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

VII Науково-практична конференція

Збірник матеріалів
(Київ, 18 березня 2016 року)

У двох частинах

Частина 1

Електронна версія на CD-ROM

Київ
2016

Електронна версія друкованого видання

Актуальні проблеми управління інформаційною безпекою держави : зб. матер. наук.-практ. конф. (Київ, 18 березня 2016 року) : у 2 ч. Ч. 1. – Київ : Нац. акад. СБУ, 2016. – 296 с.

УДК 341.123(045)(0.034.2PDF)

Організаційний комітет конференції:

Кудінов С.С. – голова організаційного комітету конференції,
т.в.о. ректора НА СБ України полковник;
Пилипчук В.Г. – заступники голови, директор
Науково-дослідного інституту інформатики і права НАПрН України;
Лещик Н. В. – завідувач сектору зовнішніх комунікацій
Інституту модернізації змісту освіти

Чорний Р. Л. – директор НОЦ НА СБ України;
Мамченко С. М. – директор ННІ ІБ НА СБ України;
Панченко В. М. – заступник директора Інституту
(з навчальної та наукової роботи) ННІ ІБ НА СБ України;
Климчук О. О. – завідувач СК-31 ННІ ІБ НА СБ України;
Гуз А. М. – завідувач СК-32 ННІ ІБ НА СБ України

Актуальні проблеми управління інформаційною безпекою держави: зб. матер. наук.-практ. конф. (Київ, 18 березня 2016 року) : у 2 ч. Ч. 1. – Електрон. дані. – Київ : Нац. акад. СБУ, 2016. – 1 електрон. опт. диск. (CD-ROM) : 12 см. – Назва з тит. екрана.

У збірнику висвітлюються актуальні проблеми забезпечення інформаційної безпеки України та науково-практичні підходи до їх вирішення. Зокрема, розглядається питання захисту інформаційного простору України, формування системи забезпечення кібернетичної безпеки України, удосконалення вітчизняного законодавства у сфері охорони державної та службової інформації, форми і напрями міжнародної взаємодії у сфері забезпечення інформаційної безпеки, шляхи оновлення змісту вищої освіти фахівців з інформаційної безпеки держави.

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

Тези доповідей публікуються в авторській редакції. Організаційний комітет залишає за собою право не розділяти думку авторів.

Шановні учасники і гості конференції!

Уже стало доброю традицією в березні кожного року збирати в стінах Національної академії Служби безпеки України науковців та практиків, котрі опікуються проблемами управління інформаційною безпекою держави. І нам дуже приємно, що завдяки створеній науково-практичній платформі ми маємо можливість щороку не лише побачитись і поспілкуватися з нашими давніми, добрими друзями, а й отримати нових, водночас проаналізувати, практично переосмислити, нормативно змоделювати вкрай важливі для нашої держави проблеми забезпечення національної безпеки в інформаційній сфері.

Понад два роки Україна перебуває у стані так званої «гібридної війни». І хоча кожен конкретний її елемент по суті не новий і раніше застосовувався майже в усіх збройних конфліктах, однак унікальним для цієї війни є зростання ваги інформаційного чинника. Причому в окремих випадках він не менш важливий, ніж військовий. Про масштаби інформаційної війни, розгорнутої Російською Федерацією проти України, найбільш точно сказав Головнокомандувач об'єднаних Збройних сил НАТО в Європі Філіп Брідлав: «Це найбільш дивовижний інформаційний бліцкриг, який ми коли-небудь бачили в історії інформаційних воєн».

Інформаційний фронт «гібридної війни» розгортається одразу на кількох напрямах, передусім: серед населення в зоні конфлікту; серед населення країни, проти якої здійснюється агресія, але територія якої не охоплена конфліктом; серед як громадян країни – агресора, так і міжнародного співтовариства. Сьогодні ми маємо справу не просто з ворожою пропагандою, а й, як її характеризують, фахівці «війною смислів». Трансграничним середовищем боротьби став кіберпростір, правила гри в якому не регламентовані ні вітчизняним законодавством, ні міжнародним правом.

Однією з причин недосягнення успіхів у зазначеному протистоянні є відсутність в Україні сформульованого на концептуальному рівні правового підґрунтя для захисту інформаційної сфери, необхідність приведення законодавства в цій сфері до стандартів країн ЄС та НАТО. Так, на сьогодні розроблено низку нормативно-правових актів – Концепція забезпечення інформаційної безпеки України, Стратегія розвитку інформаційного простору

України. Проте сьогодні вони залишаються лише проектами, побіжний аналіз яких свідчить про їхню неузгодженість та відсутність системності у підходах до формування загальнодержавного механізму забезпечення інформаційної безпеки. І це в той час, як Російська Федерація, за оцінками фахівців НАТО, на сьогодні має найбільш продуману й ефективну військову доктрину в інформаційній сфері.

