операцій, пов'язаних з державною обороною;

2. систем, проектів, планів або потужності обладнання (установок), що мають відношення до державної безпеки;

3. інформації, розробленої іноземними або міжнародними організаціями або в результаті співпраці між Естонською Республікою і вищевказаними організаціями, стосовно якої встановлено вимогу про те, щоб ця інформація, її джерело або факт співпраці зберігалися в таємниці;

4. діяльності розвідки або контррозвідки, а також джерел і методів, використовуваних розвідкою або контррозвідкою;

5. міжнародних відносин, міжнародної зовнішньополітичної і зовнішньоекономічної діяльності Естонської Республіки, які зачіпають державну безпеку;

6. наукових, технологічних і економічних питань, які зачіпають державну безпеку;

7. криптографічних інформаційних систем і шифрувальної апаратури;

8. осіб, які надавали або щодо яких є підстави припускати, що вони надають Естонській Республіці інформацію з питань, що стосуються державної безпеки, за умови, що інформація або зв'язок з цими особами повинна зберігатися в таємниці;

9. іншої інформації, яка в інтересах забезпечення державної безпеки потребує захисту від розголошення, якщо таке рішення приймає особа, наділена правом віднесення інформації до державної таємниці» [1, с. 3].

Важливою ремаркою для системи охорони державної таємниці Естонії є пункт 3 статті 2 Закону. В ньому йдеться про те, що інформація відноситься до державної таємниці у випадку, якщо її розголошення може принести шкоду державній безпеці.

«Інформація, зазначена в частині 1 цієї статті, відноситься до державної таємниці, якщо її розголошення безпосередньо або в контексті іншої інформації може завдати шкоди державній безпеці. При цьому у випадках з іноземною інформацією, конфіденційними іноземними джерелами, а також джерелами та методами, використовуваними розвідкою і контррозвідкою, свідомо передбачається, що їх розголошення завдасть шкоди державній безпеці» [1, с. 2].

Відповідно до закону розрізняють грифи «цілком таємно» та «секретно».

(1) Для інформації, що становить державну таємницю, в залежності від її змісту, встановлюються три ступені секретності і відповідні їм грифи секретності для носіїв зазначеної інформації:

1) «цілком таємно» – якщо є вагома підстава вважати, що розголошення цієї інформації може спричинити непоправну шкоду для державної безпеки;

2) «секретно» – якщо є вагома підстава вважати, що розголошення цієї інформації може завдати шкоди державній безпеці.

(3) Іноземна інформація класифікується відповідно до ступеня її секретності, яка у внутрішньодержавному масштабі відповідає ступеню, що вимагається стосовно такої інформації в іноземній державі» [1, с. 5].

Особливістю системи охорони державної таємниці Республіки Естонія, що в Законі чітко визначені категорії віднесення до державної таємниці і не знаходяться в окремому документі, а також особливістю є акцент на формулюванні «Державна безпека», що вказує на керівну роль держави як суб'єкта забезпечення безпеки суспільства. Строк на який можливо віднести інформацію до державної таємниці не має перевищувати 50 років, а до інформації отриманої з розвідувальних або контррозвідувальних джерел тривалість може сягати до 75 років.

**Література**

1. О государственной тайне. Закон Республіки Естонія від 22 жовтня 1997 року. URL: http://estonia.news-city.info/docs/sistemsr/dok_iegiso.htm?fbclid=IwAR0TDS57-RL722fboTfCr-574KFkdnRpzkD_OlOrcdgeodp7LhgAGWsCOkY.

*УДК 343.321.2*

**Зейкан К. Т.**
**Шепета О. В.**
кандидат юридичних наук, доцент,
Національна академія СБ України

## КЛАСИФІКАЦІЯ ТА ЗАСЕКРЕЧУВАННЯ СЕКРЕТНОЇ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ФРАНЦУЗЬКОЇ РЕСПУБЛІКИ

Класифікація секретної інформації у Франції має специфічні особливості варті окремої уваги, по причині того, що має види інформації з обмеженим доступом аналогів яких немає в світі.

Законодавство про секретність національної оборони (про державну таємницю) визначено в Кримінальному кодексі. Згідно до Кримінального кодексу Франції, статті 413-9, державною таємницею є «процеси, об'єкти, документи, інформація, комп'ютерні мережі, комп'ютеризовані дані або файли національної оборони, які були предметом заходів класифікації, спрямованих на обмеження їх поширення і класифікуються як секрети національної оборони» [1; с. 46].

У Франції секретною є інформація оборонного значення, яка за ступенем секретності поділяється на 3 рівні :

Confidentiel Défense («Конфіденційна оборонна»): інформація, розголошення якої вважається потенційно небезпечним для національної оборони, або може призвести до розкриття інформації, віднесеної до вищого рівня безпеки.

Secret Défense («Секретна оборонна»): інформація, розголошення якої може завдати істотної шкоди для національної оборони. Така інформація не може поширюватися без дозволу відповідних властей, крім виняткових ситуацій.

Très Secret Défense («Надзвичайно секретна оборонна»): інформація, розголошення якої вважається вкрай небезпечним для національної оборони. Ніяка організація не має права здійснювати зберігання, передачу, відображення або знищення інформації цього рівня секретності без дозволу прем'єр – міністра Франції або секретаря національної оборони. Част-

кове або вибіркове відтворення цієї інформації також суворо заборонено. Менш чутлива з точки зору оборони інформація у Франції визначається як «захищена» та поділяється на такі рівні в міру зростання:

1. Non Protégé (незахищена).

2. Diffusion restreinte administrateur («поширення обмежене адміністрацією»).

3. Diffusion restreinte («поширення обмежене»).

4. Confidentiel personnels Sous-Officiers («Конфіденційно, для молодших службовців»).

5. Confidentiel personnels Officiers («конфіденційно, для службовців») [2].

Процедура розсекречення документів, в сфері реалізується незалежним та окремим органом від розвідувального товариства, Консультативною комісією із захисту таємниць національної оборони.

Розголошення секретної інформації у Франції є злочином, передбаченим статтею 413-9 Кримінального кодексу. У разі несанкціонованого витоку секретної інформації проводиться розслідування компетентними органами, до яких належать Міністерство внутрішніх справ Франції, спеціальний слідчий з оборони та безпеки відповідного міністерства, а також генеральний секретар національної оборони. За розголошення секретної інформації Кримінальний кодекс Франції передбачає покарання до 7 років позбавлення свободи і 100 000 євро штрафу, а якщо злочин скоєно з необережності чи недбалості – до 3 років позбавлення волі і 45 000 євро штрафу [3].

Крім, згаданих вище типів інформації, в системі інформації з обмеженим доступом Франції є вид інформації, котрий не має аналогів в інших системах інформації з обмеженим доступом, це інформація з позначкою «spécial France» («тільки для громадян Франції»), яка не є рівнем секретності.

Французька система охорони державної таємниці має більш поглиблене структурування і деталізацію, та більшу кількість грифів, порівняно з системами охорони державної таємниці інших держав.

Таке ускладнення характерно, відображається і на функціях посадових осіб, які працюють з державною таємницею в Франції, бо режим секретної інформації для кожної інформації різний крім того, ознаки режимів секретності можуть переплітатися, чим ускладнюють її класифікацію, а як наслідок віднесення до правильної категорії.

**Література**

1. Кримінальний кодекс Французької Республіки. URL: https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070719&idArticle=LEGIARTI000020933029&dateTexte=20180928 (Дата звернення 5.03.2020).

2. Стаття 413 – 9. *Кримінальний кодекс Французької Республіки*. URL:https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070719&idArticle=LEGIARTI000020933029&dateTexte=20180928.
3. Information classée secrète en France. URL: https://fr.wikipedia.org/wiki/Information_class%C3%A9e_secr%C3%A8te_en_France (Дата звернення 5.03.2020).

*УДК 34.037*
**Клименко К. О.**
**Костенко О. В.**
НДІ інформатики і права НАПрН України

## СУЧАСНИЙ СТАН ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СФЕРІ АДВОКАТУРИ

В умовах розвитку інформаційно-комунікаційні технології створюються суспільні відносини, невід'ємною складовою яких є обробка даних в електронному вигляді. Ці зміни торкнулися і сфери адвокатури, що суттєво покращило швидкість і якість адвокатської діяльності і одночасно викликало багато проблемних питань з інформаційної безпеки.

На сьогодні питання інформаційної безпеки діяльності адвоката досліджується вітчизняними та закордонними фахівцями досить активно. Однак ці дослідження спрямовані на створення локальних адміністративних або технічних рішень. В той же час питання створення комплексної системи інформаційної безпеки адвоката є малодослідженими, що становить проблему, яку потрібно вирішувати.

В умовах поширення новітніх інформаційних технологій, створення державних і недержавних реєстрів, інформаційних систем і баз даних, формування національного і глобального інформаційного простору та розвитку інформаційного суспільства проблема інформаційної безпеки та захисту персональних даних стає однією із ключових в систем і захисту прав і безпеки людини.

Для української адвокатури цифровізація відіграє значну роль і місце. Розвиток інформаційно-комунікаційних технологій дає адвокату широкий вибір інструментів для забезпечення інформаційної діяльності, а саме:

– технічні (смартфони, комп'ютери, телекомунікаційні мережі, сканери, принтери, фото-, аудіо- відео реєстратори тощо);

– спеціалізовані адвокатські інформаційні ресурси (Єдиний реєстр адвокатів та реєстри адвокатських об'єднань, електронний кабінет адвоката);

– спеціалізовані судові інформаційні ресурси: електронний суд, Єдиний державний реєстр судових рішень, Державний реєстр атестованих судових експертів, Реєстр методик проведення судових експертиз, Єдиний реєстр приватних виконавців України;

– державні інформаційні реєстри: Єдиний державний реєстр юридичних осіб та фізичних осіб-підприємців, Єдиний державний реєстр нормативно-правових актів, Державний реєстр речових прав на нерухоме майно, Державний реєстр обтяження речового права на нерухоме майно, Єдиний реєстр боржників, Державний реєстр актів цивільного стану громадян тощо;

– спеціалізовані інформаційні реєстри нотаріальної сфери: Єдиний реєстр спеціальних бланків нотаріальних документів, Єдиний реєстр нотаріусів, Реєстр спеціальних бланків документів інформаційної системи Міністерства юстиції України, Єдиний реєстр довіреностей, Спадковий реєстр тощо;

– спеціалізовані інформаційні реєстри Міністерства внутрішніх справ України, Держгеокадастру, Міністерства освіти, МТСБУ тощо.

Фактично під контролем адвоката зосереджується достатньо інформації різних видів: відкрита, з обмеженим доступом, конфіденційна, службова, така, що містить державну, банківську, нотаріальну, лікарську та адвокатську таємницю, обмеженого використання.

В той же час проблеми захисту інформації та персональних даних покладаються виключно на адвоката.

З метою створення належних умов інформаційної безпеки в сфері адвокатури доцільно розробити та впровадити типову комплексну систему захисту інформації адвоката, яка би включала:

– технічний захист інформації (захист інформації від несанкціонованого доступу, захист інформації від витоку технічними каналами);

– організаційні заходи захисту інформації (комплекс адміністративних та обмежувальних заходів, спрямованих на оперативне вирішення задач захисту шляхом регламентації діяльності адвоката і порядку функціонування засобів (систем) забезпечення інформаційної діяльності та засобів (систем) забезпечення технічного захисту інформації.

Розробка комплексних заходів інформаційної безпеки потребує модернізації законодавчої бази, що регулює діяльність адвокатури та внесення нових сучасних норм та дефініцій, в тому числі таких як «інформаційна діяльність адвоката» та «інформаційне забезпечення діяльності адвоката», що сприятиме адаптації адвокатської діяльності до європейського правого поля і забезпечення вимог законодавства і сфері захисту інформації та персональних даних.

**Література**

1. Пилипчук В.Г. Розвиток системи захисту персональних даних в контексті забезпечення інформаційної безпеки людини, суспільства, держави / В.Г. Пилипчук: Всеукраїнська науково-практична конференція «Актуальні проблеми управління інформаційною безпекою держави», електронне видання НА СБУ, 2019. – 99 с.

2. Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96.

*УДК 343.1*
**Князєв Д. С.**
**Князєв С. О.**
кандидат юридичних наук,
старший науковий співробітник,
Національна академія СБ України

# ОЦІНКА ВАЖЛИВОСТІ ІНФОРМАЦІЇ

Реалії сучасного життя людини тісно пов'язані із постійним використанням різноманітної інформації. Загалом, термін «інформація» (від лат. informatio-роз'яснення, викладення, обізнаність), який по суті є багатозначним та багатоаспектним, використовується для опису та пояснення різних процесів та явищ. Ще у XIX столітті британські економісти пропонували враховувати інформацію як складову капіталу, вказуючи на те, що знання та організація є потужними двигунами виробництва.

Згідно визначенню UNESCO – інформація є універсальна субстанція, що пронизує усі сфери людської діяльності та яка слугує втіленню знань та думок, є інструментом спілкування, взаєморозуміння та співробітництва, встановлює стереотипи мислення та поведінки.

Варто згадати й Закон України «Про інформацію»,який під поняттям «інформація», розуміє будь-які відомості та/або дані, які можуть бути збережені на матеріальнихносіях або відображені в електронному вигляді.

Кількість наявної у світі інформації має стійку тенденцію до збільшення її кількості у геометричній прогресії.

Отже, із поняттям «інформація» тісно пов'язано і поняття «кількість інформації» або «обсяг інформації». Обсяг інформації досить часто співвідносять із числовою характеристикою певної кількості інформації з кількістю саме цінної, важливої інформації.

Звідти, перед споживачем інформації цілком логічним постає питання щодо можливості виділення серед усього масиву саме тієї інформації яка потрібна йому для задоволення своїх інформаційних потреб. Такі потреби можуть бути пов'язані з роботою, навчанням, вибором товару, отриманням довідкової інформації тощо.

Разом з тим, отримана різноманітними шляхами інформація, навіть якщо вона й стосується потрібної сфери, може дати найбільшу користь за умови виділення із наявного масиву більш корисної, важливої інформації. Таке аналітичне опрацювання прийнято співвідносити із способами оцінювання інформації, що у першу чергу включає:об'єктивність, достовірність, значимість, своєчасність, узгодженість, повноту, можливість використання і т.п.

Наприклад, рівень достовірності інформації залежить від джерела її отримання й може поділятись на: абсолютно надійний; звичайно надійний; не дуже надійний; не надійний; не відомий.

Причинами не достовірності інформації можуть бути: цілеспрямоване викривлення (дезінформація); не передбачуване викривлення у результаті впливу випадкових завад; помилки під час фіксації інформації тощо.

Також при оцінці інформації слід враховувати такий фактор як ергономічність, тобто – зручність форми або обсягу інформації для даного користувача.

Спрощений алгоритм оцінки важливості інформації може виглядати наступним чином: отриману інформацію оцінюють з точки зору співвідношення із необхідною сферою (напрямом діяльності і т.п.). Далі питання її достовірності. Потім – актуальність. Після цього, за необхідності, здійснюється оцінка за іншими критеріями.

Оцінка важливості інформації логічно ґрунтується на основних принципах інформаційних відносин визначених у статті 2 Закону України «Про інформацію», серед яких:

гарантованість права на інформацію;

відкритість, доступність інформації, свобода обміну інформацією;

достовірність і повнота інформації;

свобода вираження поглядів і переконань;

захищеність особи від втручання в її особисте та сімейне життя.

А також правомірність одержання, використання, поширення, зберігання та захисту інформації. Даний принцип охоплює й сферу обігу інформації з обмеженим доступом.

Відповідно до Законів України «Про інформацію» та «Про доступ до публічної інформація» інформація з обмеженим доступом поділяється на: конфіденційну, службову і таємну.До категорії таємно відносяться комерційна таємниця, державна таємниця та інші передбачені законом таємниці.

Стосовно комерційної таємниціїї важливість визначається власником з урахуванням, у першу чергу, переваг які вона йому надає у комерційному середовищі. Крім того, у комерційному обігу виділяють «виробників» та «користувачів» інформації. Сформувався й «інформаційний ринок» на якому продаються та купуються «інформаційні продукти» як масиви акумульованої інформації, яка спеціально розрахована на користувача.

Оцінка важливості державної таємниці співвідноситься з обрахуванням можливої шкоди національній безпеці у випадку не правомірного використання державної таємниці.

Таким чином, оцінку важливості інформації можливо визначити як певний процес спрямований на визначення узагальненого показника, що характеризує з однієї сторони значимість інформації з огляду тих завдань на вирішення яких вона спрямована, а з іншого методи та способи організації її обробки.

**Література**

1. Закон України «Про інформацію» // ВВР. – 1992. – № 48. – ст. 650.

2. Закон України «Про доступ до публічної інформації» // ВВР. – 2011. – № 32. – ст. 314.

3. Архипов О. Ворожко В. Системні аспекти оцінювання рівня важливості секретної інформації // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, 2(15) вип., 2007. – С. 10–12.

*УДК 32.019.51*

**Когут В. Є.**
**Шемаєв В. М.**
доктор військових наук, професор,
Національна академія СБ України

## МІФ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ ПРО ЗРИВ УКРАЇНОЮ МІНСЬКИХ ДОМОВЛЕНОСТЕЙ

Переглядаючи сторінки історії, можна спостерігати, що проти України завжди була направлена державна політика Росії, зокрема інформаційна. А нині можна спостерігати ще більший натиск на наш імідж та в цілому на державу, суспільство та окрему особу. Тому важливим є розуміти, яка інформація є неправдивою, на кого вона впливає і як протистояти такому впливу. Одним з методів протистояння є розвінчування міфів Російської Федерації, які найчастіше лунають з перших вуст російського керівництва, офіційних представників та засобів масової інформації.

Одним з прикладів міфів можна назвати міф Російської Федерації про зрив Україною Мінських домовленостей, що був поширений засобами масової інформації, висловлений в офіційному виступі президента В. Путіна, а також представником Російської Федерації у Міжнародному суді.

Мінські домовленості були вимушеним кроком для України, що передбачав не лише урегулювання збройного конфлікту, а й встановлення особливого статусу Донбасу. Також це було способом уникнення подальшого розгортання бойових дій з прямою чи непрямою участю Росії – для України, а для Росії – повного зняття санкцій США та Європи, які були запроваджені після анексії Криму. Це мало показати, що Російська Федерація бажає мирно врегулювати конфлікт, хоча б задля послаблення цих санкцій. Ще одна сторона цих домовленостей – посланець ОБСЄ, представник ЄС та США виступав посередником, суддею для ефективності переговорів.

Багато експертів вказують на те, що Мінські домовленості мали безліч неточностей, через те й не були такими успішними. Наприклад, можна сказати декілька слів про підписантів даної домовленості: це не були глави України та Росії, наша держава поклала обов’язки представника в цих домовленостях на Другого Президента України – Леоніда Кучму, а Росія,

в свою чергу, – на свого посла в Україні, Михайла Зурабова. Варто звернути увагу також і на інших учасників даних переговорів – представників, яких ніхто не призначав і не обирав, із самопроголошених республік, які не були визнані світовою спільнотою. Інші аспекти, що завадили успішності домовленостей, – це відсутність чіткого визначення щодо особливого статусу Донбасу, способів завершення бойових дій та механізмів реалізації положень протоколів Мінських домовленостей [1].

Щодо міфу про зрив домовленостей – Росія заявляла, що українські військові одразу після підписання домовленостей, порушили «режим тиші». Проте це є дезінформацією, за допомогою якої намагалися дискредитувати позицію України на світовому рівні, особливо перед сторонами, які допомагали у врегулюванні конфлікту. Росія зазвичай використовує для цього потужні канали ЗМІ, що мають високі рейтинги та ступінь довіри великої аудиторії людей. Також вони можуть бути спрямовані не лише на своє населення, але й на населення України та Європейської спільноти. Гучні слова в сторону України звучать особливо переконливо для російського народу з вуст їхнього президента, який навіть не соромиться використовувати відверту брехню у своїх виступах [2].

Вже довгий час Російська Федерація тримає під прицілом Україну, яка повсякчас відчуває на собі різні види атак. Серед них вже є приклади військових, психологічних, інформаційних, економічних, фінансових атак. Також широко застосовують політичні і культурні атаки. Тому гібридну війну України з Росією не можна назвати суто військово-інформаційною, адже цей процес захопив й інші сфери життя нашої держави. Багато дослідників доводять, що російські історики навіть змінюють історію своєї держави, задля переконання своїх громадян та усього світу, що їхня держава завжди була могутньою і поклала початок низці інформаційних, політичних і культурних процесів.

Щорічно уряд Росії витрачає від 1,4 до 8 мільярдів доларів на інформаційні атаки, які не лише поширюються на нашу державу, а й виходять далеко за її території і досягають як сусідніх держав України, так і далеких куточків світу. Але ця війна відбувається не за окремі території, а за окремих людей, їх прихильність і віру [3].

В цих умовах для України є важливим популяризувати свою справжню культуру, рідну мову, традиції та досягнення в Європі та світі в цілому. Варто просувати українські канали на міжнаціональному рівні, розказувати про нашу історію доступно та цікаво і навчати такій історії сучасну молодь та дітей, які також потребують належного інформаційного виховання.

Крім того, Україні сьогодні важливо аналізувати інформаційні потоки задля розроблення стратегії захисту власного інформаційного простору, протидії ворожим атакам і забезпечення виховання у суспільстві «імуніте-

ту» до неправдивих новин, виступів, статей та інших продуктів гібридної війни Росії.

**Література**

1. https://commons.com.ua/uk/minski-ugodi-istoriya-interesi-perspektivi/.
2. https://www.ukrinform.ua/rubric-world/2770858-rosia-vikoristovue-dezinformaciu-dla-rozkolu-ta-manipulacii.html.
3. http://publications.lnu.edu.ua/bulletins/index.php/journalism/article/viewFile/8339/8293.