Наявність зазначених загроз та умов визначає необхідність і важливість підготовки фахівців, які оволодіють відповідною компетенцією у сфері інформаційної безпеки як державного, так і міжнародного рівнів. Незважаючи на відсутність у новому переліку галузей знань напряму підготовки «Інформаційна безпека», Національна академія СБ України, за підтримки керівництва СБ України, відстоюючи позицію про доцільність його повернення, наполегливо працює над збереженням цього напряму підготовки в умовах мінливості вітчизняного законодавства в освітянській сфері. Так, у 2016 році до Навчально-наукового інституту інформаційної безпеки планується набір студентів за спеціальностями: «Менеджмент» (спеціалізація – організація захисту інформації з обмеженим доступом); «Право» (спеціалізація – забезпечення інформаційної безпеки) та «Кібербезпека» (спеціалізація – управління інформаційною безпекою). Для забезпечення системи охорони державних секретів висококваліфікованими кадрами, на виконання Річної національної програми співробітництва Україна-НАТО на 2016 рік, затвердженої Указом Президента України від 12 лютого 2016 року № 45/2016, у грудні 2016 р. на базі Національної академії СБ України планується проведення семінару з підвищення кваліфікації працівників державних органів, підприємств, установ та організацій України, що працюють з інформацією НАТО з обмеженим доступом.

Актуальність обговорення і важливість пошуку шляхів вирішення проблем протидії інформаційній агресії, удосконалення правового забезпечення інформаційної сфери, формування загальнонаціональної системи кіберзахисту та міжнародної співпраці у цій сфері, а також підготовки кадрів підтверджена нашим кворумом. Адже взяти участь у роботі нашої конференції виявили бажання більше 200 фахівців з питань інформаційної безпеки із 6 міністерств, відомств, та понад 20 навчальних закладів і наукових установ.

У цьому році ми дещо змінили формат заходу, організувавши його роботу відповідно до кращих європейських практик. Сподіваємося, що саме такий підхід надасть можливість налагодити дискусію і згуртувати наші зусилля навколо вирішення проблем, а не лише їхнього обговорення.

Традиційно, у межах нашого форуму організовано майданчик для молодих учених – студентів, курсантів та аспірантів. Сподіваємося на їхню активну участь у роботі конференції та подальший наполегливий пошук вирішення проблемних питань забезпечення інформаційної безпеки.

Дякую за увагу і бажаю всім плідної роботи!

ЕФЕКТИВНІ МЕХАНІЗМИ ВЗАЄМОДІЇ ТА КООРДИНАЦІЇ ДЕРЖАВНИХ ОРГАНІВ УКРАЇНИ В УМОВАХ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА

УДК 005.3

Аблазов І. В.
кандидат політичних наук, доцент
Воєнно-дипломатична академія імені Є. Березняка
Хамула С. В.
кандидат технічних наук, доцент
Воєнно-дипломатична академія імені Є. Березняка

ШЛЯХИ ОПТИМІЗАЦІЇ ДЕРЖАВНОЇ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ В УКРАЇНІ В УМОВАХ ЗОВНІШНІХ ІНФОРМАЦІЙНИХ ВПЛИВІВ

Ситуація у інформаційному просторі довкола України формується під впливом змін, що відбуваються в системі міжнародних відносин, воєнно-політичної обстановки в регіоні і світі, та, частково, від розвитку внутріполітичної обстановки в нашій Державі [1, с. 33]. Активізація інтеграційних процесів на глобальному і регіональному рівнях характеризується постійним інформаційним протиборством між світовими лідерами, об'єктами якого, як правило, виступає вище державне керівництво, населення, окремі соціальні, політичні та національно-етнічні групи значимих в геополітичному, а також регіональному відношенні країн, і, в першу чергу, України [2, с. 27].

Збройна агресія Російської Федерації проти України стала довгостроковим чинником впливу на українську політичну, економічну, військову та соціальну реальність. І в ній РФ застосовує цілий спектр технічних засобів та комунікативних каналів для широкомасштабного впливу як на населення України, на своє власне населення так і на міжнародну спільноту, здійснюючи вагоме фінансування інформаційних акцій та органів впливу.

Основними напрямами та способами маніпулятивних психоінформаційних технологій РФ відносно України були (та і залишаються надалі):

- поступове пониження міжнародного іміджу України з метою послаблення її геополітичного значення;

- відповідне дозування та спотворення інформації з метою дестабілізації ситуації в державі та впровадження власної політики “керованого хаосу”;

- формування стереотипу меншовартості та вторинності українців, а також відповідне руйнування почуття нації та народу;

- домінування російської мови, культури та традицій для утвердження самоідентифікації при одночасному витісненні української мови та культури [3].

Дієвість інформаційної політики може бути набагато кращою, якщо органи державної влади України стануть активним учасником інформаційного протистояння проводячи власну цілеспрямовану та ефективну інформаційну політику. Необхідно формувати власний інформаційний продукт та створити необхідне технічне підґрунтя для його впровадження, забезпечивши тим самим правдивою інформацією населення України та захистивши свій імідж за кордоном.

Таким чином, в умовах інформаційного впливу Російської Федерації на державну інформаційну політику України, органам державної влади необхідно здійснити комплекс заходів протидії як на власній території так і за кордоном.

Література

1. Аблазов І. В. Аналіз та прогнозування результатів інформаційного впливу на воєнно-політичну ситуацію / І. В. Аблазов // Віче. – 2007. – № 21–22. – С. 33–34.

2. Петрик В.М. Забезпечення інформаційної безпеки держави / В. М. Петрик, М.М. Присяжнюк // Підручник – К. : ДНУ «Книжкова палата України», 2015. – 675 с.

3. Конах В.К. Щодо окремих напрямів вдосконалення державної інформаційної політики України (Аналітична записка) [Електронний ресурс] / Конах В.К. – Режим доступу : www.niss.gov.ua. – Заголовок з екрану.

УДК 351.86: 007

Антонюк В. В.
Національна академія державного управління
при Президентові України

ДЕРЖАВНА ІНФОРМАЦІЙНА ПОЛІТИКА УКРАЇНИ У КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ ПОЛІТИЧНОЇ БЕЗПЕКИ

Ефективність державної інформаційної політики у контексті забезпечення політичної безпеки залежить не від самого процесу її реалізації, а саме від результативності, ефективності впливу на українське населення, ключовими оцінками чого є зростання у народу довіри до влади, вітчизняних ЗМІ, позитивне ставлення цільової аудиторії до роботи українського уряду та реалізації ним реформ, зниження рівня дестабілізаційних чинників у державі. Крім того важливим чинником успішності державної політики є її здатність забезпечити захист свідомості українців від різноманітних деструктивних інформаційно-психологічних впливів, що породжуються у т.ч. реалізацією гібридних загроз, забезпечення ефективного інформаційного впливу на іноземну цільову аудиторію з метою поступового формування проукраїнських політичних поглядів та належного позиціювання України у світі [1, с. 123].

У контексті протидії гібридним загрозам політичній безпеці України, вбачається, що одним із негативних факторів є комерціалізація національних ЗМІ, їх залежність від політичних і економічних (як зовнішніх так і внутрішніх) груп тиску. Зокрема, політичні та економічні групи тиску використовують комерційні (приватні) ЗМІ для досягнення власних інтересів, не завжди враховуючи інтереси суспільства і держави. Вони користуються недосконалістю законодавчого урегулювання “правил гри” в інформаційному полі України. Засоби масової інформації є важливим компонентом у проведенні гібридних війн проти нашої держави. Крім того, ЗМІ є механізмом як підвищення напруги у суспільстві, так і врегулювання соціальних конфліктів. Тому у цьому випадку вникає дилема між питаннями демократичного розвитку країни та її національною безпекою. У цьому сенсі мають місце позитивні зрушення, зокрема, прийняття Закону України “Про внесення змін до деяких законів України щодо забезпечення прозорості власності засобів масової інформації, а також реалізації

принципів державної політики в сфері телебачення і радіомовлення" від 03.09.2015 року № 674-VIII [2].

У ході реалізації державної інформаційної політики у контексті забезпечення політичної безпеки доцільно враховувати наступні пропозиції:

1. Необхідність розробки та прийняття Концепції/Стратегії інформаційно-психологічних операцій (ІПсО) і плану реалізації заходів інформаційно-психологічного впливу із залученням досвідчених фахівців. На її основі розробити програми, проекти, сценарії щодо реалізації українського інформаційного проникнення в інформаційний простір Російської Федерації (а також, до окупованих територій Донбасу, Криму) з метою створення необхідного впливу на світогляд російського населення, що сформований у вакуумі ідеології "русского мира". Таке проникнення доцільно здійснити і до союзних республік Росії, інформаційний простір яких, переважно інтегрований в російський. Зазначене може спростити підходи проникнення до російського інформаційного поля. Одночасно поширення зазначеної інформації буде корисно і на українських територіях, особливо на Сході та Півдні України.

2. Стратегія повинна бути спрямована на формування як позитивних, так і негативних стереотипів. Позитивні - стосовно політичної, стратегічної та національної культури України; вибраного нашою державою західноєвропейського курсу розвитку, закономірностей вказаного процесу; бажання українського народу позбутися корумпованої політичної еліти; устремління українців до розвитку на основі демократичних цінностей, жити за правилами глобальної економіки як єдиного гармонійного всесвітнього організму; розкриття позитивних сторін європейського заможного стилю життя, розвитку економіки, культури, духовних цінностей, ринку праці, рівня достатку у країнах ЄС у порівнянні з російською дійсністю.

Негативні - щодо недолугості політики діючого російського уряду, її відсталості від сучасних вимог глобалізованого світу; монополізації і корумпованості російської економіки; застарілості і догматичності русько-православної ідеології; проблем соціально-класових взаємовідносин в РФ, у контексті соціальної несправедливості і нерівності, безмежній корупції у владі тощо; наявних загроз демографічної кризи в Росії, на фоні поступового

демографічного поглинання тюркським населенням РФ; акцентувати увагу на відсталості РФ у розвитку від держав Європейського союзу та на тому факті, що переважна більшість олігархічної еліти Росії віддає перевагу західноєвропейському стилю життя та навчанню власних дітей, саме, в країнах Заходу, споживає західні товари та послуги на противагу російським неякісним товарам і послугам тощо.