*УДК 34:004*

**Кузьменко В. В.**
**Пуркар Д. П.**
**Шепета О. В.**
кандидат юридичних наук, доцент,
Національна академія СБ України

## ЯК ЗАХИСТИТИ ПЕРСОНАЛЬНІ ДАНІ НА ТЕЛЕФОНІ У СУЧАСНИХ УМОВАХ

На сьогодні телефонні пристрої є найбільш використовуваними електронними пристроями у світі, у яких зберігається не тільки інформація з мережі Інтернет, а й персональні дані користувача. Існує безліч порад та способів, які допоможуть забезпечити безпеку ваших персональних даних. Як не дивно, це є найпростішими базовими правилами пошуку в Інтернеті та користування мережею, яких необхідно дотримуватись.

Якщо звернутися до термінології, то відповідно до закону України «Про захист персональних даних», персональні дані –це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Відомо, що зараз на телефоні будь-якої особи зберігається неймовірна кількість інформації про неї та її життя, такої як паспортні дані, паролі від банківських карт, особиста інформація та навіть біометричні дані, наприклад, відбиток пальця. У разі, коли інформація такого типу потрапляє до зловмисників, це може нанести значної матеріальної або ж моральної шкоди особистості, якій належали вказані дані.

Для того, щоб впевнитись у безпеці ваших даних на телефонному пристрої, ні в якому разі не слід зберігати фото або знімки екрану, де зазначені паспортні дані, ідентифікаційний код, банківські рахунки, фото прав на авто та інших документів, завдяки яким можна ідентифікувати особу та підробити її особистість.

Також рекомендовано використовувати неслабкі та небанальні паролі від пошти, акаунтів у соціальних мережах, банкінгу та ін. Впевненість у

надійності пароля дає впевненість у тому, що сама особа докладає зусиль до збереження власних персональних даних [3].

Для запобігання інфікуванню шкідливими програмами варто здійснювати своєчасне оновлення операційної системи та окремих додатків, яке передбачає виправлення вразливостей та помилок в програмному забезпеченні. На локальному рівні дотримання усіх рекомендацій у кіберпросторі називається кібергігієною [2].

Необхідним кроком для уникнення втрати важливих даних є регулярне резервне копіювання інформації на зовнішній жорсткий диск або у, так звану, хмару. Це допоможе відновити потрібні дані у разі їх шифрування програмою-вимагачем або видалення шкідливим програмним забезпеченням. До того ж не менш важливим правилом кібергігієни є використання надійного рішення для захисту смартфона від різних загроз, зокрема програм-вимагачів, шпигунських програм, вірусів, троянів та фішинг-атак, тобто антивірусів, програм-чисток та видаленняхешованої інформації та кукі-файлів. На сьогодні одним з найбільш діючих методів захисту інформації та доступу до паролів є двухфакторнааутентифікація, яка передбачає підтвердження особистості під час входу в певний акаунт [1].

Для зручності існують спеціальні програми, які допомагають відслідкувати чи викрадені ваші паролі зловмисниками. Відомо, що слід завантажувати тільки найнеобхідніші мобільні додатки та файли, адже будь-яка програма, завантажена з Інтернету, ставить під загрозу всю інформацію на смартфоні. Також під час завантаження кожного додатку варто звертати увагу на дозволи, які ви надаєте. Часто шкідливі програми надсилають запит на отримання великої кількості дозволів, які не відповідають їх функціоналу.

Ці основні рекомендації кібергігієни допоможуть Вам своєчасно виявити підозрілу діяльність зловмисників та запобігти втраті персональних даних та іншої особистої інформації. Із зазначеного вище, стає зрозумілим, що недотримання вимог безпечного користування телефоном або іншим цифровим пристроєм, може призвести до втрати, викрадення та зловмисного використання персональних даних особи, що у подальшому призведе до фінансових збитків або може нанести моральної шкоди особі.

**Література**

1. Конфіденційна інформація, інформація про особу та персональні дані: співвідношення і регулювання // [Електронний ресурс]. – Режим доступу: https://cedem.org.ua/analytics/konfidentsijna-informatsiya-informatsiya-pro-osobu-ta-personalni-dani-spivvidnoshennya-i-regulyuvannya/.

2.Як вберегти персональні дані під час роботи в мережі?- поради // [Електронний ресурс]. – Режим доступу: https://cybercalm.org/novyny/yak-vberegty-personalni-dani-pid-chas-roboty-v-merezhi-porady/.

3. Як захистити персональні дані на мобільному телефоні: поради експерта // [Електронний ресурс]. – Режим доступу: https://konkurent.in.ua/publication/44344/yak-zahistiti-personalni-dani-na-mobilnomu-telefoni-poradi-eksperta/.

*УДК 343.9:343.346.8:004*

**Леонов О. С.**
Воєнно-дипломатична академія
імені Євгенія Березняка

## ТЕНДЕНЦІЇ ЩОДО УНОРМУВАННЯ БОРОТЬБИ З ДЕЗІНФОРМАЦІЄЮ В УКРАЇНІ ТА ЇХ ВПЛИВ НА БЕЗПЕКУ КОРИСТУВАЧІВ СОЦІАЛЬНИХ МЕРЕЖ

Розвиток та популяризація соціальних медіа-ресурсів призвели до того, що сучасний медіапростір став важливим майданчиком для ведення інформаційного протиборства. Дедалі частіше джерелами поширення дезінформації являються різноманітні соціальні мережі, месенджери, та інші інтернет-платформи. В умовах гібридного протистояння з Російською Федерацією, в якому інформаційний чинник відіграє не останню роль, потреба у боротьбі з правопорушеннями в інформаційній сфері являється актуальним питанням, що потребує негайного вирішення.

Намагаючись розв'язати проблему з розповсюдженням фейкової інформації, у січні 2020 року Міністерство культури, молоді та спорту України презентувало законопроєкт «Про протидію дезінформації» [1]. У ньому вказані основні виклики українському інформаційному середовищу та їх можливі варіанти вирішення. Зокрема, в даному законопроєкті вказано на прогалини у чинному законодавстві України, яке не передбачає можливості звернення до суду з приводу розповсюдження дезінформації та, як наслідок, відсутності відповідальності за її поширення. Автори законопроєкту також вказують на низьку медіаграмотність населення України, неможливість ідентифікувати особу, яка розповсюджує масову інформацію, та знецінення статусу журналіста. Щоб розв'язати дану проблему, проєктом визначено наступні кроки. По-перше, пропонується створити посаду уповноваженого з питань інформації, основними функціями якого будуть фіксація та перевірка інформації на предмет наявності ознак дезінформації за відповідними зверненнями, та звернення до суду із позовами про спростування та надання права на відповідь щодо дезінформації. Крім цього, законопроєктом передбачено обов'язкове навчання основам медіаграмотності, а також створення так званого «індексу довіри», що підтверджуватиме дотримання медіа принципів журналістської етики та вимог щодо

перевірки інформації. Щодо поширювачів масової інформації, їх планують зобов'язати розміщувати власні ідентифікаційні дані, щоб мати змогу визначити, хто створює і поширює масову інформацію. Цікавим розділом законопроєкту являється створення організації журналістського самоврядування, яка буде слідкувати за дотриманням професійної етики та стандартів, а також встановлення адміністративної та кримінальної відповідальності за системне та умисне масове розповсюдження дезінформації.

Треба відзначити, що опублікування даного законопроєкту досить серйозно здивувало маже весь український медіа-ринок. Більшість пунктів законопроєкту сприйнялись як обмеження роботи ЗМІ, свободи вираження поглядів та самоцензури. Проти реєстрації цього законопроєкту виступили Комісія з журналістської етики, низка народних депутатів з Комітету з питань гуманітарної та інформаційної політики, Рада з питань свободи слова та захисту журналістів при президентові України [2], Моніторингова місія ООН [3], представники ОБСЄ та генеральний секретар Європейської федерації журналістів [4].

Виходячи з вище сказаного, нескладно спрогнозувати, що у нинішньому вигляді законопроєкт «Про протидію дезінформації» навряд чи буде ухваленим. Беручи до уваги необхідність розбудови в Україні ефективного механізму протидії розповсюдженню дезінформації, необхідно знайти баланс між дотриманням демократичних прав суспільства та забезпеченням інформаційної безпеки, спираючись на досвід європейських держав. До уваги можна взяти Німеччину [5], де операторів соціальних мереж зобов'язали невідкладно видаляти контент, який містить очевидно протиправну інформацію під загрозою серйозних штрафних санкцій. 22 листопада 2018 року у Франції [5] ухвалили законопроєкт щодо «боротьби з маніпулюванням інформацією», згідно якому національний регулятор отримав повноваження для припинення трансляції телеканалів, що контролюються іноземною державою. Поряд із цим, у грудні 2018 р. керівництво Великої Британії та Республіки Польща [5] домовилися про створення спільного підрозділу з протидії поширенню дезінформації (насамперед з боку РФ).

Як бачимо, унормування боротьби з дезінформацією ( в першу чергу через середовище соціальних мереж) являється не лише українським питанням. Протидія поширенню фейків як головної загрози інформаційному середовищу, турбує і європейське суспільство. Тому для ефективного вирішення вищезазначеної проблеми необхідна консолідація профільних фахівців та досвід передових країн світу.

**Література**

1. Презентація законопроекту «Про протидію дезінформації». URL: http://mkms.gov.ua/files/InformPolityka.pdf (дата звернення: 03.03.2020).

2. Роботу на законопроектом про дезінформацію продовжили мінімум на місяць. URL: https://detector.media/infospace/article/174577/2020-02-07-robotu-nad-zakonoproektom-pro-dezinformatsiyu-prodovzhili-minimum-na-misyats/ (дата звернення: 07.03.2020).

3. Закон про дезінформацію: в ООН застерігають українську владу від «непотрібних обмежень» для ЗМІ. URL: https://www.radiosvoboda.org/a/news-oon-pro-zakon-pro-dezinformatsiu/30410220.html (дата звернення: 05.03.2020).

4. У ОБСЄ висловили занепокоєння щодо положень законопроєкту про протидію дезінформації. URL: https://www.radiosvoboda.org/a/news-obse-dezir-zakonoproyekt-dezinformatsiya/30393652.html (дата звернення: 04.03.2020).

5. Черниш Р.Ф. Правовий досвід країн Європейського Союзу у сфері протидії поширенню фейкової інформації. URL: http://pgp-journal.kiev.ua/archive/2019/10/22.pdf (дата звернення: 08.03.2020).

*УДК 351/354*

**Лепецький Т. Б.**
Національна академія СБ України

## ДОДАТОК ДЕРЖАВНИХ ПОСЛУГ «ДІЯ» – КРОК ВПЕРЕД У ВЗАЄМОВІДНОСИНАХ ГРОМАДЯН ТА ДЕРЖАВИ

Відповідно до ст. 3 Конституції України, найвищою соціальною цінність в Україні визнаються: людина її життя та здоров'я, честь та гідність недоторканість та безпека. Відповідно до цієї статті, права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави, передбачається, що держава відповідає перед людиною за свою діяльність [1]. Виходячи з даного положення, можна зробити висновок, що одним із завдань держави та її органів, є охорона прав людини, сприяння її законній діяльності спрямованій на реалізацію прав та законних інтересів. Так для реалізації функцій держави, спрощення механізму одержання громадянами послуг органів державної влади, 6 лютого Міністерство цифрової трансформації презентувало мобільний додаток «Дія», завданнями якого є мінімізація бюрократичних процесів шляхом:розміщення в ньому електронних документів, отримання через додаток державних послуг, а у подальшій перспективі, ще й можливість участі через додаток у виборах різних рівнів. Реалізація такого проекту призведе не тільки до оптимізації надання державних послуг, а і до мінімізації рівня корупції в даному напрямі. До кінця 2020 року уряд планує оцифрувати близько 80% державних послуг та зробити їх доступними через «Дію». Зокрема, незабаром у додатку має з'явитись український та закордонний паспорти, студентський квиток, страхові поліси тощо [2].

Під брендом «Дія» (укр. Держава і я) працює не тільки мобільний додаток для смартфонів, а і Єдиний веб-портал електронних послуг, в якому кілька разів на місяць, як обіцяють у Мінцифрі, розширюватимуть сервіс. На презентації мобільного додатку чиновники похвалилися досягненнями і в цьому напрямі. Так, прем'єр-міністр відзвітував про запуск електронного кабінету забудовника, що «вперше в історії дозволило ухвалювати рішення про видачу документа не людині, а алгоритму, знизивши кількість відмов до нуля», також додаток принесе користь і молодим батькам, адже тепер з'явилася можливість реєструвати новонароджених онлайн просто з палати пологового будинку. Звичайно, від традиційної смуги перешкод у вигляді походів по кабінетах одразу ніхто не відмовиться. Зазначається також, що онлайн-режиму віддають перевагу тільки 9% українців. Щоб розвіяти таке «мракобісся» доцифрової епохи, Мінцифра запустила проект з навчання цифрової грамотності, де всім охочим пояснюють, як ефективно користуватись додатком [4]. Поки на національній онлайн-платформі доступні три освітні серіали – базові цифрові навички (сезон 1, сезон 2, сезон 3),цифрові навички для вчителів і серіал для батьків «Безпека дітей в інтернеті». Згодом будуть з'являтись нові освітні серіали.

Важливим напрямком діяльності держави є підтримка малого і середнього бізнесу, представники якого формують основу середнього класу, який у свою чергу і відображає реальний добробут в державі. Щоб не словом, а ділом надавати допомогу в створенні та реалізації нових ідей, в додатку відображатимуться такі онлайн-послуги:

– Каталог бізнес ідей зі зручними шаблонами;

– Перелік усіх необхідних юридичних документів для відкриття бізнесу;

– Онлайн-сервіси та програми підтримки для підприємців на одній сторінці;

– Довідки підприємці – на основі матеріалів профільних державних органів та провідних компаній України;

– Кейси контретних проблем, питань та запитів.

Вже навесні запрацює новий блок-консалтинг-зона для підприємців. Кожен підприємець зможе отримати онлайн-консультацію із фахівцями за допомогою відеозв'язку. Консультуватись можна на теми систематизації бізнес-процесів фінансового управління, взаємодії з державою, психології бізнесу, HR, маркетингу та продажів. Відкриття першої консалтинг-зони для підприємців заплановано на Квітень – Травень 2020 року у Харкові [7].

В процесі функціонування додатку важливо не забувати і про безпеку даних, які будуть циркулювати в ній. Розробники запевняють, що додаток зберігає мінімум інформації про своїх користувачів, що і вимагає ч. 3 ст. 6 Закону України «Про захист персональних даних», усі дані передаються і зберігаються у шифрованому вигляді, а для частини критичних даних використовується блокчейн технологією розподіленого зберігання даних [2, 5].

Блокчейн – це мегамозок, який зберігає в собі необмежену кількість інформації. А блоки – це його звивини пам'яті, які нереально замінити або підмінити. Тому що механізм дуже ретельно перевіряє попередні дані і якщо побачить помилку або шахрайство, то просто проігнорує запит на виконання. А тепер простіше. Блокчейн – це величезна записна книжка, де в блоках зберігається інформація про транзакції, угоди, контракти всередині мережі та все це представлено в криптографічному вигляді. Також блоки формують строгий ланцюг, а для того щоб створити новий блок, потрібно поступово зчитати інформацію про старі блоки [5].

Піднімаючи тему блокчейн, хочеться сказати ще про таке:

• Blockchain як технологія вже відбулась, а процес змін вже почався, і він незупинний. Питання тільки в тому, хто перший в цьому буде найкраще розбиратись?

• Блокчейн – це технологія, яка дозволяє реалізовувати найстійкіші цифрові реєстри в світі. Увага: це рішення доступне будь-якій людині чи об'єкту з доступом до інтернету та практично безкоштовно. Корпорації та держави витрачають мільярди доларів для забезпечення цілісності своїх даних.

• Трансконтинентальні корпорації намагаються знайти застосування технології в своїх процесах, так як це справді може економити їм сотні мільйонів доларів щороку.

• Наразі відбувається стрімка адаптація технології до традиційних секторів економіки.

• Кількість успішних стартапів у цій сфері в десятки разів більша, ніж в традиційному IT.

• Бази даних публічних блокчейн не підконтрольні жодній з організацій чи держав.

• Запис в публічні блокчейни доступний абсолютно кожному. Варто тільки мати незначну технічну підготовку.

• Використання Blockchain дуже часто зводить нанівець потребу в посередниках.

• Держави розглядають та ухвалюють законодавчі ініціативи в цьому напрямку.

• Стенфорд, Гарвард та інші ТОП-університети світу почали з 2016 року активно вивчати Blockchain.

**Література**

1) Ст. 3 Конституції України.

2) https://plan2.diia.gov.ua/.

3) http://novobuzka.gromada.org.ua/news/1581322955/.

4) https://amp/s/ua.112.ua/statji/dokumenty-zalyshte-vdoma-yak-pratsiuie-prohrama-diia-i-chomu-pratsiuie-ne-u-vsikh-524900-amp.html.

5) Ч. 3 ст. 6 ЗУ «Про захист персональних даних».
6) https://ideyne.com/ua/article/blokchein__potencial_21_stolet.
7) https://amp/s/www.epravda.com.ua/news/2020/02/28/657571/index.amp.
8) https://dou.ua/lenta/articles/why-is-blockchain-in-trends/.

*УДК: 329.09.5*
**Лисенко Д. Ю.**
**Шепета О. В.**
кандидат юридичних наук, доцент,
Національна академія СБ України

## СУЧАСНІ ТЕХНОЛОГІЇ МАНІПУЛЮВАННЯ СУСПІЛЬНОЮ СВІДОМІСТЮ ТА ЇХ ВПЛИВ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ ДЕРЖАВИ

В Оксфордському тлумачному словнику англійської мови слово маніпуляція (manipulation) трактується як поводження із об'єктами зі спеціальним наміром, особливою метою, як ручне управління, ручні дії. У переносному значенні словник визначає маніпуляцію як акт впливу на людей або управління ними із зневажливим контекстом, як приховане управління чи обробка.

В інформаційному аспекті маніпулятивний вплив є особливим видом інформаційного впливу, при якому інформація виступає як засіб примушення особи до здійснення вчинків, які є невластивими або неприйнятними для неї.

У загальному випадку маніпуляція може призвести до таких наслідків руйнування людської свідомості [3]:

- некритичне сприйняття інформації та подій, що відбуваються;
- неадекватне розуміння ситуації;
- байдуже сприйняття подій;
- викривлення уявлень про події;
- маніакальне споживання інформації;
- страх перед інформацією (інфофобія) тощо.

Небезпека реалізації інформаційних загроз значно зростає через застосування різноманітних методів, методик і прийомів маніпулятивного інформаційно-психологічного впливу з урахуванням їх дії на суспільну та індивідуальну свідомість. Основні технології маніпуляції суспільною свідомістю розглянемо далі.

Однією із сучасних маніпулятивних технологій є інформаційно-пропагандистський вплив на суспільство [4].

Принциповою особливістю пропаганди є нав'язування інформації зверху від суб'єкта до об'єкта, тобто реалізація спрямованості комунікації «зверху-донизу». Ефективність такого впливу буде визначатися тим, на-

скільки суб'єкт впливу є авторитетним для об'єкта впливу. Тому принципово важливим моментом для пропаганди є максимальне завищення статусу суб'єкта.

Принциповою особливістю пропаганди є нав'язування інформації зверху від суб'єкта до об'єкта, тобто реалізація спрямованості комунікації «зверху-донизу». Ефективність такого впливу буде визначатися тим, наскільки суб'єкт впливу є авторитетним для об'єкта впливу. Тому принципово важливим моментом для пропаганди є максимальне завищення статусу суб'єкта [2].

До маніпулятивних технологій суспільною свідомістю відносяться також ПР-технології.

На думку Г.Г. Почепцова будь-яка кампанія в галузі ПР може розглядатися як інформаційна міні-війна, оскільки в ній завжди присутні агресивні цілі (не за способом досягнення, а за результатом). ПР-технологія як технологія маніпуляції суспільною свідомістю на $180^{o}$ змінює схему впливу пропаганди. ПР основним в комунікації вважає зв'язок від об'єкта впливу (тобто від аудиторії, народу). ПР будується навколо двох центральних понять цільова аудиторія й ключове повідомлення.

Принциповою особливістю ПР є завищення статусу об'єкта впливу. Для технології маніпуляції це є небезпечним, оскільки претензії висловити нікому, все, що робиться суб'єктом, подається від імені народу (об'єкта), а тому і звинуватити суб'єкт неможливо.

Ще однією новою маніпулятивною технологією є нейролінгвістичне програмування (НЛП).

Спочатку НЛП спеціалізувалося на моделюванні методів роботи видатних американських психотерапевтів Ф. Перлза, М. Еріксона, В. Сатир. Перші техніки и моделі НЛП представляли собою формалізовані прийоми їх роботи з пацієнтами. Це привело багатьох НЛП-істів в психологію і психотерапію, а психологів і психотерапевтів в НЛП. Це значною мірою пояснює те, що часто НЛП вважають напрямком в психології або/і набором психотерапевтичних технік, не дивлячись на те, що такі визначення доволі сильно розходяться з точкою зору принаймні одного з засновників НЛП – Джона Гріндера [1].

Сучасний рівень знань та технологічні можливості надали такої різноманітності каналам і формам інформаційно-психологічного впливу, що не буде великим перебільшенням говорити про глобальні масштаби його використання. На користь привабливості застосування інформаційно-психологічного впливу свідчать такі його переваги в порівнянні з відомими зразками зброї масового ураження:

– Масовість впливу. Вже зараз розміри телеаудиторій при показі окремих подій перевищують рубіж у два мільярди. І цей показник має тенденцію постійного зростання;

– Вибірковість впливу. Методи інформаційно-психологічного впливу дозволяють, використовуючи ті ж самі канали, впливати як на окрему

державу, так і організувати дискредитацію, наприклад, окремих верств суспільства або відтворити бажаний імідж політичному діячу тощо.