Зазначена інформація може мати форму: повідомлення, роз'яснення, розповіді, розважання, музикально-пісенних творів (особливо, сучасних популярних виконавців), полеміки, науково-освітніх оглядів, кіно-творчості тощо. Вона повинна формуватися у контексті політики, економіки, історії, культури, творчості, музики, спорту, науки, психології, соціології, етно-культурних взаємовідносин, бізнесу тощо. Використовуватися для її поширення повинні всі наявні інформаційні ресурси та можливості держави, приватного сектору, волонтерів, Інтернет-блогерів (зокрема, супутникове телебачення, Інтернет-мережа, радіо тощо). Водночас, дії повинні здійснюватися у єдиному стратегічному задумі та за відповідної фінансової і матеріальної підтримки держави.

3. Особливу увагу необхідно звернути на організацію протидії російській пропаганді в зоні АТО. Міністерство інформаційної політики України , спільно з іншими силами сектору безпеки і оборони доцільно відпрацювати стратегічну тактику протидії російському пропагандистському і дезінформаційному впливу у зоні АТО. Зокрема, підвищити стійкість українських військовослужбовців і місцевого населення до російських деструктивних інформаційних атак. У цьому сенсі, основним завданням державної інформаційної політики має бути - забезпечення систематичного надходження до зони АТО правдивої інформації про Україну, її розвиток та наявні проблеми, причини російсько-українського конфлікту, роз'яснення позиції України у світі та стратегічні цілі діяльності українського уряду.

Крім того, необхідно зосередитися на організації інформаційно-просвітницької роботи у зоні АТО, і не тільки використовуючи сучасні інформаційно-технологічні мережі, але й шляхом безпосереднього контакту представників органів влади держави, Міністерства інформаційної політики України, командування МОУ, ЗМІ, волонтерів з населенням підконтрольних територій та українськими військовослужбовцями.

4. Спільно з компетентними органами сектору безпеки та оборони України розробити спеціальні заходи, зорієнтовані на технічне придушення телекомунікацій ДНР і ЛНР, що використовуються сепаратистами з метою здійснення пропагандистського і психологічного впливу на українських військовослужбовців та населення у зоні АТО. Крім того, вжити адекватні інформаційно-психологічні заходи щодо проукраїнського впливу на окуповані території Донбасу і Криму. З цією метою використати усі наявні національні інформаційно-телекомунікаційні ресурси, а також можливості наших міжнародних партнерів.

Література:

1. До щорічного послання Президента України до Верховної Ради України "Про внутрішнє та зовнішнє становище України в 2015 році": Національний інститут стратегічних досліджень при Президентові України// Аналітична доповідь. – К. : НІСД, 2015. – 684 с.

2. Про внесення змін до деяких законів України щодо забезпечення прозорості власності засобів масової інформації, а також реалізації принципів державної політики в сфері телебачення і радіомовлення: Закон України // Відом. Верховн. Ради України – 2015. - № 674-VIII // [Електронний ресурс]. – Режим доступу: www.rada.gov.ua

УДК 354.42.44

Горовий В. Г.
доктор історичних наук, професор
Національна академія СБ України

АКТУАЛЬНІ ПРОБЛЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ

Дієвість впровадження сучасної Воєнної доктрини України значною мірою залежить від реалізації заходів по досягненню системності в забезпечення воєнної безпеки. І хоча даний документ прямо не визначає інформаційної, інформаційно-психологічної війни як характерної особливості воєнних протистоянь інформаційного суспільства в якості як обов'язкових компонентів силових операцій, так і в якості комплексу спеціальних заходів для досягнення самостійних результатів, однак він окреслює основні проблеми, пов'язані із необхідністю мобілізації суспільства на

створення ефективних механізмів протистояння інформаційній агресії. І даний компонент в системі організації воєнної безпеки з урахуванням закономірностей суспільного розвитку набуває першорядного значення.

Воєнна доктрина вказує на «недостатні та непрофесійні зусилля органів державної влади України у сфері протидії пропаганді та інформаційно-психологічним операціям Російської Федерації, необхідність «удосконалення державної інформаційної політики у воєнній сфері; попередження та ефективна протидія інформаційно-психологічним впливам іноземних держав, спрямованим на підрив обороноздатності, порушення суверенітету і територіальної цілісності України, дестабілізацію внутрішньої соціально-політичної обстановки, провокування міжетнічних та міжконфесійних конфліктів в Україні» [1]. Документ акцентує увагу на необхідності «підвищення ефективності спеціальних інформаційних заходів впливу в районі проведення антитерористичної операції в Донецькій та Луганській областях і на тимчасово окупованій території та зосередження сил і засобів для організації ефективної протидії проведенню ворожих інформаційно-психологічних операцій проти України» [1].

Реалізації положень доктрини мають сприяти зокрема також заходи по забезпеченню наукових установ інформаційними, аналітичними та іншими матеріалами щодо світових досягнень у сфері науки, техніки і технологій, розвитку озброєння, військової та спеціальної техніки, що має також сприяти зростанню наукового, науково-технологічного вкладу вітчизняної науки у зміцнення оборонного потенціалу України, якісному вдосконаленню інформаційного наповнення національних інформаційних комунікацій, що в свою чергу сприятиме вдосконаленню аналітичних спроможностей та взаємозв'язків на державному рівні.

Реалізація передбачених документом завдань обумовлює необхідність максимального використання національного інформаційного потенціалу на рівні, як мінімум, прийнятному для членства в ЄС і НАТО, що сприятиме створенню умов для відновлення державного суверенітету та територіальної цілісності України. Мова при цьому йде саме про результат. І він має здобуватися з урахуванням специфіки розвитку науково-інформаційної системи України.