– Висока рентабельність засобів. Інформаційна зброя надана суспільству самою природою, вона не потребує великих капітальних вкладів, а ефективність від її застосування може мати вирішальне значення. Крім того, її застосування не руйнує матеріальні цінності країни, які є метою впливу, і при вдалому використанні дає слухняну робочу силу (людський ресурс).

– Практична відсутність міжнародних правових актів щодо заборони та регламентації засобів, методів та форм впливу (це пов'язане, в першу чергу, з прихованою дією: так, інформаційно-психологічний вплив легко прикрити боротьбою ідей, полемікою з опозицією, приватними висловами, привабливими ідеями: типу відкритого суспільства, тощо) **.**

Потрібно зазначити, що без необхідного контролю залишаються й різні канали інформаційного впливу на осіб, які приймають рішення у сфері державного управління. Зокрема, необхідна організація рефлексивного аналізу потоків вхідної інформації й процесів її обробки з метою виявлення загрози потенційного управління особами, що приймають рішення.

**Література**

1. Бутузов В.М. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз): моногр. / В.М. Бутузов; Рада нац. безпеки і оборони України, Міжвід. наук.-дослід. центр з пробл. боротьби з організ. злочинністю. – К.: КИТ, 2010. – 408 с.

2. Жарков Я.М. Історія інформаційно-психологічного протиборства : підруч. / [Я.М.Жарков, Л.Ф.Компанцева, В.В.Остроухов, В.М.Петрик, М.М.Присяжнюк, Є.Д.Скулиш] ; за заг. ред. Є.Д.Скулиша. – К. : Наук.-вид. відділ НА СБ України, 2012. – 202 с. (Затверджено МОН молоді та спорту України).

3. Кара-Мурза С.Г. Маніпуляція свідомістю: навч. посіб. – К.: Оріони, 2003. – 500 с.

4. Литвиненко О.В. Спеціальні інформаційні операції та пропагандистські кампанії : моногр. / О.В. Литвиненко. – К.: ВКФ Сатсанга, 2000. – 222 с.

*УДК: 340.1*

**Лукашенко М. І.**
Інститут підготовки юридичних
кадрів для Служби безпеки України
Національного юридичного
університету імені Ярослава Мудрого

## КІБЕРБЕЗПЕКА УКРАЇНИ В УМОВАХ РОСІЙСЬКОЇ АГРЕСІЇ

Останнім часом в межах кіберпростору України спостерігається збільшення кількості небезпечних дій, що спрямовані на завдання шкоди ін-

тересам нашої держави. З огляду на те, що зазначені дії вчиняються через використання комп'ютерних систем та в кіберпросторі України, подібний злочин йменується кібернетичною інтервенцією або кібернетичною війною.

Дійсно, інтервенція має місце, оскільки відбувається вчинення насильницьких посягань зі сторони інших суб'єктів на політичні, економічні, державні інтереси, шляхом втручання в процес функціонування їх учасників.

На сьогодні, прикладом поєднання на різних рівнях різноманітних комбінацій методів та форм негативного впливу, в межах якого лідируючим напрямом є саме кібернетичний та інформаційний, слід вважати гібридну війну Росії проти України.

В умовах проведення військових дій на Сході, захист та належне функціонування кібернетичного простору є одним із пріоритетних завдань нашої держави [1, с. 111].

Нажаль, спостерігається негативна тенденція щодо зростання обсягів матеріалів інформаційного характеру, котрі мають відверту антиукраїнську спрямованість та упереджене висвітлення майже всіх зовнішніх та внутрішніх процесів, що мають місце як на території України, так і за її участю на міжнародному рівні.

Найбільш вразливими у кіберпросторі від періодичних кібератак стали приватні та державні компанії, і як свідчать факти, вони зовсім були не готові до них. Причиною цьому є відсутність в нашій державі на теперішній час ефективних механізмів та інструментів, метою яких будуть превентивні дії щодо можливих атак, а також протидія таким. Однак на сьогодні ми можемо спостерігати лише недієві та безуспішні заходи.

Актуальним є дослідження кіберзагроз, що існують внаслідок розвитку інформаційного суспільства в умовах військової агресії з боку Російської Федерації. Але спочатку слід визначити що являє собою поняття кібербезпеки.

Так, серед науковців існують різні погляди на зазначене поняття. Деякі з них, під кібербезпекою пропонують розуміти стан захищеності важливих інтересів держави, суспільства та особи як від внутрішніх, так і від зовнішніх загроз, що пов'язані із використанням ресурсів інформаційно-телекомунікаційних систем, так званого кіберпростору, за наявності якого забезпечуються гарантовані умови для реалізації державної інформаційної політики.

В свою чергу, відповідно до Стратегії кібербезпеки України, що затверджена Указом Президента України від 15.03.16 року № 96/2016, даний термін визначений як «стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі [2].

Головним завданням Стратегії кібербезпеки України постає формування умов для безпечного існування кіберпростору держави, використання його в інтересах особи та суспільства. Даним документом також пе-

редбачається ряд заходів, що спрямовані на протидію кіберзагрозам, поглибленню міжнародної співпраці в зазначеній сфері, забезпечення захисту державних електронних інформаційних ресурсів та інфраструктури в інформаційній сфері.

Одним із заходів на виконання даної Стратегії стало створення Радою національної безпеки і оборони України Національного координаційного центру кібербезпеки, що функціонує як робочий орган Ради.

Є зрозумілим, що і до агресії з боку Російської Федерації в Україні спостерігалася велика кількість кіберзлочинів, коли під атаку хакерів потрапляли банки, інтернет-магазини, сайти різних політичних партій. Але наразі, з існуванням агресії, ця кількість, а також їх інтенсивність зросла у великих масштабах, та слід також зауважити, що наслідки таких злочинів призводять до необхідності витрачання чималої суми.

Найбільш поширеним різновидом кіберзлочину сьогодні є кардінг – крадіжка грошей з банківських карток, електронних рахунків. Для вчинення таких злочинів, російськими спецслужбами залучаються як власні хакери, так і хакери з іноземних країн, метою цього є дестабілізація країн, які є ідейними супротивниками. Також, можна спостерігати високий рівень інтеграції хакерів з військовими організаціями, державними і приватними структурами, що спричинено наявністю різних інтересів та чималих коштів [3, с. 331].

Ще одним прикладом кіберзлочину можна навести руйнівні кібератаки, які мали місце у 2014 році, і були спрямовані на комп'ютерні мережі Центральної виборчої комісії. Це відбулося за тиждень до виборів, однак на щастя, всі заходи щодо дискредитації результатів голосування, що готувалися російськими спецслужбами, було вчасно нейтралізовано та відновлено роботу телекомунікаційного та серверного обладнання [4].

Отже, задля ефективної боротьби з кіберзлочинами в нашій державі, необхідним є розроблення належних та дієвих інструментів регулювання національної державної політики у відповідній сфері, посилення кібернетичного захисту об'єктів, що перебувають в районі проведення воєнних дій на сході країни, та які віднесені до критичної інформаційної інфраструктури. Необхідним заходом також є проведення повного та широкомасштабного моніторингу кібернетичного простору, з метою своєчасного виявлення та оперативної нейтралізації кібернетичних загроз.

**Література**

1. Лук'янчук Р.В. Державна політика у сфері забезпечення кібернетичної безпеки в умовах проведення антитерористичної операції / Р.В. Лук'янчук // Вісник НАДУ : зб. наук. праць. – 2015. – Вип. 3. – С. 110-116.

2. Стратегія кібербезпеки України: затверджена Указом Президента України від 15 березня 2016 року № 96/2016 [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/96/2016#n2.

3. Грицюк Ю.І. Кіберінтервенція та кібербезпека України: проблеми та перспективи їх подолання. Науковий вісник НЛТУ України. 2016. Вип. 26.8. [Електронний ресурс]. – Режим доступу: http://nltu.edu.ua/nv/Archive/2016/26_8/52.pdf.

4. Інформаційна та кібербезпека в сучасному світі: досвід СБУ [Електронний ресурс]. – Режим доступу: https://ua-news.liga.net/politics/opinion/informatsiyna-ta-kiberbezpeka-v-suchasnomu-sviti-dosvid-sbu.

*УДК 351.86*

**Малай О. О.**
Національна академія СБ України

## ДЕРЖАВА У СМАРТФОНІ: БЕЗПЕКА ОСОБИСТИХ ДАНИХ УКРАЇНЦІВ

Країна, де публічні послуги в онлайн, а міністерства оцифровані, – вимога сучасності. Адже кожен день ми в середньому витрачаємо в інтернеті 6 годин і 42 хвилини [1]. Але коли країна в цифрі і онлайн, безпека даних – ключове завдання. Про запуск програми «Дія» чув мало не кожен українець. В основному чули те, що це і є та сама «Держава в смартфоні». У даній статті ми розглянемо що потрібно знати про мобільний додаток, як він працюватиме, якими послугами можна буде скористатись через нього, і чи безпечно це.

Під час виборчої кампанії Володимир Зеленський казав, що вірить у створення «держави в смартфоні», яка полегшить життя українців.

“Дія” (скорочення від «Держава і я») – це онлайн-сервіс, що згодом стане універсальною точкою доступу громадян і бізнесу до всіх електронних державних послуг за єдиними стандартами. Як вказано на сайті самого порталу “Дія” це:

6. Портал (онлайн-сервіс державних послуг, де все швидко, чітко й зрозуміло. Тут можна отримати послугу там і тоді, коли потрібно).

7. Застосунок (мобільний застосунок з електронними документами, та даними про людину з реєстрів).

8. Освіта (портал з онлайн-курсами: базовий із цифрової грамотності, для вчителів і для батьків «Онлайн-безпека дітей»).

9. Бізнес (портал з допомоги малому і середньому бізнесу).

10. ЦНАПи (центри надання адміністративних послуг у кожному куточку України. У майбутньому Центри Дії) [2].

За півроку після старту проекту президент разом із командою Міністерства цифрової трансформації презентував мобільний додаток «Дія». На теперішній час застосунок «Дія» завантажили понад 1,7 млн разів. Урядо-

вий додаток міцно закріпився на перших позиціях українських App Store і Play Market, випередивши популярні сервіси Tik Tok, Telegram, YouTube і Viber.

На поточний момент в застосунку «Дія» доступні водійські права і «техпаспорт» в електронному вигляді. Після авторизації ці документи повинні автоматично з'явитись у смартфоні. Якщо документів немає, застосунок пропонує верифікувати їх в електронному кабінеті водія. Після обробки даних документи синхронізуються із додатком. У березні повинні з'явитись цифровий поліс страхування на авто, цифровий студентський, цифровий паспорт та цифровий закордонний паспорт, а у квітні - штрафи на авто, цифровий податковий номер та дані з реєстрів.

І тут виникає питання – а що ж з безпекою даних і чи можна взагалі цьому всьому довіряти?

Зважаючи на необхідність доступу до особистої інформації, у Міністерстві цифрової трансформації України наголошують на високому ступені захисту додатку.

Коли користувач тільки завантажив «Дію», перше, що він робить – авторизується з програми за допомогою технології BankID. Ця технологія дає громадянину можливість пройти ідентифікацію через свій банк, у якому зберігається необхідна інформація про клієнта. Такий спосіб ідентифікації є досить надійним і його застосування – традиційна практика для багатьох розвинених країн світу. До застосунку підключені популярні Приватбанк, а також система BankID Національного банку України, в яку входять 12 банків, а, як всім відомо, до банківських систем пред'являються високі вимоги безпеки.

Забезпечити високий рівень захисту застосунку багато в чому дозволила співпраця з компанією EPAM – одним зі світових лідерів у сфері IT-розробок.

«Архітектура «Дії» побудована таким чином, що на серверній частині програми не здійснюється постійне зберігання персональних даних користувачів. При цьому інформація в каналах передачі даних передається в зашифрованому вигляді, а на деяких етапах використовується подвійне шифрування» (мін. цифр. транс. Михайло Федоров.)

Захист персональних даних у мобільному застосунку «Дія» виконаний за кращими практиками безпеки для рішень такого типу, використано підхід «глибокого захисту» (defense-in-depth).

Крім того, разом з IT-фахівцями EPAM серйозно підійшли до тестування застосунку. Зокрема провели так звані пен-тести, тобто тестування безпеки програми. Тобто спробували, в тому числі із залученням зовнішніх IT-фахівців, «хакнути» «Дію», щоб виявити всі вразливі місця.

Платформа використовує блокчейн технологію, що не дозволить ні хакеру, ні чиновнику змінити дані. При будь-якій спробі злому, система автоматично створює нову копію даних і блокує втручання.

В підсумку можна сказати, що забезпечення безпеки – це не результат, а процес. Над «Дією» працює команда професіоналів, що постійно розвиває і покращує мобільний застосунок. Це дозволяє сказати, що «Дія» на сьогоднішній день є достатньо захищеним застосунком. Але на 100% убезпечитися від абсолютно всіх вразливостей неможливо.

**Література**

1. wearesocial.com [Електронний ресурс] : [Інтернет-портал]. – Електронні дані. – [2008–2020 We Are Social Ltd.]. – Режим доступу: https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates.

2. Державні послуги онлайн – Дія [Електронний ресурс] : – [diia.gov.ua, 2020]. – Режим доступу: https://plan2.diia.gov.ua/.

*УДК 342.95 (477)*

**Микитенко Я. Р.**
Національна академія СБ України

## АКТУАЛЬНІ ПРОБЛЕМИ АДМІНІСТРАТИВНОЇ ВІДПОВІДАЛЬНОСТІ ЮРИДИЧНИХ ОСІБ ЗА ВЧИНЕННЯ ПРАВОПОРУШЕНЬ В ІНФОРМАЦІЙНІЙ СФЕРІ

В сучасному світі, з розвитком та поширенням ринкових відносин юридичні особи все більше впливають на суспільне життя. Враховуючи той факт, що Україна стоїть на порозі переходу до інформаційного суспільства, варто звернути особливу увагу на вплив юридичних осіб на забезпечення інформаційної безпеки.

Слід погодитись із науковцями, які зазначають, що саме юридичні особи як суб'єкти інформаційних відносин можуть становити загрозу, вчиняючи адміністративні правопорушення в інформаційній сфері [1, с. 19]. Наведемо окремі адміністративні правопорушення в інформаційній сфері передбачені Кодексом України про адміністративні правопорушення (далі – КУпАП), котрі можуть бути вчинені в інтересах юридичних осіб:

– ненадання інформації для ведення колективних переговорів і здійснення контролю за виконанням колективних договорів, угод (ст. 41-3);

– приховування, перекручення або відмова від надання повної та достовірної інформації за запитами посадових осіб і зверненнями громадян та їх об'єднань щодо безпеки утворення відходів та поводження з ними (ст. 82-3);

– неповідомлення (приховування) або надання неправдивої інформації про загрозу посівам, деревним насадженням, іншій рослинності відкритого та закритого ґрунту, а також продукції рослинного походження від шкідливих організмів (п. 3, ч. 1 ст. 83-1);

– порушення правил реалізації, експлуатації радіоелетронних засобів та випромінювальних пристроїв, а також користування радіочастотним ресурсом України (ст. 146);

– порушення правил охорони ліній і споруд зв'язку (ст. 147);

– демонстрування і розповсюдження фільмів без державного посвідчення на право розповсюдження і демонстрування фільмів (ст. 164-6);

– порушення умов розповсюдження і демонстрування фільмів, передбачених державним посвідченням на право розповсюдження і демонстрування фільмів (ст. 164-7);

– недотримання квоти демонстрування національних фільмів у разі використання національного екранного часу (ст. 164-8);

– незаконне розповсюдження примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, баз даних (ст. 164-9);

– порушення порядку подання інформації та виконання рішень Антимонопольного комітету України та його територіальних відділень (ст. 166-4);

– невиконання законних вимог національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації (ст. 188-7);

– порушення законодавства у сфері захисту персональних даних (ст. 188-39);

– порушення законодавства про державну таємницю (ст. 212-2);

– порушення права на інформацію (ст. 212-3) [2].

На даний момент КУпАП на відміну від інших нормативно-правових актів, зокрема, Закон України «Про відповідальність за правопорушення у сфері містобудівної діяльності» [3], Закон України «Про державне регулювання ринку цінних паперів» [4], Закон України «Про охорону культурної спадщини» [5], не визначає юридичну особу як суб'єкта відповідальності, що на нашу думку є прогалиною у законодавстві, і потребує усунення.

Отже, можна дійти висновку, що стан правового регулювання інституту адміністративної відповідальності не відповідає потребам сьогодення і підлягає удосконаленню. Одним із актуальніших напрямів такого реформування повинно стати запровадження у КУпАП адміністративної відповідальності юридичних осіб, зокрема, відповідальності за вчинення правопорушень в інформаційній сфері.

**Література**

1. М. М. Присяжнюк, О. О. Климчук, С. М. Сидоренко Організаційно-правові основи забезпечення інформаційної безпеки: Курс лекцій. Київ : Нац. акад. СБУ, 2017. 328 с.

2. Кодекс України про адміністративні правопорушення: Закон України від 07 грудня 1984 р. № 8073-X / Верховна Рада Української РСР. *Відомості Верховної Ради Української РСР.* 1984. №51. Ст. 1122.

3. Про відповідальність за правопорушення у сфері містобудівної діяльності: Закон України від 14 жовтня 1994 р. № 208/94-ВР / Верховна Рада України. *Відомості Верховної Ради України*. 1994. № 46. Ст. 411.

4. Про державне регулювання ринку цінних паперів в Україні: Закон України від 30 жовтня 1996 р. № 448/96-ВР / Верховна Рада України. *Відомості Верховної Ради України*. 1996. № 51. Ст. 292.

5. Про охорону культурної спадщини: Закон України від 8 червня 2000 р. № 1805-III / Верховна Рада України. *Відомості Верховної Ради України*. 2000. № 39. Ст. 333.

*УДК 354.42/.44*

**Миткалик М. С.**
Національна академія СБ України

## ДЕСТРУКТИВНИЙ ВПЛИВ РЕКЛАМИ В СОЦІАЛЬНИХ МЕРЕЖАХ

Сучасне суспільство важко уявити без Інтернету та соціальних мереж, в яких звичайна людина проводить велику частку свого часу. Швидкий прогрес та інформаційна революція дали змогу людству швидше та ефективніше розвиватися. Разом із тим, емоційна насиченість реклами в соціальних мережах дозволяє здійснювати інформаційні маніпулятивні впливи на свідомість як окремої особи, так і населення з метою зміни (корекції) їх світогляду, певних цілей, планів і вчинків.

Таку рекламу в соціальних мережах можна назвати інформаційною зброєю, оскільки вона базується на використанні особливостей людини та соціуму. Наприклад, вчені Кембриджського університету виявили, що навіть про те, як користувач ставить «лайки» у Фейсбук або Інстаграм, можна багато чого розповісти, адже сучасні комп'ютерні програми дозволяють отримати певну інформацію з соціальних мереж та здійснити її аналіз [1].

З активним розвитком соціальних мереж значення набули реклами, які автоматично з'являються в наших «гаджетах» та можуть містити інформацію з закликами приєднатись до злочинних діянь, або іншого неправомірного дійства. І що важливо, користувачі не можуть відмовитися чи заблокувати цю рекламу, бо так запрограмований додаток.

Виникає питання, скільки ж коштів витрачається для того, щоб примусово донести будь-яку інформацію суспільству. Дослідження показують, що ціна реклами в Інстаграмі та Фейсбуці залежить від кількості її повторів. До прикладу, тариф «Інста-М», та «Фейс-М» за 5 повторів вимагає 299 доларів, а пакети «Інста-XL» та «Фейс-XL» коштують 799 доларів за 30 повторів.

Обмеження цієї реклами здійснюється лише певними додатками, які фільтрують інформацію, що суперечить моральним принципам суспільст-

ва, з нецензурною лексикою та порнографією. Дослідження фахівців Національного університету імені В. Н. Каразіна показують здатність зазначеного сервісу прогнозувати масові акції, та інші події значно швидше, ніж певні структури зі значним випередженням. При цьому, інформація, що має негативний (деструктивний) вплив, відслідковується відповідними органами, але по факту, коли інформація вже поширилася на користувачів.

Що стосується збору інформації, варто зазначити, що з соціальними мережами пов'язаний новий вид розвідки – розвідки у соціальних мережах – «social media intelligence», або «SOCMINT», який повною мірою використовують як силові, так і різноманітні цивільні структури [2].

Кількість людей, що мають свій профіль в соціальному медіа-маркетингу, динаміка їх взаємодії та часу перебування, що збільшується, – важливі чинники інтересу такої складової комунікації, як реклама. Компанії, що управляють соціальним медіа-маркетингом, збирають детальні дані про кожного клієнта, які надходять від створення профілю та від ведення історії діяльності користувачів. Маючи інформацію про особу та її діяльність, такі компанії розуміють, який вид реклами буде найбільш сприйнятливий для неї. Наприклад, якщо особа цікавиться хімією, змішуванням хімічних сполук, злочинці в соціальних мережах з легкістю можуть «підкинути» їй рекламу з закликами до співпраці щодо виготовлення незаконних хімічних препаратів за привабливу ціну. Вірогідність того, що особа погодиться на це є великою.

Виникає питання щодо протидії деструктивному впливу реклами в соціальних мережах та забезпечення інформаційної безпеки населення.

**Література**

1. Гвоздик О. Соціальні мережі – вільний обмін думками чи маніпулювання свідомістю? [Електронний ресурс] / О. Гвоздик. – Режим доступу: http://xpress.sumy.ua/article/society/5700.

2. Попова Т. Соціальні мережі, кібератаки та гібридні війни [Електронний ресурс]. – Режим доступу: http:/www.radiosvoboda.org/a/28598299.html.

*УДК 39.394*

**Михайлова А. Ю.**
Національна академія СБ України

## МІФИ РОСІЙСЬКОЇ ПРОПАГАНДИ ПРО ВІДСУТНІСТЬ ЇХ ВІЙСЬКОВОЇ ТЕХНІКИ І ВІЙСЬКОВОСЛУЖБОВЦІВ НА ТИМЧАСОВО НЕКОНТРОЛЬОВАНІЙ УКРАЇНОЮ ТЕРИТОРІЇ ДОНБАСУ

Російська окупація Донбасу є складовою "гібридної" війни проти України, що розпочалася у лютому 2014 році з незаконної анексії Криму.

Проте все ще існує набір міфологем, котрі російські медіа артикулюють постійно та методично. Їх переважно використовують, коли потрібно знищити супротивника, показати його слабкість.

*Доказами російської агресії на сході України неодноразово ставали і могили російських військових*, які вдавалося виявити журналістам та активістам. Так, у жовтні 2014-го у російському Кронштадті поховали 18-річного Є. Пушкарьова – бойовика – кулеметника, який утік з дому воювати на Донбасі протии України.

На початку 2015 року СБУ викрила, що Росія н намагається приховати загибель своїх солдатів на Донбасі за допомогою підміни їх документів.

Загалом, попри *наявність великої кількості вагомих доказів, які доводять, що російські військові, зброя та техніка залучені у бойових діях на Донбасі*, Росія свою причетність до цього усіляко заперечує. Заступник голови Спеціальної моніторингової місії ОБСЄ Александр Гуґ в інтерв'ю виданню Foreign Policy заявив, що вона не зафіксувала «на місцях прямих доказів» участі Росії в конфлікті на Донбасі. «Водночас ми бачили конвої, які залишали й в'їжджали до України на ґрунтових дорогах посеред ночі в місцях, де немає офіційного кордону», – додав заступник голови СММ ОБСЄ. При цьому Гуґ заявив: «ми бачили людей із прикметними знаками Російської Федерації».

У середині травня 2015 року українські військові під час бою біля міста Щастя Луганської області затримали двох бойовиків – Євгена Єрофеєва та Олександра Александрова. Під час прес-конференції у Генштабі ЗСУ журналістам показали спеціалізовану безшумну снайперську гвинтівку Єрофеєва – «Вінторез», яку випускають на Тульському збройовому заводі і якою користуються російські війська спецпризначення. На допиті затримані підтвердили, що є російськими військовослужбовцями з тольятинської бригади ГРУ. Утім, Міністерство оборони Росії це заперечило, стверджуючи, що вони звільнилися з російського війська ще у грудні минулого року.

Дуже влучно ситуацію охарактеризував депутат Європарламенту Е. Брок: "Найгірше, що може трапитися з Росією – це якщо Україна стане демократичною та економічно успішною державою, де пануватиме верховенство права. Це буде катастрофою для Кремля…" [1].

Російська присутність на Сході України фіксується також структурами НАТО. За оцінками Голови військового комітету НАТО генерала П. Павела, у військовій структурі і місцевих адміністраціях "ДНР-ЛНР" працює багатотисячний контингент російських фахівців [2].

Проведений аналіз інформаційних джерел беззаперечно свідчить про наявність військової техніки і військовослужбовців РФ на тимчасово неконтрольованій Україною території Донбасу.

**Література**

1. Элмар Брок: Худшее, что может случиться с Кремлем, – демократическая и экономически успешная Украина. – УНИАН, 23 декабря 2016. [Електронний ресурс]. – Режим доступу: http://interfax.com.ua/news/interview/392660.html.

2. В адміністраціях "Л/ДНР" працює 3-5 тисяч російських фахівців – НАТО. – Радіо Свобода, 4 травня 2018 р. - [Електронний ресурс]. – Режим доступу: https://www.radiosvoboda.org/a/ news/29208416.html.

*УДК 004.056:327.5 (045)*

**Міщенко Д. В.**
**Хомич О. Р.**
Національний технічний університет України
«КПІ імені Ігоря Сікорського»і

## ЗАГАЛЬНІ ЗАСАДИ ДЕРЖАВНОЇ ПОЛІТИКИ КІБЕРБЕЗПЕКИ (НА ПРИКЛАДІ США ТА УКРАЇНИ)

Забезпечення інформаційного суверенітету, формування ефективної системи безпеки в інформаційній сфері є актуальною проблемою для України, яка часто є об'єктом зовнішньої інформаційної експансії, маніпулятивних пропагандистських технологій та руйнівного інформаційного вторгнення. За ефективністю та наслідками застосування «кіберзброї» [3, с. 12], можна прирівняти до зброї масового ураження. Тому забезпечення кібербезпеки в Україні – одна з основних проблем, що викликає занепокоєння. Розглянемо систему, що була розроблена владою Сполучених Штатів Америки для забезпечення інформаційної безпеки держави.

В основі підходу Сполучених Штатів Америки до проблем захисту міжнародного кіберпростору лежить переконаність в тому, що технології мають величезний потенціал для країни і світу. Так, у 2005 р. в США було прийнято Федеральну програму **Дослідження та розробка мереж та інформаційних технологій** (Networking and Information Technology Research and Development (NITRD) на здійснення діяльності якої щорічно виділяється 2,5 мільярда доларів. Програма NITRD забезпечує наукові дослідження і розробки, спрямовані на забезпечення технологічного лідерства США в сфері розробки передових мереж, обчислювальних систем та програмного забезпечення. Програма NITRD здійснює наукові дослідження і розробки для задоволення потреб федерального уряду для великих мереж, обчислювальних систем і програмного забезпечення, пов'язаних з інформаційними технологіями. В рамках Програми NITRD здійснюється комплекс заходів, спрямованих на прискорення розробки і впровадження технологій з метою: зміцнення національної оборони і національної без-

пеки; підвищення конкурентоспроможності США і розвиток довгострокового економічного зростання; а також поліпшення якості життя [3, с. 24].

Підписана Президентом США в 2011 році **Міжнародна стратегія дій у кіберпросторі (Процвітання, безпека і відкритість в мережевому світі) (**International Strategy for cyberspace (Prosperity, Security and Openness in a Networked World) розкриває план співпраці між країнами і народами з метою його реалізації, а також визначає головні характеристики: відкритість для інновацій; взаємодія по всьому світу; надійність, здатна підтримати роботу [2].

Відповідно до п. 5 ч. 1 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. № 2163-VIII: «кібербезпека – 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» [1].

В Україні державна політика щодо захисту кібербезпеки покладається на низку державних органів, а саме на Державну службу спеціального зв'язку та захисту інформації України, Національну поліцію України, Службу безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України. В кожному із зазначених органів діють відповідні підрозділи.

Проте, незважаючи на велику кількість кримінальних проваджень, що з кожним роком збільшується на 2,5 тисяч, Департамент кіберполіції Національної поліції України не озвучує реальних результатів таких розслідувань. Наприклад, звітуючи за 2018 рік НПУ, вказуючи на кількість виявлених правопорушників у кількості 800 осіб, немає жодної інформації про кількість реальних обвинувальних вироків, винесених судами щодо притягнення вказаних осіб до відповідальності. Зі звіту незрозуміло, чи оголошено всім вказаним особам підозру, чи висунуто обвинувачення та в якому статусі вони перебувають.

Підсумовуючи наведене вище, слід констатувати наявність справжньої кризи в системі кібербезпеки в Україні. Хакерські атаки (на кшталт вірусу Petya у 2017 р.) є відповіддю на численні питання про сучасний стан кіберзахисту України. За кілька років війни Україна так і не спромоглася захистити свій кіберпростір. Тим більше, впровадженням закону № 2163-VIII не вдалося «залатати дірки» технічної неспроможності та відсутності висококваліфікованих спеціалістів цієї сфери на державній службі. Тому в Україні необхідно створити окрему організацію за прикладом програми NITRD у США та ліквідувати всі вже існуючі установи, що регулюють інформаційну безпеку в Україні, тому що вони з року в рік виявляють свою неспроможність протистояти як численним кібератакам, так і забезпечити дотримання чинного законодавства, що стосується захисту інформації.

**Література**

1. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. № 2163-VIII. Відомості Верховної Ради України. 2017. № 45. Ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 08.03.2020).

2. International Strategy for cyberspace (Prosperity, Security and Openness in a Networked World), [2011]. 30 с. URL: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (дата звернення: 08.03.2020).

3. Елин В. М. Сравнительный анализ правового обеспечения информационной безопасности в России и за рубежом: монография / под ред. Баранова А.П. [Б.м.], [2016]. 182 с. URL: https://publications.hse.ru/mirror/pubs/share/folder/ie7oj6cz00/direct/202314863 (дата звернення: 08.03.2020).

*УДК 316.625*

**Мокієнко О. С.**
Національна академія СБ України

## ІСТОРИЧНІ ВИТОКИ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ПРОТИБОРСТВА

Аналіз витоків інформаційно-психологічного протиборства (ІПсП) варто починати з «Трактатів про воєнне мистецтво» відомого китайського філософа і полководця IV ст. до н. е. Сунь-Цзи, елементи яких використовуються до цього часу. На його думку, одним із найефективніших методів ведення війни є введення в оману, що є актуальним і в сучасних реаліях. Проте, історики визначають й інші методи впливу на ворога за допомогою слова, які використовувались ще з давніх-давен. Один з яких полягає у тому, що в таборі противника поширювали чутки про переваги своїх військ. Внаслідок чого, створювався певний психологічний тиск. Інший метод використовувався під час збройної боротьби і передбачав створення рисунків та написів на каменях із закликами до супротивника – тогочасні аналоги нинішніх листівок.

Яскравим історичним прикладом є дії царя спартанців Лісандра (Стародавня Греція), який удвічі підняв платню гребцям на власних кораблях, а афінянам оголосив, що вони отримають таку саму платню, якщо перейдуть до нього на службу. Внаслідок чого, афінський флот залишився майже без гребців, а спартанцям вдалося здобути перевагу на морі без кровопролиття. Ще один приклад, коли перський воєначальник Ксеркс перед військовим походом на Грецію навмисно поширив чутки про численність перського війська у вигляді легенди про те, що якщо всі перські

воїни одночасно випустять стріли в повітря, то вони затьмарять світло сонця. Це створило певний художній образ, який у свою чергу максимального деморалізував ворога [1].

У Стародавньому Китаї використовувався інформаційно-психологічний вплив за допомогою пропагування справедливого характеру війни зі свого боку і несправедливого з боку противника. «Написане до початку війни політичне обвинувачення противника служило в ході всієї війни основним документом для обґрунтування законності дій сторони, що написала його» [2].

Цей метод ІПсП активно використовується і в XXI ст., підтвердженням чого є дії Російської Федерації, щодо Автономної Республіки Крим і тимчасово окупованих територій Донецької та Луганської областей.

У Стародавньому Римі досить успішно використовували риторику як засіб переконання проти своїх ворогів та як засіб для створення сприятливих умов у суспільстві для застосування агресії щодо супротивників. Так, полководець Сципіон Африканський, прибічник війни з Карфагенською державою, кожний свій виступ в Сенаті закінчував фразою: «Втім, Карфаген має бути знищений». Цей прийом багатократного повторення певної тези активно використовується й сьогодні.

Варто зазначити, що у Стародавньому Римі маніпулятивний вплив на суспільство здійснювався не лише у військових цілях. Суспільством маніпулювали також під час судових засідань, голосувань (виборів), задля підвищення та закріплення авторитету вищих посадових осіб тощо. Саме з цією метою була заснована одна з перших газет під назвою «Acta diurna populi romani», основним завданням якої було здійснення пропагандистського впливу на населення [3].

Таким чином, можна зробити висновок, що ще з давніх-давен відбувається формування основних методів ІПсП як способу набуття тієї чи іншої переваги над противником, його ослаблення. Основними методами ІПсП у цей час були: використання найбільш очевидних суперечностей у таборі противника і внесення розколу в його ряди; дезінформування; залякування своєю могутністю; проголошення справедливого характеру війни зі свого боку і несправедливого – з боку противника; використання письмових джерел. Зазначені методи інформаційно-психологічного протиборства в давнину мали характер військових хитрощів, але з розвитком людства вони удосконалювалися, внаслідок чого, отримали своє відображення у військовій теорії. Нині можна стверджувати, що ключову роль у воєнному протистоянні посіло інформаційно-психологічне протиборство. Підтвердженням чого слугує думка проте, що у XXI столітті лідерство в міжнародному співтоваристві визначається не військовим або економічним показником, а саме здатністю контролювати інформаційний простір.

**Література**

1. Історія інформаційно-психологічного протиборства : підручн. / [Я. М. Жарков, Л. Ф. Компанцева, В. В. Остроухов В. М. Петрик, М. М. Присяжнюк, Є. Д. Скулиш] ; за заг. ред. д.ю.н., проф., засл. юриста України Є. Д. Скулиша. – Київ : Наук.-вид. відділ НА СБ України, 2012. – 212 с.

2. Інформаційно-психологічне протиборство: підручник. Видання третє доповнене та перероблене / [В. М. Петрик, В. В. Бедь, М. М. Присяжнюк та ін.]; за заг. ред. В. В. Бедя. – К.: ПАТ «ВІПОЛ», 2018. – 388 с.

3. Гібридна війна і журналістика. Проблеми інформаційної безпеки : навчальний посібник / за заг. ред. В. О. Жадька ; ред.-упор. : О. І. Харитоненко, Ю. С. Полтавець. – Київ : Вид-во НПУ імені М. П. Драгоманова, 2018. – 356 с.

*УДК 621.391:519.2*

**Мостюк Д. Л.**
**Конюшок С. М.**
кандидат технічних наук, доцент,
ІСЗЗІ Національного технічного
університету України «КПІ імені Ігоря Сікорського»і

## ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ МЕТОДУ ОЦІНКИ *k*-ВИМІРНОСТІ БУЛЕВИХ ФУНКЦІЙ

Відповідно до [1], однією з суттєвих складових забезпечення інформаційної безпеки є запобігання порушення конфіденційності інформації. Основним інструментом за допомогою якого забезпечується конфіденційність інформації наразі є криптографічний захист інформації, в першу чергу, шляхом застосування сучасних алгоритмів шифрування. Одним з найбільш розповсюджених класів алгоритмів шифрування є синхронні потокові шифри.

В роботі [2] автори доповіді розглянули сучасні методи криптографічного аналізу, що дозволило виділити криптографічні властивості булевих функцій, які впливають на ефективність реалізації криптографічних атак. Детальному аналізу властивостей булевих функцій, які визначають стійкість сучасних шифрів присвячені роботи [3, 4].

Проведений аналіз дозволив виділити найбільш ефективні атаки на синхронні потокові та продемонстрував, що оцінка стійкості шифрів відносно вказаних атак потребує ефективних алгоритмів перевірки $k$-вимірності булевих функцій. В роботі [5] запропонований найбільш ефективний імовірнісний тест $k$-вимірності. При цьому верхня межа ймовірності помилки першого роду запропонованого тесту не залежить від $k$. Цей тест дозволить за практичний час обрахувати $k$-вимірність та визначати стійкість криптосистем відносно статистичних атак.

Потреба в ефективних методах оцінки стійкості сучасних шифрів ставить перед дослідниками прикладне завдання пошуку ймовірнісних методів аналізу криптографічних властивостей булевих функцій та визначає актуальність мети дослідження представленого в доповіді, що полягає в аналізі ефективності ймовірнісного тесту $k$-вимірності булевої функції.

В доповіді викладені результати дослідження ефективності вказаного методу, що проведені на прикладі синхронного потокового шифру Decim$^{v2}$, який включений до міжнародного стандарту [6]. В структурі Decim$^{v2}$ можливо виділити нелінійну функцію $f$ від 192 змінних для генерації двійкової послідовності. З огляду на велику кількість змінних виділеної функції, дослідження її криптографічних властивостей детермінованими алгоритмами має обчислювальну складність, яка вимагає тривалого часу виконання, що є неприйнятним з практичної точки зору.

Обчислювальні експерименти проведені на мови програмування C++ на ПЕОМ типу Intel(R) Core(TM) i7-3770K 3,5 GHz, 8 Gb RAM, GeForce GTX 670 (2Gb) в середовищі операційної системи Windows 10.

Представлені в доповіді результати обчислювальних експериментів продемонстрували, що тест вірно встановив значення $k$, при цьому, ймовірності помилок 1 та 2 роду відповідали вихідним параметрам тесту. Програмна реалізація продемонструвала середній час роботи 274 секунди, що дозволяє використовувати її для задач оцінки стійкості сучасних шифрів та зробити висновок про можливість застосування ймовірнісного тесту $k$-вимірності булевої функції в якості інструменту оцінки стійкості сучасних шифрів за практичний час.

**Література**

1. Закон України Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки. (Відомості Верховної Ради (ВВР), 2007, № 12, ст. 102) [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/537-16.

2. Мостюк Д.Л. Аналіз сучасних методів криптоаналізу / Д.Л. Мостюк, С.М. Конюшок // Матеріали науково-практичної конференції курсантів (студентів), аспірантів, докторантів та молодих учених «Актуальні питання застосування спеціальних інформаційно-телекомунікаційних систем», м. Київ, 21-22 травня 2019 р. – К.: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2019, С. 68.

3. Мостюк Д.Л. Аналіз властивостей булевих функцій, які визначають стійкість криптосистем / Д.Л. Мостюк, С.М. Конюшок // Збірник тез наукових доповідей X Всеукраїнської науково-практичної конференції «Актуальні проблеми управління інформаційною безпекою держави», м. Київ, 4 квітня 2019 р. – К.: Нац. акад. СБУ, 2019, С. 250 – 251.

4. Мостюк Д.Л. Питання оцінки стійкості криптосистем: вплив властивостей булевих функцій на ефективність методів криптоаналізу / Д.Л. Мостюк,

С.М. Конюшок // Матеріали науково-практичної конференції «Інформаційно-телекомунікаційні системи і технології та кібербезпека: нові виклики, нові завдання», м. Київ, 19-20 листопада 2019 р. – К.: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2019, С. 29-30.

5. А.Н. Алексейчук, С.Н. Конюшок Усовершенствованный тест *k*-мерности для булевых функцій, Кибернетика и системный анализ. – 2013. – Т. 49. – № 2. – С. 27 – 35.

6. ISO/IEC 18033-4: 2011(E). Information technology – Security techniques – Encryption algorithm – Part 4: Stream ciphers, 2011. – 92 p.

*УДК 34:004*

**Назаренко А. О.**
Національна академія СБ України

## ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ЗАБЕЗПЕЧЕННЯ ЗБЕРЕЖЕННЯ ПЕРСОНАЛЬНИХ ДАНИХ У КОНТЕКСТІ ПОЛІТИКИ ДІДЖИТАЛІЗАЦІЇ

Останній рік одним з пріоритетних напрямів роботи українського уряду є запровадження так званої «Держави в смартфоні» – низки організаційно-правових заходів, спрямованих на переведення певних адміністративних процедур у електронний формат. Діджиталізація зачіпає не тільки організаційно-правові аспекти роботи публічних органів, а є процесом, наскрізним для всіх сфер суспільства – економічної, соціальної, політичної. Іншими словами, впровадження електронного урядування здійнюється чи має здійснюватись на чотирьох рівнях: розміщення інформації про державу, комунікації та транзакції з державою та залучення до управління державою.

Як така, політика діджиталізації не є новою для України: концепція електронного врядування як один з напрямів розвитку держави була запроваджена ще у 2010 році, коли Кабінет Міністрів схвалив відповідну концепцію. За 2016–2018 роки Міністерство економічного розвитку разом із Державним агентством з питань електронного урядування перевели в онлайн понад 120 послуг для громадян та бізнесу. Лише за 2019 рік більше 1,5 млрд українців скористались електронним підписом [1]. Процес переведення адміністративних послуг та інши публічних процедур у електронний формат триває досі і навряд чи завершиться у найближчому майбутньому.

Варто зауважити, що діджиталізація як така – це інструмент, а не як самоціль. При системному державному підході цифрові технології мають

стимулювати розвиток відкритого інформаційного суспільства як одного з істотних факторів економічного зростання, створення робочих місць, а також покращення якості життя громадян України [2].

Більш прикладне значення електронного урядування полягає у зменшенні корупційних ризиків. При зменшенні впливу «людського фактору» на прийняття адміністративного рішення щодо запиту особи в рази зменшується вірогідність прийняття неправомірного та несправедливого для неї рішення. Відповідно, це впливає і на корупційний фактор – якщо рішення приймаються автоматизовано, то і можливість маніпуляцій та корупційної вигоди знижуються до мінімуму [3, с. 23].

Водночас варто зауважити, що попри «електронний оптимізм» політика діджиталізації має і певні ризики, на які, на жаль, не так часто звертають увагу як можновладці, так і самі ІТ-спеціалісти. Мова йде про інформаційну безпеку держави та захищеність електронних даних у державному ресурсі. Особливої уваги в цьому аспекті заслуговує проблема захищеності персональних даних громадян у розрізі діджиталізації.

В Україні ця проблема не має як широкого розголосу, так і правових механізмів подолання. Закон України «Про захист персональних даних» не регулює відносини щодо порушення безпеки персональних даних (data security breach), на відміну від GDPR (Загального регламенту щодо захисту персональних даних), що діє в ЄС, чи інших подібних зарубіжних актів.