Дана специфіка, по-перше, полягає в історично обумовленому процесі концентрації виробництва наукової інформації у

системі академічних установ, в організаційній єдності академічної науки [2], що дає можливість для проведення комплексних суспільнозначимих досліджень, в тому числі при вирішенні багатоаспектної проблеми національної інформаційної безпеки, для оперативного співставлення достовірності наукової інформації на міжгалузевому рівні [3], координації досліджень на державному рівні із врахуванням потреб національної оборони.

По-друге, ця специфіка проявляється в розгалуженій системі бібліотечних закладів, що можуть бути в сучасних умовах, при певному рівні комп'ютеризації, використані в якості фільтра негативної інформації, комплектування новими суспільно значимими інтернет-ресурсами вітчизняних інформаційних баз, в якості джерел наповнення якісною інформацією соціальних комунікацій, протистояння в цих комунікаціях ворожій пропаганді.

На ще один негативний фактор вітчизняної специфіки в сфері організації протистояння інформаційній агресії вказується в тексті Воєнної доктрини, де зазначається «недостатній рівень координації і узгодженості дій органів державної влади, органів місцевого самоврядування, низький рівень підготовки їх спеціалістів з питань безпеки і оборони» [1]. Даним рівнем пояснюється відсутність повноцінного державного замовлення в інформаційній сфері, координації відповідної діяльності структур з державним фінансуванням, академічної та університетської науки, мережі бібліотечних та інших, в тому числі інформаційно-аналітичних установ [4], в умовах, коли наявною є потреба в мобілізації суспільних зусиль для забезпечення протистояння негативним інформаційним впливам з-за кордону.

Вітчизняний досвід протистояння в процесі повномасштабної інформаційної війни свідчить, що для забезпечення рівня використання національного інформаційного потенціалу, співзмірного із вимогами до членства в ЄС і НАТО, в умовах надзвичайної інформаційної ситуації необхідним є конкретизація відносин держави з усіма видами ЗМІ, про що вже йшлося в минулих публікаціях [5]. Важливим для протистояння в багатоаспектній інформаційній агресії з застосуванням найновіших, до ментальних включно, інформаційних технологій є чітко вибудуваний національний інформаційний комплекс, що забезпечує необхідну координацію в швидкоплинних процесах інформаційної війни [6].

Таким чином, організація обороноздатності українського суспільства за стандартами НАТО зовсім не означає зламу всієї

вітчизняної структури інформаційного забезпечення суспільства і негайного переведення інформаційних процесів на забезпечення за зразками країн Заходу. З огляду на обсяги затрат на створення такої системи, виходячи із наших економічних реалій сьогодення, видається за доцільне орієнтація на уніфікацію за стандартами західних партнерів саме на рівні результатів, необхідних для оборонних потреб в умовах сучасної інформаційної війни, з урахуванням своєрідності і можливостей наявної в Україні інфраструктури суспільного інформування.

Література

1. Воєнна доктрина України http://www.president.gov.ua/documents/5552015-19443.

2. Сайт Президії НАН України. – http://www.nas.gov.ua/UA /Pages/default.aspx

3. Валлерстайн И. Конец знакомого мира : Социология XXI века (Пер. с англ. под ред. В.Л. Иноземцева). - М.: Логос, 2003. – С.326.

4. Неурядові аналітичні центри в Україні: стан і тенденції розвитку // Національна безпека і оборона. – 2003. – № 10. – С. 44 – 50.

5. Горовий В.М. Надзвичайний інформаційний стан як засіб протистояння інформаційній агресії //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. 224 – 232.

6. Національний інформаційний комплекс і його роль у глобальному інформаційному просторі / [О. С. Онищенко, В. М. Горовий, В. І. Попик та ін.]; НАН України, Нац. б-ка України ім. В. І. Вернадського. – К.: НБУВ, 2014. – 264 с.

УДК 343.326:316.774:004.738.5

Ірха Ю. Б.

Науково-дослідний інститут інформатики і права Національної академії правових наук України

ЗАСОБИ МАСОВОЇ ІНФОРМАЦІЇ ЯК СУБ'ЄКТИ ПРОТИДІЇ ЕКСТРЕМІЗМУ В УКРАЇНІ

У сучасному житті інформація відіграє надзвичайну важливу роль. Щоденно особа отримує її з різних джерел, зокрема, навколишнього середовища, літератури, баз даних, засобів масової

інформації (далі – ЗМІ), спілкування з іншими людьми. Водночас, з об'єктивних причин не можливо засвоїти відомості про всі події, процеси, факти, явища, які існують або відбуваються у суспільному житті. Крім того, не реально перевірити всю або значну частину інформації на достовірність, неупередженість, повноту і точність.

Зазвичай особа критично оцінює та перевіряє невеликі об'єми отриманої інформації, фактично лише ті, які вона вважає важливими для себе. З одного боку, це природно, адже надмірна перевірка відомостей займає багато часу й ресурсів, відволікає від поставлених цілей та, за певних умов, може дійти до абсурду. Водночас з іншого боку – «інформаційний ідеалізм» використовується багатьма для маніпулювання свідомістю та поведінкою людей заради досягнення, як правило, неправомірних цілей у політиці, економіці, міжнародних відносинах тощо. Знаючи, що більшість довірливо сприймає інформацію, недобросовісні суб'єкти намагаються спотворити її, передати у вигідному для себе руслі.