Наведемо приклади нещодавних витоків персональних даних в Україні, що відбулись у січні 2020 року. Так, на веб-порталі вакансій у державній службі career.gov.ua виявилось, що шляхом маніпуляції із номерами в URL посиланні можна отримати доступ до персональних даних шукачів (зокрема, копіям паспортів, дипломів про вищу освіту тощо). На веб-сайті КП «Головний інформаційно-обчислювальний центр» було виявлено можливість побачити персональні дані платника комунальних послуг (ПІБ, адресу проживання та інші дані) шляхом маніпуляції із номерами в URL посиланні, що відкривається через QR-код, що розміщений на квитанції про сплату комунальних послуг [4].

Обидва із зазначених пробілів у захищеності персональних даних було усунуто, проте вони є показовими в частині сучасного стану захищеності та реагування на порушення захисту персональних даних з боку держави. По-перше, інциденти було виявлено громадськими активістами, про що вони оголосили самостійно у соціальних мережах, а не самим державними спеціалістами. По-друге, інформаційне висвітлення цих інцидентів як публічне, так і приватне шляхом персональних звернень до тих суб'єктів, дані яких стали доступними до широкого загалу, було фактично відсутнє. По-третє, масштаби витоків персональних даних залишились невизначеними, державні спеціалісти обмежились лише усуненням самих джерел витоків, проте не зробили нічого із наслідками цих витоків.

Так чи інакше, вищезазначене обумовлює необхідність врегулювання відносин щодо забезпечення безпеки персональних даних та наслідків їх витоку, що є особливо актуальним у розрізі все більш масштабної діджиталізації.

**Література**

1. Більше 1,5 млрд разів українці скористалися електронним підписом за 2019 рік // Міністерство та Комітет цифрової трансформації [Електронний ресурс]. – Режим доступу: https://thedigital.gov.ua/news/bilshe-15-mlrd-raziv-ukraintsi-skoristalisya-elektronnim-pidpisom-za-2019-rik?fbclid=IwAR0f4Dh1ohJ25W0BkeMxiSz0Uti1L-EunhbqKRVfO5QoTPmu_J6hNBO8d6g.

2. Першочергові сфери, ініціативи, проекти "цифровізації" України до 2020 року [Електронний ресурс]. – Режим доступу: https://ucci.org.ua/uploads/files/58e78ee3c3922.pdf.

3. Електронне урядування та електронна демократія: навч. посіб. у 15 ч. / за заг. ред. А. І. Семенченка, В. М. Дрешпака. – К., 2017. Частина 5 / [Ю. Б. Пігарєв, І. С. Куспляк, В. М. Дрешпак]. – К.: ФОП Москаленко О. М., 2017. – 58 с.

4. Офіційні повідомлення Офісу Омбудсмана в Україні [Електронний ресурс]. – Режим доступу: https://www.facebook.com/office.ombudsman.ua/photos/a.280613289217519/5342098005245 32/?type=3&__tn__=-R.

*УДК 323: 3*

**Наконечний Д. В.**
кандидат історичних наук,
**Чорногор Я. О.**
Військовий інститут Київського національного університету імені Тараса Шевченка

## ДОЦІЛЬНІСТЬ БЛОКУВАННЯ УРЯДОМ УКРАЇНИ РОСІЙСЬКИЙ РЕСУРСІВ У 2017 РОЦІ ДЛЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ ДЕРЖАВИ

Процеси, що відбуваються в інформаційному полі між Україною та РФ висувають багато питань і змушують дослідників переосмислити значну кількість проблем. Однією з актуальних для України є проблема гарантування інформаційної безпеки суспільства в сучасних умовах.

Актуальністю дослідження є те, що 15 травня 2017 р. було введене в дію рішення РНБО України «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)». Особливостями

якого було блокування інтернет-провайдерами доступу до веб-ресурсів інтернет-компаній «ВКонтакті», «Одноклассники», «Mail.ru», «Яндекс», «Лабораторія Касперського», «Dr.Web» тощо. Відповідно до прийнятого «пакету Ярової», сервіси мали зберігати аудіо- та відеофайли, повідомлення та іншу приватну інформацію, яка поповнювала бази даних, до якої мали прямий доступ російські спецслужби.

Об'єктом дослідження є блокування інформаційних ресурсів держави-агресора у гібридній війні між Україною та Росією.

Мета дослідження: довести доцільність проведення санкцій та рішення про блокування російських сервісів на прикладі деяких російських програм.

Кібератаки мають певну ціль для враження. Коли проводилось розслідування атак на український фінансовий сектор, які відбулися у грудні 2016 р., то виявилося, що на значній більшості вражених машин було встановлено російське програмне забезпечення. Відповідно, було висловлене припущення, що російське програмне забезпечення, перш за все, надає потенційну можливість несанкціонованого доступу до інформації.

За словами представників СБУ пакет програм «1С» становить небезпеку. «1С» присутня на українському ринку вже тривалий час та завоювала статус монополіста. Однак, вся інформація, яку отримує «1С», оновлення програми йде через російські сервери. Збираються дані, типу як big data, яка може бути використана в інтересах підриву економіки, збору даних, підриву окремих галузей окремих секторів економіки нашої держави.

Згідно з аналізом InformNapalm, кремлівське керівництво використовує пошуковий сервіс «Яндексу» як інструмент ведення інформаційної війни. Зокрема, видача новин у ньому зазнає жорсткої цензури.

У квітні 2016 р. стало відомо, що «Укравтодор» підписав меморандум із «Яндекс. Карты». «Укравтодор» інформуватиме про стан проїзду українськими автошляхами за допомогою сервісів Яндекс.Карти і Навігатор. Користуючись цими додатками, кожен водій матиме змогу дізнатися про усі ремонтні роботи та несанкціоновані перекриття на автошляхах загального користування. Тобто ми самі надавали дані щодо доріг та їх характеристики противнику, які він міг використовувати при плануванні можливого нападу на Україну.

Отже, противник використовує російські ресурси не лише для пропаганди і контрпропаганди, вербування агентури та відпрацювання планів її мобілізації, але для проведення кібератак. Введення санкцій на російські ресурси було необхідним та доцільним рішенням у протидії загрозам гібридної війни із РФ.

*УДК 323. 3*
**Нечипорук С. В.**
Національна академія СБ України

# ПРОБЛЕМНІ ПИТАННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

Шлях, яким рухається Україна у розбудові власної кібербезпеки, потребує докорінних та невідкладних змін, необхідність яких підтверджена атаками на об'єкти критичної інфраструктури, сумнозвісними вірусними атаками Petya та WannaCry та багатьма іншими інцидентами, які протягом останніх років створили Україні репутацію одного з головних кіберполігонів.

Розглянемо основні чинники проблем кібербезпеки України.

*Неефективна нормативна база та система управління.*

Аналіз першопричин призводить до цілої низки системних проблем у галузі, ігнорувати які з кожним наступним інцидентом стає дедалі важче. Одна з головних – неефективна нормативна база та система управління.

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» та серія нормативних документів про технічний захист інформації (НД ТЗІ) безнадійно застарілі. Більше того, вони зобов'язують органи державної влади, об'єкти критичної інфраструктури та приватні компанії, які хочуть надавати послуги державним органам (наприклад, Інтернет-провайдери), впроваджувати так звану Комплексну систему захисту інформації (КСЗІ). Вона впродовж багатьох років довела свою неефективність.

*Низька готовність реагувати на кібератаки.*

Більшість компаній ще не готові організаційно до нових хвиль кібератак та не мають підготовлених в достатній мірі фахівців у своєму штаті.

Відсутнє й централізоване управління силами реагування на кіберінциденти на загальнодержавному рівні.

Також потребує іншого підходу питання обізнаності громадян в основних засадах кібербезпеки. Державна програма для заповнення цієї прогалини в Україні наразі, на жаль, відсутня. Низький рівень залучення професійної спільноти, відсутність трансформаційного підходу. Загалом управління кібербезпекою в Україні на державному рівні важко назвати ефективним.

Відсутній трансформаційний підхід до управління національною кібербезпекою, що передбачає наявність організації, яка керує впровадженням програми з кібербезпеки, та регулярного контролю за процесом впровадження.

До того ж, через специфіку багатьох галузей (охорона здоров'я, енергетика, телекомунікації тощо) існує гостра потреба в окремих галузевих стандартах з кіберзахисту.

*Кіберрозвідка потребує покращення*

Ще одна суттєва проблема – в Україні все ще недостатньо ефективно працює система кіберрозвідки (ThreatIntelligence). Є приклади, коли приватні організації та волонтерські угрупування попереджають державу про атаки, які плануються. Але ж в умовах існуючих загроз цього видається недостатньо.

*Низька якість аудиту кібербезеки*

Окрема проблемна ділянка – аудити кібербезпеки. В системі координат НД ТЗІ, дозвіл на проведення аудиту мають лише акредитовані державою організації. Міжнародні сертифікати з інформаційної безпеки та ІТ-аудиту наразі не визнаються, що негативно впливає на якість аудиту.

*Бізнес має визначати галузеві вимоги щодо кібербезпеки*

Питання регулювання та контролю можна делегувати галузевим регуляторам або саморегулюючим організаціям. Одним із прикладів останніх є NERC CIP в США, що розробила галузеві стандарти з кібербезпеки для енергетичного сектора. Прикладами інших галузевих регуляцій, які було б доцільно розглянути на предмет можливості їх впровадження в України, є HIPAA із забезпечення захисту електронних медичних даних в сфері охорони здоров'я, Ofcom для телекомунікацій тощо.

*Визначення чітких критеріїв об'єктів критичної інфраструктури.*

Критерії віднесення об'єктів до критичної інфраструктури мають бути чітко визначені. Критерії повинні розроблятися експертами та бути такими, що можна виміряти. Сучасний ландшафт кіберзлочинів стає дедалі складнішим. Всупереч поширеній думці, безпека – це не стан, а процес. Крім того, в умовах сьогодення недостатньо покладатися виключно на захист. Для того, щоб мінімізувати збитки від кібератак, важливо фокусуватися не лише на захисті, але й на побудові правильних процесів реагування на інциденти. Значну роль у налагодженні цих процесів відіграє навчання реагуванню керівників компаній, пересічних громадян тощо.

Потрібно створити національний портал кібербезпеки із електронними курсами та запровадити кампанію із підвищення обізнаності населення в ЗМІ.

Не менш важливим є формування культури кібербезпеки у суспільстві. З правилами кібергігієни дітей потрібно знайомити ще за шкільною партою, як, наприклад, зараз це відбувається з правилами безпечної поведінки на дорозі.

Визнання міжнародних сертифікацій та запровадження обов'язкової міжнародної сертифікації для посадовців, які займаються кібербезпекою та аудитом.

*Профільна освіта з кібербезпеки в Україні потребує вдосконалення.*

Нестачу профільних знань фахівці компенсують зазвичай міжнародними професійними сертифікатами (наприклад CISSP, CISM, OSCP, GSEC

та інші), які дають хороший базовий рівень. У той же час на державному рівні такі сертифікати визнання не отримали. Ситуацію варто було б змінити. На додачу, державну акредитацію аудиторів з кібербезпеки, яка наразі створюється, потрібно замінити акредитацією на основі міжнародних сертифікацій.

*Співпраця з дослідниками та створення галузевих центрів реагування на кібератаки.*

Необхідне налагодження обміну інформацією про кіберінциденти та тісна співпраця держави з приватними компаніями й дослідниками, які мають працювати не на волонтерських засадах, як це відбувається зараз, а в межах встановлених правил.

Створення галузевих центрів реагування на кіберінциденти (SOC) та центрів обміну інформацією про кібератаки (ISAC) допоможе з вирішенням цієї проблеми. Причому локальні SOC-и та ISAC-и мають налагодити тісну взаємодію з міжнародною мережею подібних організацій. Залучення професійної спільноти до цього процесу є обов'язковим кроком.

*Аудити кібербезпеки за міжнародними стандартами.*

Для оцінки захищеності інформаційних систем пропонується впровадити аудити на відповідність міжнародним стандартам. Аудити потрібно проводити регулярно, із залученням незалежних (бажано, зовнішніх) спеціалістів, які мають міжнародну сертифікацію.

*Створення національної експертної ради з кібербезпеки.*

Важливим кроком має стати створення експертної ради з питань кібербезпеки за участю представників бізнесу, професійних спільнот та державних органів. Така рада має готувати пропозиції щодо нормативно-правових актів у цій сфері, давати рекомендації по функціонуванню національної системи кібербезпеки та вирішувати інші завдання та проблеми, які потребують належної експертизи. Прикладом такої організації є Національна Рада Кібербезпеки в Нідерладнах. Впровадження кібербезпеки вимагає трансформаційного підходу. Усі ініціативи з кібербезпеки мають бути сформовані в єдину програму трансформації кібербезпеки.

Необхідне внесення змін в законодавство, включаючи закони України «Про захист інформації», «Про основні засади кібербезпеки» тощо.

Функції регулярного контролю за виконанням програми повинні належати офісу з кібербезпеки, який може існувати на базі неурядової організації, уповноваженої впроваджувати реформи у сфері кібербезпеки.

*УДК 343.98*
**Омельян О. С.**
Національна академія СБ України

# АКТУАЛЬНІ ПИТАННЯ ВПРОВАДЖЕННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ У ДІЯЛЬНІСТЬ СУДОВОГО ЕКСПЕРТА

З розвитком науково-технічного прогресу активно використовуються зі злочинною метою й сучасні ІТ-технології: полегшується доступ до матеріальних цінностей, змінюються способи підготовки, вчинення і приховування злочинів (зокрема, незаконний обіг наркотичних засобів, психотропних речовин та їх аналогів шляхом використання інтернет-магазинів та електронних платіжних систем), здійснюються кібератаки на банківські установи та комерційні підприємства, вчиняються «безконтактні» злочини шляхом віддаленого доступу. У подібних ситуаціях значно скорочується число традиційних трасологічних слідів, в той же час виникає значна кількість цифрових слідів злочинних діянь.

Для оперативного встановлення всіх обставин злочину і причетних до них осіб правоохоронні органи мають значно випереджати кримінальні структури за ефективністю використання новітніх науково-технічних засобів і технологій та пов’язаних із ними можливостей для застосування у розкритті та розслідуванні зазначених правопорушень.

Впровадження і використання сучасних цифрових та інноваційних технологій в галузі судової експертизи є важливим додатковим інструментарієм і розширенням можливостей експертних досліджень різноманітних об’єктів з метою отримання доказової інформації в інтересах розслідування [1, с. 11].

Однією з актуальних проблем, що виникає протягом розслідування сучасних злочинів, є виявлення, фіксація, вилучення та збереження значної кількості цифрових слідів, які утворюються під час вчинення правопорушення.

Цифровими слідами в криміналістиці, на думку Г. К. Авдєєвої, «є матеріальні невидимі сліди, які містять криміналістично-значущу інформацію (відомості, дані), зафіксовану в цифровій формі на матеріальних носіях і можуть бути виявлені, зафіксовані й досліджені за допомогою певних цифрових пристроїв» [2, с. 91].

Характеризуючи цифрові сліди, як явище для вивчення в криміналістиці та експертології, слід зазначити наступне. По-перше, це інформація, що зафіксована у цифровому вигляді, тобто у форматі, зрозумілому для електронно-обчислювальних машин. По-друге, ця інформація міститься в різного роду цифрових пристроях зі створення, обробки, збереження та передачі цієї інформації (комп’ютерах, носіях інформації, комунікаційних

системах тощо). По-третє, цифровий слід відображає злочинну діяльність, так як причинно пов'язаний з подією злочину і дозволяє встановити як обставини вчиненого правопорушення, так і особу злочинця.

Цифрові сліди можуть міститися у різного роду об'єктах експертних досліджень, як то лог-файли, дампи оперативної пам'яті, дампи мережевих трафіків, інші файли або їх частини (у разі пошкодження), як наявні, так і видалені, а також службовій інформації про ці файли тощо. Вказані об'єкти зазвичай розташовуються на матеріальних носіях інформації у вигляді цифрових кодованих послідовностей або спеціально записуються (копіюються) на матеріальні носії інформації для подальшого використання у процесі доказування. Доступна сприйняттю людиною така інформація тільки за допомогою використання спеціалізованих програмних і апаратних засобів, що здійснюють декодування і візуалізацію в звичній графічній, текстовій або звуковій формі [3, с. 116].

Спеціалізованими високотехнологічними засобами для виявлення та аналізу цифрових слідів судовими експертами на сьогодні є:

– експертне програмне забезпечення для криміналістичного дослідження комп'ютерних носіїв інформації, наприклад «Forensic Toolkit», «EnCase Forensic», «X-Ways Forensics», «Belkasoft Evidence Center», «Magnet AXIOM»;

– мобільні комплекси, що дозволяють добувати, декодувати та аналізувати цифрову інформацію, отриману з мобільних пристроїв, зокрема «Cellebrite UFED Touch 2», «MSAB XRY Field», «MOBILedit Forensic Express Pro»;

– програмне забезпечення з відновлення комп'ютерних даних «R-Studio», «UFS Explorer» тощо.

Слід зазначити, що якісна робота із вказаними програмними та апаратно-програмними засобами потребує високої кваліфікації судового експерта (спеціаліста). Крім теоретичних знань у сфері цифрових технологій необхідні й практичні навички роботи з комп'ютерним і телекомунікаційним обладнанням, а також спеціалізованим програмним забезпеченням.

Підсумовуючи вищенаведене, вважаємо, що оскільки використання сучасних цифрових технологій суттєво підвищує ефективність проведення експертних досліджень, а також відкриває широкі можливості та перспективи у попередженні, розкритті і розслідуванні злочинів, існує необхідність їх якнайшвидшого впровадження у практику проведення судових експертиз. Саме тому, на наш погляд, необхідно вже зараз розробляти та реалізовувати державну програму цифровізації судово-експертної діяльності, в якій передбачити механізми заохочення розробок таких технологій українськими науковцями, а також підготовку висококваліфікованих спеціалістів у цій сфері вітчизняними закладами освіти та науки.

**Література**

1. *Александренко О.В., Женунтій В.І.* Інновації та цифрові технології в криміналістиці та судовій експертизі: сучасні можливості та проблеми застосування // Інноваційні методи та цифрові технології в криміналістиці, судовій експертизі та юридичній практиці : матеріали міжнар. «круглого столу» (Харків, 12 груд. 2019 р.) / редкол.: В. Ю. Шепітько (голов. ред.), – Харків : Право, 2019. – С. 10-14.

2. *Авдєєва Г.К.* Сутність цифрових слідів в криміналістиці / Г. К. Авдєєва // Актуальні питання судової експертизи та криміналістики : зб. матеріалів міжнар. наук.-практ. конфер., присвяч. 95-річчю створення Харків. НДІ суд. експертиз ім. засл. проф. М. С. Бокаріуса (Харків, 10–11 жовт. 2018 р.). – Харків, 2018. – С. 90-93. URL: http://dspace.nlu.edu.ua/bitstream/123456789/15677/1/Avdeeva_90-93.pdf.

3. *Семикаленова А.И.* Цифровые следы: назначение и производство экспертиз // Вестник Университета имени О.Е. Кутафина (МГЮА). 2019. № 5(57). С. 115-120.

*УДК 354.42/.44*

**Онищенко Я. В.**
Національна академія СБ України

## МАНІПУЛЯТИВНІ ТЕХНОЛОГІЇ СУЧАСНИХ СОЦІАЛЬНИХ МЕРЕЖ

Маніпулювання є різновидом психологічного впливу, професійна реалізація якого призводить до виникнення в іншої особи намірів та бажань, які не збігаються з її дійсними, але яких бажає маніпулятор. Під час маніпулювання особа, яка впливає, постійно прагне до того, щоб людина, яка є об’єктом маніпуляції, визнала сама навіювану їй ідею єдиною вірною для себе. Для досягнення цієї мети маніпулятор удається до методик переконання, а іноді й примушення. Це переконання засновується саме на умисному введенні в оману або ж на навіюванні. Суб’єкту маніпулювання необхідно створити у свідомості об’єктів впливу подвійну ілюзійну картинку: по-перше, що реальність є саме такою, якою її навіюють, і, по-друге, що відповідь на цю реальність залежить від самої особи, яка є об’єктом маніпуляції [1].

З розвитком мережевих технологій і появою нових засобів комунікацій в 80-90-х рр. вживання терміну «соціальні мережі» поступово змістилося з соціології у сферу інформаційних технологій. З роками соціальні мережі набули поширення по всьому світу, приваблюючи все більшу кількість користувачів мережі Інтернет. Початок 2000-х рр. слід вважати епохою розквіту соціальних мереж. У 2003-2004 рр. з’явилися такі мережі як

LinkedIn, MySpace та Facebook. У 2006 р. запрацював Twitter, а також найпопулярніша на території східної Європи соціальна мережа "ВКонтакте".

Серед основних завдань соціальних мереж варто відзначити такі:

1) комунікативна (встановлення контактів з іншими користувачами, обмін новинами, інформацією);

2) інформативна (інформація може як надходити до користувача, так і йти від нього до інших);

3) соціальна (об'єднання «друзів» в різні групи за інтересами);

4) ідентифікаційна (при реєстрації особа вносить свої особисті дані, завдяки чому іншим користувачам не завдає великих клопотів знайти цю особу);

5) самовираження (поведінка користувачі в мережі є більш впевненою та вільною, тобто їх майже не стримують ті чинники, які присутні в реальному житті).

Для впливу на користувачів мережі використовуються спеціальні маніпулятивні техніки. У соцмережах як у найбільш довірчих колах спілкування дуже небезпечними є сугестивні технології. Сугестивні технології впливають на психіку особи шляхом зниження критичності мислення при отриманні навіюваної інформації. Засоби сугестії діляться на мовленнєві та текстові. Мовленнєві бувають вербальними (фрази, слова, наголоси), паралінгвістичними (висота, тон, тембр) та невербальними (міміка, жести).

Ще одним сучасним маніпулятивним методом у соціальних мережах є мікротаргетинг. Мікротаргетинг полягає в тому, що він надає змогу підбирати користувачів за віком, місцем проживання, хобі та комунікувати з певною групою осіб або окремим індивідом, привертати їхню увагу та бути для них цікавим як особа з подібними інтересами.

Також в Інтернеті широко проявляється стандартний, залучений ще з німецької пропаганди Другої світової війни, спосіб «багаторазового повторювання». Завдяки цьому способу при багаторазовому повторювані однієї і тієї ж думки серед індивідів певної групи, ці особи з часом починають сприймати цю тезу за істину.

Оскільки для сучасних технічних засобів не існує ніяких перешкод зробити вид масової підтримки, необхідної маніпуляторам думки, то відповідно до принципу «соціального доказу», люди, для того щоб визначити, чому довіряти і як саме необхідно діяти в тій чи іншій ситуації, орієнтуються на те, чому саме довіряють і як діють у подібній ситуації інші особи. Цей принцип заснований на теорії «безпеки великих чисел» – тобто значна кількість осіб не може помилятися в одному і тому ж питанні. Наприклад, «…зубна паста Colgate одна з найкращих у світі – мільйони людей по всьому світу не можуть помилитись!» [2].

Також в соціальних мережах активно використовують і метод мотивації загроз. Згідно з експертними дослідженнями, люди погоджуються з тією чи іншою думкою, навіяною манерою ставлення тощо, найімовірні-

ше, якщо є загроза втратити чого-небудь. Це надає змогу маніпулятору навіювати людині (групі) потрібну маніпулятору думку (дію). Цей принцип ретельно досліджував психолог Р. Чалдіні та описував під назвою – «принцип дефіциту» [3].

Соціальні інтернет-мережі мають змогу сконцентровувати інформацію, щоб формувати точки зору, погляди, певні настрої, посилювати чи послаблювати становище певних кіл осіб, знаходити, групувати. Варто відзначити те, що інформація в соціальних мережах викладається в чітко визначений період, що надає змогу концентрувати на ній увагу користувачів, нав'язуючи її з системною частотою, не залишаючи великих проміжків часу між повідомленнями без інформації, тобто маніпулятор тримає користувача «постійно в темі».

**Висновки.** Соціальні мережі стали невідривною складовою комунікації людей в наш час, проте завдяки існуванню сучасних деструктивних інформаційних технологій вони стали також засобом маніпулятивного впливу для певних осіб, які прагнуть здійснити цей вплив.

Саме тому варто зазначити, що основною психологічною та фізичною небезпекою під час деструктивних впливів маніпулятивних технологій є те, що з'являються можливості змінювати риси характеру людини, її нормальну поведінку, знижувати інтелект та критичне сприйняття дійсності, змінювати творчі можливості та призводити навіть до підміни самої особистості. Наслідком такого впливу може стати поява певних емоційних груп осіб, керованих на психологічному рівні та готових виконати будь-яку команду свого маніпулятора.

Для точного та повного розуміння тієї чи іншої ситуації людина повинна ґрунтовно аналізувати отриману нею інформацію та мати власне критичне мислення, яке так бажають «приспати» маніпулятори в мережі та навіяти «свою правду». З цією метою в сучасному глобалізованому інформаційному просторі кожна людина має бути обізнаною з питань інформаційної безпеки. Адже, якщо людина обізнана, то вважається «озброєною» та такою, що може протистояти деструктивному маніпулятивному впливу в інформаційному просторі на її свідомість.

**Література**

1. Інформаційна безпека держави: підручник / [В.М.Петрик, М.М. Присяжнюк, Д.С.Мельник та ін.]; в 2 т. / за заг. ред. В.В.Остроухова. – К.: ДНУ «Книжкова палата України», 2016. – Т. 1. – 264 с. Т. 2. – 328 с.

2. Деркаченко Я. А. Соціальні мережі, як середовище для технологій маніпулятивного впливу / Я. А. Деркаченко // Сучасний захист інформації. – 2016. – № 1. – С. 51-59 [Електронний ресурс] – Режим доступу: http://nbuv.gov.ua/UJRN/ szi_2016_1_8.

3. Чалдини Р. Б, Психология влияния. [Електронний ресурс] – Режим доступу: http://bookz.ru/ authors/4aldini-robert/chaldinir01/1-chaldinir01.html.

*УДК 342.727(045)*
**Орел Г. П.**
НДІ інформатики і права НАПрН України

# СТАН НАУКОВОЇ РОЗРОБКИ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНИХ ПРАВ ЛЮДИНИ В СОЦІАЛЬНИХ МЕДІА

Первинно, інформаційна безпека розглядалась, насамперед, як інформаційна безпека держави. Згодом інтенсифікація процесів інформатизації в усіх сферах, а особливо, зростання значення технічного захисту інформації зумовило становлення правового забезпечення захисту інформації, як невід'ємної складової безпеки підприємств, установ та організацій, а також окремих галузей господарства.

Соціальні медіа вже давно стали дієвим механізмом як для впливу на суспільну думку, так і для сприяння розвитку компаній. Соціальна мережа – соціальна структура, утворена індивідами або організаціями. Вона відображає зв'язки між ними через різноманітні соціальні взаємовідносини, починаючи з випадкових знайомств і закінчуючи тісними родинними вузами.

Затребуваним є дослідження впливу соціальних мереж на соціокультурні зміни, структуру та ідентичність особистості, соціально-економічні та соціально-політичні процеси. Комунікативні ресурси Н. Коритнікова вивчала Інтернет-представництва; А. Алдишкіна, І. Остапенко присвятили свої роботи соціальній структурі, віртуальній ідентичності, гендерній саморепрезентації в Інтернеті. Є. Прохоренко досліджувала феномен кіберкультури в інформаційно-технологічному відтворенні соціуму. Увагу соціологів привертає проблематика кількісного та якісного складу аудиторії Інтернет. Цим питанням присвячені роботи Є. Головахи, Б. Головка, А. Горбачика, Н. Костенко, О. Личковської, Т. Рудницької, В. Щербини та ін. О. Сирота досліджувала психологічні особливості постійних відвідувачів соціальної мережі "В контакті". Соціальні мережі є маловивченим феноменом у соціології; незважаючи на актуальність теми, на сьогодні майже відсутні емпіричні дослідження і теоретичні роботи, які повною мірою розкривають зміст означеної нами проблеми.

О. Ю. Сирота виділяє такі особливості спілкування у соціальних мережах: 1) анонімність; 2) своєрідність протікання процесів міжособистісного сприйняття в умовах відсутності невербальної інформації; 3) добровільність і бажаність контактів. Користувач добровільно налагоджує контакти або йде від них, а також може перервати їх у будь-який момент; 4) обмеженість емоційної компоненти спілкування і в той же час стійке прагнення до емоційного наповнення тексту, що виражається у створенні спеціальних значків для позначення емоцій; 5) прагнення до нетипової, ненормативної поведінки [3].

Безперечно, наукову основу дослідження становлять напрацювання з інформаційного права. Окрім того, значну роль щодо забезпечення власної інформаційної безпеки автор відводить безпосередньо людині, за умови розбудови демократичної правової держави та розвинутого громадянського суспільства. Тому інформаційна безпека людини не може досліджуватись відірвано від системи інформаційної безпеки суспільства, держави і глобальної інформаційної безпеки людства.

Основою інформаційних прав людини Марущак А.І., визначає право на інформацію, яке включає право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір. При цьому основою права на інформацію вважає право людини на доступ (отримання) до інформації, свободу вираження поглядів і переконань, свободу обміну інформацією [1].

Слід зазначити, що право на інформацію не є абсолютним і необмеженим. Реалізація права на інформацію громадянами, юридичними особами і державою не повинна порушувати громадські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи і законні інтереси інших громадян, права та інтереси юридичних осіб.

В останні роки дослідження питань пов’язаних з інформаційною безпекою, в тому числі правового її забезпечення, особливо актуалізувалось, що має як позитивні, так і негативні наслідки для вітчизняної науки і українського суспільства.

Для забезпечення захисту, потрібно створення ефективної системи забезпечення інформаційної безпеки є однією з базових потреб сучасної держави, яке вимагає розробки відповідної державної політики, її закріплення і реалізації на всіх рівнях. При цьому політика інформаційної безпеки не може існувати у правовому вакуумі – вона виступає невід’ємною складовою інформаційної політики держави та політики національної безпеки, окрім того має базуватись на міжнародних стандартах інформаційної безпеки і відповідати національним потребам та реальному стану розвитку інформаційного суспільства в державі.

Забезпечення інформаційної безпеки України, безпеки її національних інтересів в інформаційній сфері передбачає пріоритетний розвиток системи нормативно-правового регулювання відносин у цій сфері протидії загрозам цих інтересів та впорядкування відповідного правотворчого процесу [2].

**Література**

1. Марущак А.І. Визначення поняття “інформаційні права людини”. Інформація і право. 2011. № 2(2). С. 21–26.

2. Олійник О.В. Нормативно-правове забезпечення інформаційної безпеки в Україні. Право і суспільство. 2012. № 3. С. 132-137.

3. Про інформацію : Закон України від 02.10.92 р. № 2657-12. ВВР України. 1992. № 48. Ст. 650.

4. Сирота Е. Ю. Личностные особенности постоянных посетителей сайта www.vkontakte.ru. [Текст] / Е. Ю. Сирота// Вестник КемГУ. – 2010. – № 3(43). – С. 115–118.

5. Человек в социальных сетях [Електронний ресурс] / Режим доступу: http://www.timeout.ru/journal/feature/6557/1/.

*УДК 004.5*

**Остапчук Д. О.**
Національна академія СБ України

## ТЕОРЕТИЧНІ АСПЕКТИ СУТНОСТІ ЗАХИСТУ ІНФОРМАЦІЇ В УКРАЇНІ

Роль інформації в усіх сферах життєдіяльності людини складно оцінити, адже цей продукт сприяє формуванню багатьох аспектів соціального розвитку суспільства. Однак цінність інформації потребує новітніх підходів до її захисту, що має відповідати вітчизняним та міжнародним стандартам з інформаційної безпеки.

Під поняттям "захист інформації" розуміють методи і засоби, які забезпечують цілісність, доступність, конфіденційність інформації за умов впливу на неї загроз штучного чи природного характеру, реалізація яких часто може призвести до завдання шкоди власникам та користувачам інформації [1].

Як і решта інших основоположних понять, захист інформації має суб'єктів та об'єкт правовідносин. До суб'єктів ми відносимо – володільців, користувачів, спеціально визначений законодавством орган виконавчої влади України. До об'єктів захисту інформації відносять інформаційні ресурси, різного роду інформаційно-телекомунікаційні системи, що призначені для обробки цієї інформації, тощо.

Основним напрямком в системі захисту інформації є її правовий режим, як складова формування інформаційного суспільства.

Правова форма захисту інформації – це захист інформації, що "базується" на використанні статей Конституції України та законів держави, положень ЦКУ, ККУ та інших нормативно-правових документів в галузі інформаційних відносин та її захисту. Вона регламентує права та обов'язки суб'єктів, правовий статус державних органів, аспекти технічного захисту інформації та створення відповідних морально-етичних норм в цій області. Правовий захист інформації визначається як на міжнародному рівні (угоди, конвенції, міжнародні договори), так і на державному рівні, який регламентується законодавством України [2].

Також часто в науковій літературі зустрічається правовий захист інформації на локальному рівні. Наприклад, на підприємствах, установах та орнаізаціях різних форм власності можуть створюватись положення, ін-

струкції, накази щодо заходів до захисту інформації в установі з використанням технічних, адміністративних, криптографічних елементів.

Конкретні завдання із захисту інформації, що розробляються на рівні певної організації чи держави в цілому мають відповідати заздалегідь визначеній стратегії у цій сфері. Як зазначають науковці, стратегія захисту інформації є основою для побудови комплексу заходів щодо інформаційної безпеки. Суть полягає в тому, що необхідний пошук оптимального компромісу між необхідністю використання конкретних засобів захисту і наявними ресурсами, які допоможуть це реалізувати [1].

Отже, захист інформації в Україні є однією з складових забезпечення національної безпеки, оскільки її компоненти визначають першочергові підходи для формування інформаційної безпеки держави. Впродовж останніх років нормативному регулюванню сутності цієї теми приділяється особлива увага під час громадського обговорення та на законодавчому рівні. Про це свідчить перш за все прийняття ряду законодавчих актів в сфері інформаційної безпеки. Для прикладу визначено основні загрози та рівні протидії їм, тому таким чином безпекове середовище інформації в Україні вийшло на інший рівень в порівняні з минулими роками.

**Література**

1. Частина 13: Захист інформації в системах електронного урядування: навч. посіб. / О.М. Хошаба. – К.: ФОП Москаленко О.М., 2017. – 72 с.

2. Правовий захист інформації: навч.посіб. / Н.І. Логінова, Р.Р. Дробожур. – Одеса.: Фенікс, 2015. – 264 с.

*УДК 343.321.2*

**Поліщук О. В.**
**Тугарова О. К.**
кандидат юридичних наук, доцент,
Національна академія СБ України

## GDPR ЯК НОВІ ВИМОГИ ДО ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

В травні 2018 року набули чинності нові вимоги Європейського парламенту щодо захисту персональних даних. Правила закріплені в General Data Protection Regulation. Загальний регламент про захист даних або GDPR – це регламент в межах ЄС щодо захисту персональних даних громадян ЄС. Даний документ за своє природою є регламентом, значить має пряму дію та є обов'язковим для імплементації в національне законодавство усіх держав-членів Європейського Союзу [2].

Регламент стосується захисту та експорту персональних даних всіх осіб всередині ЄС та в межах Європейського економічного співтоварист-

ва. Крім того, він встановлює норми, пов'язані із захистом фізичних осіб щодо обробки персональних даних і норми, що стосуються вільного переміщення персональних даних. Також Регламент захищає основні права і свободи фізичних осіб, і, зокрема, їх право на захист персональних даних [1].

Немає значення на території якої країни світу розміщена компанія, якщо вона здійснює збір чи обробку інформації про осіб, які знаходяться на території Європейського Союзу – вона повинна слідувати нормам GDPR [3].

Головна мета GDPR – гарантія захисту персональних даних громадян ЄС без прив'язки до території держави де вони зберігаються. Акт спрямований на підсилення та уніфікацію захисту персональних даних. Тому основною вимога до компаній, які працюють з такими даними, – надійно захищати їх конфіденційність. GDPR не встановлює прив'язки до конкретних прийомів та методів захисту персональних даних, а залишає це право, і, в той же час, обов'язок за компаніями [2].

В Регламент внесено та розширено перелік прав суб'єктів персональних даних:

1. право на інформацію про обробку;
2. право на доступ до даних;
3. право на виправлення даних;
4. право на видалення даних;
5. право на обмеження обробки;
6. право переносу даних; право на заперечення;
7. права щодо автоматизованого прийняття рішень, включаючи складання профілю;
8. право знати про витоки даних [1].

Для порівняння, в Законі України «Про захист персональних даних» права суб'єкта персональних даних (ПД) це: 1) знати про обробку ПД, 2) право на доступ до ПД, 3) право вносити застереження щодо обробки ПД, право на заперечення обробки ПД та зміну ПД, право відкликати згоду на обробку ПД, право на захист від незаконної обробки, право на захист від автоматизованого рішення, яке має правові наслідки для суб'єкта ПД [6].

За порушення GDPR передбачено два типи штрафів:

1) за незначні порушення – штраф може сягати максимум 10 мільйонів євро, або 2% від річного обороту компанії

2) за значні порушення, які пов'язані з порушенням основних принципів захисту персональних даних – штраф може сягати максимум 20 мільйонів євро, або 4% від річного обороту компанії [3].

В Україні немає чіткого механізму застосування штрафів відповідно до законодавства ЄС. Не є повністю зрозумілим, яким чином можна притягти до відповідальності порушника цього регламенту. Організаційно-правове та методологічне забезпечення в сфері охорони персональних да-

них здійснює Департамент у сфері захисту персональних даних Уповноваженого з прав людини.

Департамент у сфері захисту персональних даних Секретаріату Уповноваженого Верховної Ради України з прав людини є самостійним структурним підрозділом Секретаріату Уповноваженого Верховної Ради України з прав людини діяльність якого координує представник Уповноваженого, визначений Уповноваженим Верховної Ради України з прав людини [5].

GDPR – це нормативний документ, який має суттєво підвищити рівень захисту персональних даних як в ЄС, так і за його межами. Регламент дає більше інструментів впливу на долю своїх персональних даних суб'єкту персональних даних, а крім того поновлює довіру користувача, а це дозволяє бізнесу максимально швидко використати можливості на єдиному європейському ринку товарів і послуг. GDPR об'єднує правила, які раніше регулювали питання захисту і обробки персональних даних в один уніфікований акт [2].

## Література


1. GDPR. офіційний український переклад. блог Романа Радейка. – 2018. URL: http://aphd.ua/gdpr-ofitsiinyi-ukranskyi-pereklad (Дата звернення 8.03.2020).

2. Гвоздій В. А. General Data Protection Regulation. Національна асоціація адвокатів України. – 2018. – URL: https://unba.org.ua/publications/3320-general-data-protection-regulation.html (Дата звернення 8.03.2020).

3. Кравець Р. Ю. GDPR: що варто знати про правила захисту ваших даних? 2019. – URL: https://protocol.ua/ua/gdpr_shcho_varto_pro_znati_pro_pravila_zahistu_vashih_danih_1/. (Дата звернення 8.03.2020).

4. General Data Protection Regulation. – 2019.URL: https://en.wikipedia.org/wiki/General_Data_Protection_Regulation. (Дата звернення 8.03.2020).

5. Захист персональних даних. URL: http://www.ombudsman.gov.ua/ua/page/zpd/info/. (Дата звернення 8.03.2020)

6. Права суб'єкта ПД та шляхи їх реалізації. О. О. Тихомиров, В. В. Породько, О. І. Полонська. Захист персональних даних правове регулювання. – 2016. – URL: http://zpd.inf.ua/page16.html. (Дата звернення 8.03.2020).

*УДК 355/359*
**Решитько В. Г.**
Військовий інститут Київського національного
університету імені Тараса Шевченка

# НОВІ ПІДХОДИ ДО КАДРОВОЇ ПОЛІТИКИ ЗС УКРАЇНИ В ЦИФРОВУ ЕПОХУ

Ефективна система кадрового менеджменту в ЗС України, яка здатна до підтримання та забезпечення необхідної кількості професійного особового складу із певним набором навичок та знань для тієї чи іншої військово-облікової спеціальності – важливий компонент для забезпечення безпеки та оборони України. Сьогодні ведеться активна дискусія щодо зміни підходів до управління людськими ресурсами як серед військово-політичного керівництва країни, так і серед громадянського суспільства.

На думку дослідників, застарілі принципи в кадровій політиці, позбавляють військовослужбовців мотивації та бажання до кар'єрного розвитку. Як наслідок, підготовлені фахівці йдуть із лав Збройних Сил, а їх місця можуть зайняти безініціативний та непрофесійний особовий склад, який матиме за мету заробити гроші або отримати конкретні вигоди від служби. В підрозділах досі спостерігаються випадки неналежного ставлення до військовослужбовців, порушення їх прав та свобод. Подібні ситуації мають розголос в ЗМІ, що відлякує потенційних рекрутів. ЗС України мають бути в змозі вступити у боротьбу із цивільним ринком праці та залучити висококваліфікованих працівників, тобто стати конкурентоздатним роботодавцем. Питання кадрового управління складне та потребує детального вивчення, зупинимося на проблемі стимулювання навчених та підготовлених фахівців продовжувати службу.

Підвищення грошового забезпечення, можливо важливий стимул, але не основний. Існує гостра необхідність створити сприятливі умови, щоб військові, особливо з досвідом участі в ООС-АТО, просувалися по службі, постійно покращуючи свій рівень компетентності, не боялися брати відповідальність та проявляти ініціативу. На підготовку фахівця із певної спеціальності витрачається значний час та кошти, тому його звільнення обходиться дорожче, чим навчання нового.

Військовослужбовці повинні бачити перспективи постійного зростання та ті переваги, які надаються на кожній сходинці. Доцільно створити систему із чітким набором параметрів оцінювання військовослужбовця для подальшого його кар'єрного зростання у званні та спеціальності. Правильно організована система оцінювання (цивільна та військова освіта, виконання вправ зі стрільби, якість здачі фізичних нормативів, наявність бойового досвіду та нагород, проходження додаткових курсів зі спеціаль-

ності тощо) посилить дух конкуренції та професіоналізму. Вона дозволить військовослужбовцю аналізувати власні сильні та слабкі сторони та уникати посередності, постійно стимулюючи його до розвитку. Спеціалісти з кадрового забезпечення, отримають широке поле для дослідження та впровадження нових методів відбору та підготовки фахівців. За допомогою сучасних засобів інформаційно-комунікаційних технологій, система може працювати онлайн, доступ до якої матиме військовослужбовець, його командир та представник кадрової служби.

Подібна система вдало працює в ЗС США, де кожен військовослужбовець на веб-сайті Управління Людськими Ресурсами Міністерства оборони (Human Resources Command – hrc.army.mil), в розділі Self Service може переглянути дані свого Promotion Point Worksheet (Лист з оцінювання компетенцій військовослужбовця) та інформацію щодо наступної комісії для підвищення по службі.

*УДК 004.55*

**Сичьов Д. О.**
Національна академія СБ України

## ВИКОРИСТАННЯ ОПЕРАЦІЙНОЇ БЕЗПЕКИ (OPSEC) ПРИ РОЗСЛІДУВАНІ КІБЕРІНЦИДЕНТІВ

Ця робота зосереджена на питаннях безпеки, що стосуються розслідувань кіберінцидентів. Вона охоплює різні сфери процесу розслідування та те, як інструменти та конкретні методи можуть впливати на розповсюдження чутливої інформації, що шкодить справі або розслідувачу.