Побудова демократичної, правової держави не можлива без належного забезпечення та захисту фундаментальних прав і свобод людини і громадянина, зокрема, на свободу думки і слова та на інформацію. Згідно з положеннями Конвенції про захист прав людини і основоположних свобод 1950 року кожен має право на свободу вираження поглядів; це право включає свободу дотримуватися своїх поглядів, одержувати і передавати інформацію та ідеї без втручання органів державної влади і незалежно від кордонів. Здійснення цих прав пов'язане з обов'язками та відповідальністю (стаття 10) [1]. Оскільки свобода інформації не є абсолютною, то суб'єкти інформаційних відносин мають відповідально підходити до вибору відомостей, які вони хочуть поширити. Історії відомі численні випадки, коли певні інформаційні повідомлення призводили до масових порушень громадського порядку, завдавали істотної шкоди правам і свободам людей.

У XX – XXI столітті найбільш ефективним каналом поширення суспільно важливих відомостей стали ЗМІ. Вони володіють значним арсеналом способів і методів подачі інформації у друкованому, аудіо-, відео-, фото-, кіно- та електронному форматі. Для великої кількості громадян ЗМІ стали основним джерелом відомостей соціально-політичного, міжнародного, культурно-

ідеологічного характеру. Так, у процесі опитування громадян Європейського союзу, фахівцями проекту Євробарометр було встановлено, що три з чотирьох європейців дізнаються про стан справ у Європейському союзі через телебачення, 40% – пресу, 31% – радіо, а 29% – Інтернет [2].

В епоху інформаційного суспільства суттєво зросла швидкість передачі даних, які у режимі реального часу можна практично безперешкодно розповсюджувати на будь-які відстані та необмежені аудиторії. Завдяки сучасним технологіям ЗМІ отримали надзвичайні можливості як для інформування громадян, так і для впливу на внутрішню та зовнішню політику держави. ЗМІ стали спроможними впливати на формування та реалізацію політичних рішень, громадської думки, а також на діяльність органів публічної влади, інститутів громадянського суспільства. За твердженнями Д. Дубова, роль сучасних медіа змінилась настільки, що висловів Голови комітету начальників штабів армії США Джона Шалікашвілі «…ми не перемагаємо, поки CNN не скаже, що ми перемагаємо» можна перефразувати таким чином: «…ми можемо програвати або бути розбитими, та якщо CNN скаже, що ми перемагаємо – це означає, що ми перемагаємо» [3, с. 59].

Інформаційний простір будь-якої держави є її стратегічним ресурсом, який треба оберігати і захищати від різних загроз, адже інформація, яка в ньому циркулює, здатна впливати на суспільні процеси, змінюючи їх у кращу чи гіршу сторони. Як одні з головних суб'єктів інформаційних відносин, ЗМІ не можуть бути осторонь проблем забезпечення національної безпеки та її складової – інформаційної безпеки. Безумовно, ЗМІ, виконуючи роль сторожових псів демократії, мають з недовірою ставитися до урядової риторики про національні інтереси і національну безпеку [4, с. 49], водночас, на нашу думку, вони не вправі ігнорувати або не звертати увагу на реальні та потенційні небезпеки, які загрожують життю нації чи здатні істотно вплинути на громадський порядок, суспільну злагоду, здоров'я населення, а також завдати значної шкоди правам і свободам людини і громадянина.

Внаслідок збройної агресії Російської Федерації проти України в нашій державі значно зросла екстремістська активність. Проросійськи налаштовані екстремістські угруповання, у тому числі екстремісти-одинаки намагаються дестабілізувати соціально-політичну обстановку, розпалити або поглибити міжнаціона-

льну та міжконфесійну ворожнечу з метою перешкоджання відновленню суверенітету та територіальної цілісності України. Крім того, зафіксовано непоодинокі випадки діяльності інших екстремістських угруповань, які, використовуючи скрутне фінансово-економічне становище громадян, намагаються дискредитувати органи публічної влади задля здобуття власних політичних чи економічних дивідендів.

Прикметно, що екстремісти, незалежно від поглядів, намагаються широко використовувати можливості ЗМІ та Інтернету для пропаганди своєї діяльності з метою збільшення соціальної бази, залякування опонентів. Очевидно, що така пропаганда є суспільно шкідливою і, як стверджує Г. Цирфа, явно нехтує правами і свободами людини і громадянина та порушує національні й міжнародні норми [5, с. 103].

Так як ЗМІ здійснюють вплив на індивідуальну та групову свідомість, а також забезпечують зворотній зв'язок між громадянами, суспільством і владою, то вони мають бути залучені до системи протидії екстремізму в Україні. Ми вважаємо, що ЗМІ, які цінують свою репутацію та патріотично налаштовані, можуть самостійно або на виконання відповідних державних чи муніципальних замовлень створювати інформаційну продукцію, спрямовану на зменшення рівня соціального напруження, висвітлення справжніх намірів екстремістів, спростування їх ідеологічних основ, засудження використання насильства у соціальних конфліктах. Крім того, вони можуть блокувати розповсюдження відверто деструктивної інформації.

Загалом, ЗМ,І як інститути громадянського суспільства, спроможні консолідувати Український народ, мобілізувати його внутрішні ресурси для протидії екстремістським проявам і збройній агресії. Головне, щоб журналісти, редактори, власники ЗМІ відповідально підходили до своєї роботи та усвідомлювали наслідки, які можуть настати після оприлюдненої ними інформації.

Література

1. Конвенція про захист прав людини і основоположних свобод (офіц. пер.) : Конвенція прийнята Радою Європи 4 листоп. 1950 р., м. Страсбург / [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/995_004.

2. Eurobarometer – 40 years / [Електронний ресурс]. – Режим доступу : http://ec.europa.eu/public_opinion/topics/forty_en.htm.

3. Дубов Д. Засоби масової інформації як якісно нові суб'єкти політичних комунікацій / Д. Дубов // Політичний менеджмент. – 2007. – № 1. – С. 57–65.

4. Слісаренко Ю.І. Національні інтереси, національна безпека України та засоби масової інформації / Ю.І. Слісаренко // Вісник Київського ун-ту ім. Тараса Шевченка : Журналістика. – 1999. – Вип. : 7. – С. 49–52.

5. Цирфа Г.О. Пропаганда як елемент соціалізації особистості та її наслідки // Г.О. Цирфа / Деструктивна пропаганда: шляхи протидії та проблеми відповідальності : Матеріали науково-практичної конференції / 21 травня 2015 р., м. Київ / Упорядн. : Фурашев В.М., Поперечнюк В.М. – К. : ТОВ «ІВА», 2015. – С. 102–104.

УДК 355.40:356.35

Кацалап В. О.
кандидат військових наук
Національний університет оборони України
імені Івана Черняховського

СИСТЕМА СТРАТЕГІЧНИХ КОМУНІКАЦІЙ ЗБРОЙНИХ СИЛ УКРАЇНИ

Складність створення системи стратегічних комунікацій Збройних Сил України обумовлена багатогранністю проявів інформації та інформаційних процесів. Це пов'язано зі змінами в галузі інформаційних технологій та зростанням ролі інформації в сферах, які віднесені до компетенції Міністерства оборони України. Належне виконання функцій і завдань Міністерством оборони України та Збройними Силами України, як основними суб'єктами забезпечення обороноздатності держави, котрі визначені законодавством, без досягнення необхідного стану інформаційної безпеки у воєнній сфері є неможливим. Зазначене питання на сьогодні є вкрай актуальним, адже лише в стані інформаційної безпеки, коли доступні та захищені необхідні інформаційні ресурси, можуть бути реалізовані процеси управління за кожним із визначених завдань, які здійснюються виключно інформаційними методами. Створити такі інформаційні можливості шляхом використання тільки власних ресурсів Міністерство оборони та Збройні Сили України принципово не в змозі. Без залучення потужностей держави сумнівною є можливість виконання у повно-

му обсязі такого завдання, як "інформаційна безпека Збройних Сил України". Тому ця обставина потребує глибокого аналізу умов створення системи стратегічних комунікацій Збройних Сил України в інтересах забезпечення інформаційної безпеки у воєнній сфері та відповідного загальнодержавного управління.

Аналіз ведення інформаційних операцій Російської Федерації [2, 3] проти України дозволяє з упевненістю сказати, що Росія використовує всі елементи системи стратегічних комунікацій проти своїх противників, однак успішні дії їй вдаються не всюди. Там, де завданням є впровадження у свідомість особи чи групи людей певної ідеї, модифікації їх поведінки, результати, досягнуті російськими підрозділами інформаційної операції, не завжди прийнятні для них, а іноді їх можна назвати провальними. Зокрема, загальні підсумки інформаційної війни навколо грузинсько-російського збройного конфлікту за більшістю складових є поразкою Росії. Це не означає, що в певних напрямках дії російських підрозділів інформаційних операцій не можна визнати винятково успішними.

Мета доповіді полягає у визначенні негативних чинників, що впливають на створення системи стратегічних комунікацій Збройних Сил України в умовах ведення інформаційної операції.

Сьогодні провідні країни світу не можуть обійтися без існування системи стратегічних комунікацій, призначенням якої є об'єднання загальних зусиль сектору безпеки та оборони для протидії інформаційним операціям. Першим підрозділом такого виду були частини психологічних операцій (PSYOPS) у Сполучених Штатах Америки. В цій державі підрозділи PSYOPS входять до складу сухопутних і військово-повітряних сил. Невеликі частини планують і виконують обмежені операції у складі ВМФ. На відміну від інших держав, підрозділам та службовцям PSYOPS усіх видів збройних сил заборонено здійснювати операції на території США.

У Німеччині для аналогічних потреб створено Центр оперативної інформації (Zentrum Operative Information), якому підпорядковано Батальйон оперативної інформації 950. Батальйон і центр підпорядковані новоствореному Командуванню Об'єднаної Служби Підтримки (Streitkraftebasis). Загалом, у цих підрозділах близько тисячі службовців. Німецькі фахівці інформаційної війни керують операціями НАТО в Афганістані та Косові.