Крім того, розглядається те, як розслідувачі можуть бути профільовані та самі стати жертвою розслідування. Це може бути пряма атака на їхній комп'ютер, на інфраструктуру, на їх особу, або на розслідування, що, у свою чергу, може бути настільки тонким, що може скерувати розслідування у неправильному напрямку. Більш конкретно, розмова стосуватиметься різних методів ідентифікації (або так званого «фінегрпринтінгу») через браузер або/та інфраструктуру, підключення браузера, месенджерів, захисту електронної пошти та відстеження.

Разом з тим, вироблення окремих контрзаходів та пом'якшення наслідків, які можуть допомогти розслідувачу підвищити рівень їх безпеки та зменшити цифровий слід. Крім того, у роботі буде представлено контейнеризацію та те, як її можна використовувати для сегментації та впорядкування процесу.

Слід звернути увагу «ефект спостерігача», коли спостерігач може впливати на реальність лише самим фактом спостереження. Відомо, що Інтернеті дії можуть бути і будуть записані. Коли ви під час розслідування

користуєтесь пошуковими системами такими як «Google», запит зберігається та вноситься до спеціального реєстру, і доступ до цього реєстру може отримати будь хто, у тому числі і зловмисник. Крім того шукаючи інформацію про зловмисників на хакерських форумах інформація про це зберігається у логах веб-серверу цього форуму або навіть coockies можуть перейти у їх власність, тож дана інформація може бути використана цими самими зловмисниками.

Разом з тим, на звичайних сайтах можу знаходитись так звані «tracking pixels» що дає можливість зловмисникам не володіючи інфраструктурою отримувати дані з цих сайтів.

Аналізуючи шкідливе програмне забезпечення (далі ШПЗ) або інші підозрілі файли, особисто або з використанням так званих «Sandbox» є вірогідність повідомлення зловмисників про розслідування.

Користуючись ресурсами як «Virustotal» для визначення функціоналу ШПЗ теж залишає слід. Якщо зловмисника має платний обліковий запис на цьому ресурсі, то він може отримати інформацію про те хто, коли і що перевіряв. Отримавши мінімальну інформацію про проведення розслідування дає можливість зловмиснику провести вже своє розслідування, але проти самого розслідувача, розслідування.

DNS-запити також надають певну інформацію про розслідувача. Розслідувач можете навіть не підозрювати про те, що він їх робив. Деякі текстові редактори роблять це за користувачів. Для того щоб відобразити, що гіпертекст є посиланням текстовий редактор від вашого імені (IP-адреси) робить DNS-запит щоб упевнитись у тому що домен вказаний у гіпертексті доступний. Наприклад 04.06.2019 року у популярному текстовому редакторі на базі ОС Linux «vim» було знайдено схожу, але більш серйозну вразливість CVE-2019-12735.

Крім того, сьогодні дуже розвинувся такий метод соціальної інженерії як фішинг. З приходом таких інструментів як «EvilGinx2» та скорочувачі посилань наприклад «Bitly» стало дуже важко розпізнати де справжній сайт, а де підробка в умовах безмежно великого інформаційного потоку, який людина повинна обробляти за день, особливо під час проведення розслідування. Використовуючи «EvilGinx2» можна навіть обійти двофакторну аутентифікацію що призведе до втрати ваших даних.

Крім втрати даних, за допомогою фішингу зловмисник може отримати контроль над браузером за допомогою такого інструменту як «BeEf» («Browser Exploitation Framework»). Отримавши контроль над браузером зловмисник може отримати контроль над комп’ютером, а потім і всією інфраструктурою підрозділу.

Отримавши листа на вашу електронну поштову скриньку від незнайомця, навіть якщо там немає шкідливих вкладень або будь чого іншого не варто на нього відповідайти. В деяких поштових сервісах наприклад «Gmail», відповівши на лист ви автоматично становитесь друзями і може-

те бачити статус вашого «друга» онлайн він чи ні що може надати додаткову інформацію про робочий час, часовий пояс, тощо.

Більшість месенджерів роблять перев'ю посилання для того щоб користувачу було легше приймати інформацію, але для того щоб вона з'явилась на телефоні або у браузері необхідно її обробити та відобразити що тягне за собою певні наслідки, від втрати інформації про IP-адресу версію ОС(User-Agent), до завантаження небажаного контенту від третьої сторони (Дана функція може бути відключена на більшості месенджерах).

Зважаючи на те, що вищевказані ризики можуть нанести певну шкоду як розслідуванню, підрозділу та розслідувачу особисто. Рекомендується під час розслідувань використовувати засоби віртуалізації – таких як «LXC» і «Docker» з встановленим на них браузером з можливістю віддаленого використання та засоби анонімізації – таких як VPN або TOR.

*УДК 34:004*

**Соловюк А. В.**
Національна академія СБ України

## ЦИФРОВА ТРАНСФОРМАЦІЯ БАНКІВСЬКОЇ СИСТЕМИ

Прогрес цифрових технологій вплинув на фінансові послуги у світі, і вони змушені трансформуватися та ставати більш орієнтованими на клієнтів. Вплив технологій на фінансовий сектор найбільше відчувається в роздрібних платежах.

Небанківські фінансові установи покращили покриття транзакційними рахунками і пропонують мікропозики та споживче кредитування. Завдяки конкуренції зменшилась вартість та зросла швидкість грошових переказів. Нові посередники агрегують попит малого бізнесу та фіз. осіб на міжнародні платежі й обмін валют і пропонують хороші тарифи. Банк Англії, Банк Литви та ін. дали можливість небанківським фін. установам відкривати в них рахунки. Міжнародні платіжні системи розвивають сервіси «B2B-платежі» та інвестують в національні платіжні системи. З'являються банки, що працюють тільки через мобільні додатки. А постачальники послуг інтернет-платежів розширили перелік своїх послуг і надають споживче кредитування.

Україні ж потрібна система роздрібних платежів, доступна в додатку для смартфона, і була б недорогою для користувачів, в тому числі і для невеликих торговців.

Роздрібне кредитування теж змінилося під впливом цифрових технологій. Кредитний скоринг здійснюють алгоритми, автоматично отримують дані з сторонніх систем і використовують дані про поведінку. Підвищені

вимоги до дотримання регуляторних норм забезпечують покращення та оптимізацію моніторингу та звітності. Наступним кроком буде персоналізація фін. продуктів. Ця послуга дасть можливість погашати кредити за індивідуальним графіком, а процентні ставки будуть коригуватися на основі більш повного індивідуального профілю ризику.

У роздрібному кредитуванні з'являються нові користувацькі інтерфейси. Наприклад, платформи p2p-кредитування з'єднують інвесторів і позичальників, також співпрацюють з великими постачальниками ліквідності, для яких дані платформи стають новим інструментом надання кредитів. Маркетплейси фінансових послуг надають людям можливість вибору кращих та дешевших послуг. А банки концентрують увагу на розбудові більш тісних зв'язків з клієнтами і мають на меті стати центром особистих фінансів, що створюють різноманітні фінансові продукти.

Новим інструментом монетарної політики можна вважати цифрові валюти центральних банків. Криптовалюти являються новим типом фінансового активу та систем обміну вартістю. Технологія «блокчейн» закріпилася в системах обміну вартістю, що функціонують без центрального вузла.

В Україні розвиток у сфері фінансових технологій незначний. Картові платежі та розробка програмних продуктів для фін. сектору – найрозвиненіші напрямки. Монобанк є найбільшим проривом на ринку завдяки зручним сервісам.

Криптовалюти в нашій країні є, але їх не визначено та не регульовано на рівні законодавства. Звісно ж, повільні темпи розвитку фінансових технологій в Україні можна пояснити чинниками, які являються перешкодою розвитку всіх секторів української економіки: недостатня кількість інвестицій та капіталу; застарілі нормативно-правові акти та зволікання в їх модернізації; опір змінам та інноваціям; низький рівень доходів; недовіра до фінансових установ.

Отже, вже зараз можна стверджувати, що перед українськими банками є багато викликів, пов'язаних з необхідністю інтегруватися в нову цифрову систему, яка стрімко розвивається. Водночас, саме завдяки новим технологіям та можливим законодавчим змінам, можуть з'явитися безліч нових можливостей.

**Література**

1. Інтерв'ю Олега Гороховського – співзасновника Monobank. ain.ua/special/usaid-monobank-ukr/.

2. «Цифрова економіка і трансформація банків» - «Юридична газета» (Yur-Gazeta.com).

*УДК 39.394*
**Сидоренко С. М.**
**Стеценко А. Ю.**
Національна академія СБ України

# МІФИ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ ПРО ПОРУШЕННЯ В УКРАЇНІ ПРАВ РОСІЙСЬКОМОВНОГО НАСЕЛЕННЯ

Однієї із складових інформаційної війни РФ проти України є поширення міфів та фейків. Одним із них є міф про порушення в Україні прав російськомовного населення.

Права людини – права та свободи, які кожна людина має виключно на тій підставі, що вона є людиною, і які, таким чином,є однаковими для усіх людей. Конкретний обсяг прав людини визначається законодавством тієї правової системи, в умовах якої людина перебуває [1].

Пропагандистські російські ЗМІ розповідають про український мовний закон та поширюють міфи про його недолугість. Але кожному міфу є спростування. Наведемо кілька прикладів, які яскраво демонструють неспроможність, а в деяких випадках брехливість подібних тверджень.

Міф № 1. «За російську мову саджатимуть до тюрми». Брехливість міфу спростовує Закон України «Про забезпечення функціонування української мови як державної», який не передбачає жодної кримінальної відповідальності за спілкування у побуті російською мовою.

Міф № 2. «Закон порушує Конституцію України та Хартію регіональних мов». Поширювачам даного міфу,безмовно відомо, що Закон України «Про забезпечення функціонування української мови як державної» не може порушувати Конституцію України, тому що у ній закріплено: державною мовою є українська. Що стосується Європейської хартії регіональних мов, то Закон надає право представникам національних меншин мати групи чи класи у навчальних закладах із викладанням рідної мови.

Міф № 3. «Російською можна розмовляти лише на кухні». І в даному випадку, це явна неправда. У Законі чітко зазначено, що його дія не поширюється на мову приватного спілкування та мову регіональних обрядів. Разом з тим, Закон зобов’язує державних службовців знати українську мову та користуватися нею під час виконання службових обов’язків [2].

Отже, в Україні немає жодних підстав стверджувати про порушення прав російськомовного населення. Тим більше,злочинним є обґрунтовувати військову присутність російських найманців на нашій землі порушенням цих прав [3].

**Література**

1. Поняття прав та свобод людини ЗМІ [Електронний ресурс]. – Режим доступу: https://osvita.ua/vnz/reports/gov_reg/17715/.

2. Порція фейків про мовний закон від російських ЗМІ [Електронний ресурс]. – Режим доступу: https://ms.detector.media/manipulyatsii/post/22820/2019-05-04-za-rosiisku-movu-v-tyurmu-portsiya-feikiv-pro-movnii-zakon-vid-rosiiskikh-zmi/.

3. Утиски прав російськомовних. [Електронний ресурс].–Режим доступу:https://zaxid.net/v_ukrayini_nemaye_utiskiv_prav_rosiyskomovnih__pravozahisniki_n1303908.

*УДК 351.004*

**Тимощук Є. О.**
Національна академія СБ України

## ШЛЯХИ УДОСКОНАЛЕННЯ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ

Швидкий розвиток процесів інформатизації суспільства породив нову глобальну соціотехнологічну проблему інформаційної безпеки людини, суспільства та держави. Суть її полягає в тому, що найважливіші інтереси людини, суспільства, держави та всієї світової цивілізації визначаються станом навколишньої інформаційної сфери [1].

Інформаційна безпека є складним, багаторівневим явищем. Пріоритетами державної політики України в інформаційній сфері є створення інтегрованої системи оцінки інформаційних загроз та оптимізація законодавчих механізмів реалізації зобов'язань України в межах Європейської конвенції [2].

Унікальність ситуації в Україні полягає в наявності нав'язаної їй гібридної війни. Саме в умовах гібридної війни України з Росією важливе значення надається інформаційній боротьбі, де основними дієвими суб'єктами є ЗМІ та інтернет [3]. Інформаційна боротьба, яка здійснюється протягом усієї гібридної війни, спрямована на руйнування духовного світу та менталітету, одвічних українських цінностей проти яких вона ведеться.

Додаткові можливості для російського інформаційного впливу дало олігархізоване медіасередовище та непрозорість медіавласності в Україні, що дозволило проросійському бізнесу просувати пропагандистський дискурс в Україні на шкоду національним інтересам.

Благодатним ґрунтом для антиукраїнської інформаційної пропаганди є низький рівень медіаграмотності наших громадян. Зачасту серед українського суспільства були й залишаються поширеними погляди, базовані на сприйнятті світу через призму негативних міфів та стереотипів та не поєднувані з демократичним розвитком, єдністю суспільства, повноцінним демократичним діалогом [4].

Означені соціально-психологічні процеси зумовлені в першу чергу інформаційно-психологічним впливом із боку Росії. Цей вплив був забез-

печений високим відсотком російського продукту (кіно, телепрограми, ЗМІ, інтернет, книги, шоу-бізнес) у системі інформаційного споживання українських громадян протягом усього радянського і частково пострадянського періоду. Існує великий обсяг і інших загроз із боку російських агентів впливу. Цілком очевидно, що такий стан справ є також наслідком багаторічного ігнорування державою проблем інформаційної безпеки.

Отже, сьогодні забезпечення інформаційної безпеки потребує надзусиль з боку держави. Однак, найкраща відповідь на виклики інформаційної безпеки полягає не в обороні, а в створенні системи розвитку інформаційного простору України. Держава має бути суб'єктом цього процесу, максимально використовувати можливості стратегічних комунікацій, державного та приватного партнерства, застосовувати для цього в тому числі фінансово-бюджетні інструменти, які можуть бути використані в рамках державних програм.

**Література**

1. Степанов В.Інформаційна безпека як складова державної інформаційної політики [Електронний ресурс]. – Режим доступу : http://www.kbuapa.kharkov.ua.

2. Доктрина інформаційної безпеки України: Затверджено Указом Президента України від 08.07.2009 No 514/2009 /втратила чинність 30.06.2014. Режим доступу : https://zakon.rada.gov.ua.

3. Кріслата О. Гібридна війна та її інформаційна складова [Електронний ресурс] – Режим доступу:http://www.lsl.lviv.ua.

4. Ткачук Т. Сучаснізагрозиінформаційнійбезпецідержави: теоретико-правовий аналіз [Електронний ресурс]. – Режим доступу :http://pgp-journal.kiev.ua.

*УДК 341.824:338.47 (043.2)*

**Туяхов А. О.**
Національна академія СБ України

## ГІБРИДНИЙ ТРОЛІНГ ЯК ІНСТРУМЕНТ ІНФОРМАЦІЙНИХ ВОЄН

«Здобути сто перемог в ста битвах – це не вершина військового мистецтва. Повалити ворога без бою – ось його вершина» [1].

Саме цей вираз відомого китайського філософа та полководця IV ст. до н. е. Сунь-Цзи є досить влучним, коли йдеться про інформаційну війну.

Інформаційна війна (ІВ) – форма ведення інформаційного протиборства між різними суб'єктами, що передбачає здійснення комплексу заходів із завдання шкоди інформаційній сфері конфронтуючої сторони й захисту власної інформаційної безпеки [2].

Конфлікт на сході України має характерні ознаки «гібридної війни», коли окрім традиційної збройної боротьби за допомогою вогнепальної зброї застосовується новий тип – інформаційна зброя.

З початку збройного конфлікту Російська Федерація використовувала пропаганду та дезінформацію через засоби масової інформації для дестабілізації політичної та економічної ситуації в Україні, але стала отримувати проактивну відповідь на такі свої дії. Тому агресор почав використовувати нові методи ведення ІВ, одним із яких є «гібридний тролінг».

Саме поняття «тролінг» означає комунікації, мета яких – формування розбіжностей та підбурювання конфліктів в онлайновому середовищі в інтересах окремих особистостей.

Україна стала центральною країною, в інформаційному просторі якої широко розповсюджується російський тролінг. Тролінг є лише частиною великої гібридної війни Російської Федерації проти України. Російські спецслужби використовують тролінг для дескридитації України та української влади в очах як самих українців, так і – світової спільноти.

У 2015 році Служба безпеки України офіційно заявила, що Федеральна служба безпеки Російської Федерації використовувала пропаганду для дестабілізації ситуації в Україні. Вони використовували пости в соціальних мережах, які публікувалися тролями, підконтрольними ФСБ РФ, та випуски новин, які також контролювалися ФСБ. Варто зазначити, що тролі можуть зламувати сторінки політиків, як наприклад, російські хакери у 2016 році зламали акаунти Президента України та Міністра внутрішніх справ України у Твіттері.

Тому українська влада вдалася до жорстких заходів боротьби з тролінгом. Так 15 березня 2017 року за указом Президента України були заблоковані в Україні російські інтернет-ресурси: Яндекс, mail.ru, Вконтакті (ВК) та Одноклассники. Проте блокування цих сайтів не стало досконалим способом захисту від впливу кремлівських тролів, оскільки на початку блокування ВК та Одноклассників певні громадяни України мали змогу обходити цю заборону, користуючись VPN-додатками.

Окремими сучасними видами тролінгу, які використовують іноземні спецслужби проти України є:

- *тролінгові повідомлення-звинувачення США у змові* (контент представлений довгими текстами, де логічно подана аргументація, спрямована на «викриття істини»);
- *тролінгові повідомлення-бікіні* (представлені короткими нелогічними повіломленнями. Як правило, він супроводжується фотографією профілю дівчини у бікіні);
- *агресивні тролінгові повідомлення* (даний тип повідомлень спрямований на продовження словесного конфлікту);

- *тролінгові повідомлення Вікіпедії* (містять фактичну інформацію з Вікіпедії або інших авторитетних джерел).
- *тролінгові повідомлення-вкладиші* (представлені короткими текстами з посиланнями, що містять важливу інформацію);
- *тролінгові повідомлення-провакації* (головна ідея цих повідомлень – вибратись з безнадії та зради в Україні можливо лише за умов насильства);
- *показово патріотичні тролінгові повідомлення* (містять патріотичну символіку та лозунги) [3].

**Висновки.** Гібридний тролінг як інструмент інформаційної війни – це комплекс методів пропаганди та контрпропаганди, заснований на прицинах Інтернет-тролінгу, спрямованих на деструктивний вплив в інформаційному суспільстві. Тролінг, як психологічний аспект інформаційної війни, продовжує свій розвиток, набуваючи нових форм впливу на свідомість та підсвідомість українського суспільства. Також варто звернути увагу на те, що тролінг починає виходити за межі кіберпростору та проявляться в реальному житті. Тож тролінг слід визначати як окремий елемент інформаційної безпеки України. А протидію тролінгу в інформаційному просторі України – як важливу складову забезпечення інформаційної безпеки держави в сучасних умовах інформаційних воєн.

**Література**

1. Сунь Цзи. Мистецтво війни / Сунь Цзи. – Харків: Клуб сімейного дозвілля, 2016 рік. – Режим доступу: https://www.bookclub.ua/ukr/read/ sun_tzu/the_ art_of_war/.

2. Інформаційна безпека держави: підручник / [В.М.Петрик, М.М. Присяжнюк, Д.С.Мельник та ін.]; в 2 т.– / за заг. ред. В.В.Остроухова – К.: ДНУ «Книжкова палата України», 2016. – Т.1. – 264 с., Т.2. – 328 с.

3. Alexander Fokin. Troling and Russia's Military Strategy / Alexandr Fokin. Internet trolling as a tool of hybrid warfare: the case of Latvia. – 2016. [Електронний ресурс] – Режим доступу: https://www.google.com.ua/ search?ei=6dhfXvaGB7OWjgbss7PgBg&q=Alexander+Fokin+Troling+and+Russia %27s+Military+Strategy+%5CAlexandr+Fokin&oq=Alexander+Fokin+Troling+and +Russia%27s+Military+Strategy+%5CAlexandr+Fokin&gs_l=psy-ab.3...234954.238462..239830...0.0..0.258.866. 1j4j1.....0....2j1..gws-wiz.9uqxDEQiG8&ved=0ahUKEwi2n6ycoIHoAhUzi8 MKHezZDGwQ4dUDCAo &uact=5.

*УДК 35.977.535.3*
**Фролова К. С.**
**Гоц О. В.**
Національна академія СБ України

# СТАНДАРТИЗАЦІЯ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ В УКРАЇНІ

Кожного дня держави тим чи іншим чином стикаються з кібератаками і Україна не виключення. Для управління інформаційною безпекою, виявлення злочинців та їх покарання існують міжнародні стандарти. Щоб створити повноцінну архітектуру системи безпеки, використовують стандарти, які умовно можна поділити на такі групи: 1. Оціночні стандарти; 2. Стандарти, які визначають обов'язкові вимоги до СУІБ; 3. Стандарти, щодо рекомендацій і вимог до аудиту СУІБ; 4. Стандарти, що пропонують вдосконалення і розвиток СУІБ.

Існує серія міжнародних стандартів ISO / IEC 27000 для системи управління інформаційною безпекою. Вони забезпечують інформаційну безпеку організацій. Впровадження цих стандартів в діяльність організації сприяє безпеці таких даних, як фінансова інформація, інтелектуальна власність, відомості про співробітників або інформацію, надану третіми сторонами. Існує "сімейство" стандартів 27000, їх нараховують більше десятка. Одним з цих стандартів є ISO / IEC 27001. Він найбільш відомий серед усіх стандартів, цей стандарт можна описати як збірник світових практик в області управління інформаційною безпекою.

Згідно з прийнятим 5 жовтня 2017 року Законом України «Про основні засади забезпечення кібербезпеки України», функціонування національної системи кібербезпеки, серед іншого забезпечується шляхом «досягнення сумісності з відповідними стандартами Європейського Союзу та НАТО», а також з урахуванням «кращих світових практик і міжнародних стандартів з питань кібербезпеки та кіберзахисту» [1].

Згідно з чинним законодавством України всі об'єкти кіберзахисту в Україні абсолютно вільні у виборі і розробці стандартів інформаційної безпеки, якщо інше не передбачено нормативно правовими актами. Проте згідно з законом «Про основні засади забезпечення кібербезпеки України» загальні вимоги, вимоги і порядок проведення незалежного аудиту інформаційної безпеки, відповідальність за забезпечення кіберзахисту та обмін інформацією про інциденти кібербезпеки, що містить персональні дані є особливим для об'єктів критичної інфраструктури.

З 2015 року Україна почала вводити систему міжнародних стандартів в дію: Національний орган стандартизації «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» (далі ДП «УкрНДНЦ») затвердив 4 таких національних стандартів

для України: 1. ДСТУ ISO/IEC 27000:2015 «Огляд і словник»; 2. ДСТУ ISO/IEC 27001:2015 «Вимоги»; 3. ДСТУ ISO/IEC 27002:2015 «Звід практик щодо заходів інформаційної безпеки»; 4. ДСТУ ISO/IEC 27005:2015 «Управління ризиками інформаційної безпеки» [3].

Зазначений раніше стандарт ISO/IEC 27000 оновлюється щорічно і пропонує новітні рекомендації в області інформаційної безпеки. Так, наприклад, в наказі ДП «УкрНДНЦ» від 04.08.2017 № 207 прийняті національні нормативні документи, гармонізовані з європейськими нормативними документами, методом підтвердження з наданням чинності з 01 жовтня 2017 року, серед яких є стандарти, пов'язані з інформаційними технологіями та методами їх захисту: 1. ДСТУ ISO/IEC 11577:2017 (ISO/IEC 11577:1995, IDT) Інформаційні технології. Взаємозв'язок відкритих систем. Протокол захисту мережевого рівня. 2. ДСТУ ISO/IEC 15408-1:2017 (ISO/IEC 15408-1:2009, IDT) Інформаційні технології. Методи захисту. Критерії оцінки. Частина 1. Вступ та загальна модель. 3. ДСТУ ISO/IEC 15408-2:2017 (ISO/IEC 15408-2:2008, IDT) Інформаційні технології. Методи захисту. Критерії оцінки. Частина 2. Функціональні вимоги. 4. ДСТУ ISO/IEC 15408-3:2017 (ISO/IEC 15408-3:2008, IDT) Інформаційні технології. Методи захисту. Критерії оцінки. Частина 3. Вимоги до гарантії безпеки. 5. ДСТУ ISO/IEC 19785-4:2017 (ISO/IEC 19785-4:2010, IDT) Інформаційні технології. Загальна структура форматів обміну біометричними даними. Частина 4. Специфікація формату блоку захисту інформації. 6. ДСТУ ISO/IEC 27000:2017 (ISO/IEC 27000:2016, IDT) Інформаційні технології. Методи захисту. Системи менеджменту інформаційної безпеки. Огляд і словник термінів – На заміну ДСТУ ISO/IEC 27000:2015 (ISO/IEC 27000:2014, IDT)[2].

Безумовно, зорієнтованість України на світовий досвід може позитивно вплинути та модернізувати управління ризиками і захист інформаційних ресурсів. Необхідно зазначити, що використання зазначених стандартів покращить систему менеджменту інформаційної безпеки на всіх рінях і зробить більш безпечними усі сфери інформаційного життя.

**Література**

1. Закон України: «Про основні засади забезпечення кібербезпеки України» від 21 червня 2018 р. № 31 //Відомості Верховної Ради. – 2017. – № 45. – Ст. 403.

2. Режим доступу до статті : http://csm.kiev.ua/index.php?option=com_content&view=article&id=3964:2017-08-08-06-22-17&catid=122:2015-09-15-07-01-23&Itemid=104&lang=uk.

3. Режим доступу до статті :http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66151.

*УДК: 351.1*
**Чучумашев О. І.**
**Хмельницький О. О.**
кандидат педагогічних наук,
Національна академія СБ України

# УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА ЗАХИСТІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Однією із складових частин національної безпеки країни – є інформаційна безпека, при грамотному розпорядженні інформаційної стратегії буде сприятливе забезпечення досягнення здобутку при постанові задач у соціальній, економічній, політичній, військовій та інших сферах державної діяльності.

При провадженні у життя вдалої інформаційної політики, може суттєво змінитися розв'язання внутрішньополітичних, зовнішньополітичних та військових конфліктів. Знання у сфері інформаційної безпеки виступають, з одного боку, як предмет забезпечення життя та інтересів людини, суспільства а з другого – як об'єкт безпосереднього захисту. Методологічні засади інформаційної безпеки є єдність концептуальних, технологічних і теоретичних основ забезпечення на інформаційному рівні безпеки всіх сфер політичної, економічної, соціальної, воєнної, екологічної, духовної та ін. Предмет методології інформаційної безпеки є дослідження засобів і каналів реалізації загроз національним інтересам на інформаційному просторі та їх своєчасне виявлення, запобігання та нейтралізація.

Мета вивчення дисципліни «Інформаційна безпека держави» – це основний пріоритет держави для формування знань своїх громадян про основи інформаційної безпеки, засоби забезпечення інформаційної безпеки держави, правила відношення інформації до державної таємниці, конфіденційної інформації, захист інформаційного суверенітету України. Формування в інформаційному просторі української ідентичності як невід'ємної складової сталого суспільно-політичного дискурсу, захищеність особи від втручання в її особисте та сімейне життя, недержавної конфіденційної і відкритої інформації що потребує захисту, шляхи побудови систем забезпечення інформаційної безпеки.

**Література**

1. Степанов М. М., Кравченко О. В. Інформаційна безпека держави, арх. док. – Київ : КНУ ім. Тараса Шевченка., 2017. – [1] с. – (Перелік вибіркових дисциплін).

2. Голев Д.В., Кільдишев В.Й., Кононович В.Г. Інформаційна безпека інформаційно-комунікаційних систем. Лабораторний практикум. Частина 1 – Комплекси засобів захисту інформації від НСД: навч. посіб. / за ред. чл.-кор. МАЗ В.Г. Кононовича. – Одеса: ОНАЗ ім. О.С. Попова, 2010. – С. 176.

*УДК:004.056*
**Шкромида Р. Р.**
**Воскобойніков С. О.**
кандидат педагогічних наук,
Національна академія СБ України

# PENETRATIONTESTING. МЕТОДИКА ПРОВЕДЕННЯ

Інформатизація всіх галузей науки, економіки і господарства зумовлює зручніше та швидше надання різноманітних послуг, здійснення фінансових розрахунків, доступ до публічної інформації, разом з тим створює нові загрози як для суспільства, так і для держави. Нагальними загрозами на даний час є по-перше порушення доступності інформаційних ресурсів, що зберігаються в комп'ютерних системах, по-друге, це порушення конфіденційності та цілісності інформації.

Згідно із дослідженням компанії Cisco, 53% атак на комп'ютерні мережі завдають шкоди установам, підприємствам та організаціям на понад 500 000 доларів США. Основною причиною виникнення подібних ситуацій є недостатня кількість спеціалістів в сфері інформаційної безпеки [1, 5, 7].

В нашій країні найбільш резонансними атаками (втручанням в роботу комп'ютерних систем) стали BlackEnergy (атака на інформаційно-телекомунікаційні системи Міністерства фінансів, Державної казначейської служби) та PetyaA [4].

І саме для того, щоб попередити злочини, що можуть нанести шкоду інформаційній безпеці використовують Тест на проникнення.

*Тест на проникнення* (англ. – Penetrationtesting, далі ПенТест) – метод оцінювання захищеності комп'ютерної системи чи мережі шляхом часткового моделювання дій зовнішніх зловмисників з проникнення у неї (які не мають авторизованих засобів доступу до системи) і внутрішніх зловмисників (які мають певний рівень санкціонованого доступу). Цей процес включає активний аналіз системи з виявлення будь-якої потенційної вразливості, що може виникати внаслідок неправильної конфігурації системи, відомих і невідомих дефектів апаратних засобів та програмного забезпечення, чи оперативне відставання в процедурних чи технічних контрзаходах [6].

Найчастіше ПенТест проводять для того, щоб:

– оцінити захищеність нової інформаційної системи, де буде оброблятися важлива інформація;

– оцінити захищеність системи після її покращення, оновлення;

– дотримуватись вимог міжнародних стандартів інформаційної безпеки;

– спланувати кількість витрат на забезпечення інформаційної безпеки.

Враховуючи, те, що всі комп'ютерні системи відрізняються одна від одної, виникає питання щодо раціонального підходу з проведення ПенТесту [1, 6].

На даний момент найбільш розповсюдженими методами що використовуються для проведення тестування на проникнення є:

– The Open Source Security Testing Methodology Manual (OSSTMM);

– OWASP Testing Guide;

– Penetration Testing Execution Standard (PTES);

– The National Institute of Standards and Technology (NIST) Special Publication 800-115;

– Information Systems Security Assessment Framework (ISSAF) [6].

Кожен з методів має свої особливості, недоліки та переваги. Тому для проведення тестування на проникнення потрібно вибрати найбільш оптимальний метод. Враховуючи різні фактори можна привести наступну класифікацію методів тестування на проникнення:

– за обізнаністю пентестера про цільову систему;

– білий ящик;

– чорний ящик;

– сірий ящик [2, 6].

При оцінюванні системи методом білого ящика замовник повинен надати пентестеру повну інформацію про цільову систему, її системи захисту. В деяких випадках пентестеру можуть навіть надати адміністративний доступ. Зазвичай тестування проводять в співпраці із працівниками інформаційної безпеки підприємства система якого тестується. Використовуючи даний метод можна отримати найбільш повні результати про стан захищеності системи. Також цей метод являється доволі швидким та якісним [2, 6].

У свою чергу при оцінці системи методом чорного ящика замовник не надає пентестеру ніякої інформації, або ж необхідний мінімум (наприклад адреса сайту компанії, її назва, тощо). Даний метод вважається одним із найбільш приближених до реальності. Коли проводять тестування методом чорного ящика про це повідомляється керівництво відповідних служб інформаційної безпеки компанії. Завданням пентестера являється непомітне проникнення в систему отримання з неї певної інформації та вихід з неї без залишення в ній слідів присутності, чи діяльності пентестера [1].

Результати подібного тестування залежать в першу чергу від кваліфікації пентестера та можуть не відображати справжньої ситуації з інформаційною безпекою. До того ж при проведенні подібного тестування пентестер може пропустити деякі сервіси [2, 6].

Даний варіант вважається найоптимальнішим за витратами часу та якістю.

Здійснюючи замовлення тестування на проникнення даним методом, пентестеру надають певну інформацію про систему (ip-адреси серверів, адреси сайтів даного підприємства чи адресу електронної пошти, тощо). Використовуючи даний метод тестування можна вважати, що пентестер виступає інсайдером, або людиною, що отримала певну інсайдерську ін-

формацію. Використовуючи надану інформацію він повинен ввійти в систему й розширити свої повноваження для доступу до інформації, що захищається.

За рівнем обізнаності працівників організації-замовника про проведення тестування на проникнення:

– відкрите;

– приховане.

Відкрите тестування проводиться у разі, якщо приховане тестування не призводить до будь-якої реакції зі сторони технічних працівників, або якщо проводиться тестування методом білого ящика. Дане тестування дозволяє працівникам організації-замовника ознайомитися із методами і засобами проведення тестування на проникнення та на практиці ознайомитися із приблизним порядком дій зловмисника [1, 4, 6].

Приховане тестування використовується в тому випадку, якщо замовник окрім самого тестування на проникнення хоче ще й перевірити системи попередження вторгнення в систему, організаційні чи кадрові структури. Про проведення тестування повідомляються тільки керівники сектору безпеки та керівник підрозділу, що здійснює адміністрування комп'ютерних систем. Подібний метод окрім виконання основного завдання дозволяє ще й перевірити професіоналізм працівників та якість реалізації політики безпеки організації [1, 6, 7].

За характером дій що проводяться:

– пасивне тестування;

– агресивне тестування;

– обережне тестування;

– прораховане тестування [6, 3].

При проведенні пасивного тестування цільова система сканується з метою виявлення відомих вразливостей. В тому разі, якщо їх виявили, вони не використовуються, а тільки фіксуються.

При проведенні агресивного тестування для атаки використовуються всі можливості, тому тестувальник повинен враховувати, що окрім основної системи, можуть постраждати ще й сусідні системи [1, 6, 7].

При проведенні обережного тестування даним методом виявлені вразливості будуть використані лише тоді, коли вони не завдадуть ніякої шкоди цільовій системі.

При використанні прорахованого тестування, пентестер намагається використовувати знайдені вразливості, але перш ніж їх використати, він прораховує можливі наслідки й діє в залежності від прийнятого рішення.

За повнотою виконання тестування:

– повне – даний тип тестування зазвичай проводиться для систем, що тестуються вперше. Він дозволяє найбільш повно виявити недоліки усіх комп'ютерних систем організації-замовника. Час затрачений на дане тестування залежить від одноманітності систем;

– обмежене – при даному тестуванні замовник визначає які саме системи підлягають перевірці;

– фокусоване – метод тестування для перевірки однієї підмережі або служби. Зазвичай його використовують після проведення модифікації чи розширення комп'ютерної системи. І хоча він дозволяє швидко й повно надати інформацію щодо протестованої системи, він не дозволяє дізнатися інформацію про захищеність всієї інфраструктури організації-замовника [2, 6].

За розташуванням програмно-апаратних засобів та пентестера відносно периметру організації замовника:

– зовнішнє – тестування, яке дозволяє отримати та оцінити ризики атак на комп'ютерні системи через мережу Інтернет, при проведенні подібного тестування надається початкова інформація (назва компанії, офіційний сайт, ір-адреси, тощо) та ставиться завдання щодо отримання доступу до внутрішньої мережі організації-замовника та подальше її дослідження;

– внутрішнє, при використанні подібного виду тестування замовник надає змогу пентестеру підключити своє обладнання до комп'ютерної мережі, що буде тестуватися. Внутрішній тест дозволяє замовнику оцінити які можливості будуть у зловмисника якщо він знайде спосіб потрапити у внутрішню мережу або, якщо зловмисниками будуть певні особи із організації замовника [2].

За видом інструментів, що використовуються:

– із застосуванням програмно-апаратних засобів;

– із застосуванням методів соціальної інженерії та проникнення на контрольну територію.

Дана класифікація узагальнює та структурує методи проведення пентестів. Це дозволяє визначити оптимальні шляхи проведення тестування на проникнення та погодити їх із замовником.

**Література**

1. Positive Technologiesберугрозы. I квартал 2019. Актуальные киберугрозы. I квартал 2019 [Електронний ресурс] / Positive Technologiesберугрозы. I квартал 2019 // Блог компании Positive Technologies. – 2019. – Режим доступу до ресурсу: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-q1-2019/.

2. Джеймс Фостер, при участии Майка Прайса Защита от взлома: сокеты, эксплойты, shell-код: Пер. с англ. Слинкина А.А. – М.: Издательский Дом ДМК-пресс. – 784 с.: ил. [Електронний ресурс] Д.Фостер – Режим доступу до ресурсу: https://books.google.com.ua/books?id=URDRAAAAQBAJ&printsec=frontcover&hl=ru&redir_esc=y#v=onepage&q&f=false.

3. Казарін О. В. Надійність і безпека програмного забезпечення [Електронний ресурс] / О. В. Казарін. – 2018. – Режим доступу до ресурсу: https://it-integrator.ua/sites/default/files/imce/SecurityCisco/cisco_cybersecurity2018.pdf.

4. Кенин А. М. Самоучитель системного администратора / А. М. Кенин, А.Д Колесниченко. – 4-е изд., перераб. и доп. – СПб.: БХВ-Петербург, 2016. – 528 с.

5. Компанія Эшелон. Статистика выявления уязвимостей в программном обеспечении в рамках сертификационных испытаний [Електронний ресурс] / Эшелон компанія // Блог компании Эшелон, Информационная безопасность. – 2017. – Режим доступу до ресурсу: https://it-integrator.ua/sites/default/files/imce/SecurityCisco/cisco_cybersecurity2018.pdf.

6. Парасрам Шива, Замм Алекс, Хериянто Теди, Али Шакил, Буду Дамиан, Йохансен Джерард, Аллен Ли. Kali Linux. Тестирование на проникновение и безопасность. – СПб.: Питер, 2020. – 448 с.: ил. – (Серия «Для профессионалов») [Електронний ресурс]. – Режим доступу до ресурсу : https://play.google.com/books/reader?id=0K6tDwAAQBAJ&pg=GBS.PA92.

7. Річний звіт компанії Cisco [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://it-integrator.ua/sites/default/files/imce/SecurityCisco/cisco_cybersecurity2018.pdf.

# РЕКОМЕНДАЦІЇ
## XI Всеукраїнської науково-практичної конференції: “Актуальні проблеми управління інформаційною безпекою держави”

За ініціативи Національної академії Служби безпеки України, спільно з Науково-дослідним інститутом інформатики і права Національної академії правових наук України та Інститутом модернізації змісту освіти Міністерства освіти і науки України, 15 травня 2020 року проведено XI Всеукраїнську науково-практичну конференцію «Актуальні проблеми управління інформаційною безпекою держави».

Учасники науково-практичної конференції ***констатують***:

– нинішній етап світової історії характеризується утвердженням інформаційної цивілізації, в основі розвитку якої лежать знання, засновані на інформації. Водночас суспільство, на думку багатьох дослідників, «*з великим запізненням починає осмислювати політичні, економічні, соціальні, військові, психологічні та інші наслідки глобальної інформатизації*». Інформаційним є таке суспільство, в якому відбуваються інтенсивні світоглядні трансформації, де головними цінностями стають інформація, а також пов’язані з нею симулякризація й віртуалізація, що стимулюють зміни аксіологічних пріоритетів, взаємини й комунікації людей, співвідношення свободи й відповідальності. При цьому сама цінність людської особистості знижується через превалювання аспектів утилітарності і прагматичності, як у контактах, так і в тій інформації, якою людина оперує;

– низку проблем системного характеру стосовно реалізації Стратегії кібербезпеки України, що негативно впливає на всю сферу кібербезпеки та кіберзахисту України та є свідченням формального підходу з боку відповідальних державних органів до стратегічного планування, формування та реалізації державної політики, а також здійснення відповідного стратегічного контролю;

– потребу обґрунтування закономірностей позитивних інформаційних процесів та заходів з попередження шкідливого впливу інформаційного середовища на здоров’я суспільства з еколого-гігієнічних позицій;

– саме навчання, інформаційне просвітництво, а не заборони й обмеження, мають стати пріоритетом у державній та міжнародній інформаційній політиці. Сьогодні, в епоху вибухового поширення й удосконалення інформаційно-комунікаційних технологій, заборонні, обмежувальні чи репресивні заходи можуть бути малопродуктивними та навіть мати зворотний ефект. Людина може повірити фейковій інформації, коли їй бракує відповідних знань у сфері, якої ця інформація стосується;

– доцільність прийняття базового Закону України «Про інформаційну безпеку України» задля консолідації, вдосконалення відповідного за-

конодавства, чіткої структуризації системи нормативно-правових актів у цій галузі, усунення наявних суперечностей, правових лакун тощо.

За результатами обговорення винесених на розгляд актуальних проблем учасники науково-практичної конференції ***рекомендують***:

– розширити механізми взаємодії державних органів і представників ІТ-бізнесу, приватного сектору безпеки з метою підвищення довіри між приватними суб'єктами та державними органами з використанням апробованих договірних і правових механізмів США, країн ЄС щодо обміну інформації про позиції та інтереси учасників, зокрема й визначення можливості формування недержавних регуляторних органів, формування системних підходів до підготовки й підвищення кваліфікації кадрів як державних, так і недержавних суб'єктів, з питань обміну інформацією щодо кіберінцидентів тощо;

– законодавчо визначити поняття «приватність», «конфіденційна інформація» та «безпека персональних даних» з деталізацією істотних ознак їх предметного змісту та істотних ознак (уніфікованих критеріїв) щодо поняття «конфіденційність»;

– запропонувати Міністерству освіти і науки України визначити пріоритетами у забезпеченні кібербезпеки людини заходи навчально-просвітницького характеру, особливо серед дітей та молоді. Навчання інформаційної гігієни слід розпочинати зі шкільного, ба навіть дошкільного, віку, оскільки саме тоді закладаються основи формування світогляду людини, трансформується її індивідуальна свідомість, запускаються процеси інтелектуалізації. В контексті існуючої системи освіти можна вести мову про запровадження в загальноосвітніх школах курсу інформаційної гігієни як науки, що вивчає закономірності впливу навколишнього інформаційного середовища на організм людини, здоров'я її та суспільства;

– розробити критерії та започаткувати впровадження механізму оцінки ефективності реалізації Стратегії кібербезпеки України на державному рівні.

# ЗМІСТ

## УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА ЗАХИСТІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Наукове видання

# АКТУАЛЬНІ ПРОБЛЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ

**XI Всеукраїнська науково-практична конференція**

**Збірник тез наукових доповідей**
**(Київ, 15 травня 2020 року)**

*Електронне видання*

*Авторська редакція*

Технічне редагування, макетування *Т. О. Коркач*

Видавець і виготовлювач
Національна академія Служби безпеки України,
03066, Київ, вул. Михайла Максимовича, буд. 22.
факс: (044)257-30-35
E-mail: academy@ssu.gov.ua
Свідоцтво суб'єкта видавничої справи ДК № 6844 від 17.07.2019.