У Британських ЗС цими питаннями займається П'ятнадцята Група Психологічних Операцій [3].

У Російській Федерації за інформаційну діяльність відповідає безпосередньо Адміністрація президента, на яку підпорядковуються підрозділи: Федеральна служба безпеки та Медіа Холдінг, завданням яких є інформаційна діяльність на території колишніх республік Радянського Союзу, зокрема й України. Для впливу на соціальні мережі через Інтернет створено два інформаційних центри: Ольгіно та Сколково. Загальна мета зазначених інформаційних центрів полягає у створенні в Україні плацдарму для впливу на українську політику шляхом просування відповідних політиків.

Причиною того, що росіяни програли у 2014 році виборчу кампанію на посаду Президента України, та й не змогли досягнути моральної капітуляції українців у "газовій" війні, пояснюється дією в інформаційному протиборстві інших чинників. Інформаційна операція росіян в українському інформаційному полі не була пристосована до українського середовища. Тому ефективність використання російських інформаційних розробок була низькою.

Інформаційний вплив в інтенсивному режимі сьогодні є суттєвою частиною професійної роботи низки відомств, серед яких МЗС, МВС, СБУ, МОУ, Держтелерадіо.

Таким чином, існує нагальна потреба запровадження системи стратегічних комунікацій Збройних Сил України, як механізму управління процесом забезпечення інформаційної безпеки України у воєнній сфері. Цей процес є складним і багатогранним, оскільки він може включати цільові програми, проекти та окремі дії (заходи, роботи), які спрямовані на реалізацію певного порядку забезпечення інформаційної безпеки держави у воєнній сфері. Виконавцями цього процесу повинні бути як профільні структури у складі Міністерства оборони України та Збройних Сил України, так і інших суб'єктів Сектору безпеки і оборони держави, а також задіяні підприємства і установи України, що не відносяться до названих суб'єктів.

Література

1. Шевченко О. Інформаційно-психологічні операції: концептуальні підходи НАТО і провідних країн світу // Соціальна психологія. – 2004. – № 2 (4). – С. 111-121.

2. Почепцов Г. Г. Информационные войны. Основы военно-коммуникативных исследований. К.: Вид. "АДЕФ-Украина", 1998. – С. 34.

3. Панарин И. Н. Информационная война и Россия. – М. 2000. – С. 112.

УДК 351.746:007

Копан О. В.
доктор юридичних наук, професор
Національна академія внутрішніх справ
Мельник В. І.
Відкритий міжнародний університет розвитку людини Україна

ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНА ВІЙНА ЯК ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ УКРАЇНИ

Процеси глобалізації, що мають місце в українському суспільстві, невід'ємно пов'язані з удосконаленням інформаційних технологій, що, своєю чергою, призводить до появи нових джерел небезпеки. Очевидно, що від належного функціонування глобальних комп'ютерних мереж залежить економіка та обороноздатність нашої країни. Отже, збої в їх роботі можуть мати досить серйозні наслідки.

Сьогодні Україна перебуває на межі системних перетворень у сфері забезпечення національної безпеки, зокрема й інформаційної. Відповідно до Закону України «Про основи національної безпеки України» система забезпечення інформаційної безпеки є складовою частиною національної безпеки держави та однією з найважливіших її функцій. В тому числі й забезпечення інформаційного суверенітету України [1].

На жаль, нині в Україні має місце інформаційне протистояння, яке чинить деструктивний дестабілізуючий вплив на національну безпеку і вже переросло в інформаційну війну. Та широкомасштабна діяльність Російської Федерації проти України, що наразі ведеться в інформаційному просторі (інформаційна війна), має за мету підрив політичної, економічної, соціальної та оборонної систем нашої держави, психологічну обробку населення, дестабілізуючий вплив на суспільство, поширення інформації, що розпалює міжнаціональну ворожнечу, підбурює до ненависті, дискримінації чи насильства.

Інформаційно-психологічна війна – це сукупність різноманітних форм, методів і засобів впливу на людей з метою зміни у бажаному напрямку їх психологічних характеристик (поглядів, думок, ціннісних орієнтацій, настроїв, мотивів, установок, стереотипів поведінки), а також групових норм, масових настроїв і громадської свідомості в цілому [2, с. 250].

Можемо стверджувати, що саме у високій уразливості глобальних мереж до несанкціонованих сторонніх втручань криється особлива небезпека. До речі, такі втручання з метою досягнення своїх геополітичних інтересів можуть здійснювати іноземні держави, а також організовані злочинні угруповання, що прагнуть реалізувати свої кримінальні інтереси, і навіть звичайні користувачі.

Так, глобальні інформаційні потоки, поширюючись у внутрішньому інформаційному просторі держави, впливають на мислення людей, їх певні переконання, як наслідок, є своєрідним закликом до вчинення масових дій, які можуть мати не лише конструктивний характер, а й деструктивний. Доволі часто в глобальному інформаційному просторі застосовуються засоби психологічного впливу, атаки на духовні цінності та культуру населення. Зауважимо, власне мистецтво ведення інформаційної боротьби та вміння виокремити її основні об'єкти є прерогативами у досягненні переваг у протистоянні між державами, утриманні своєї стратегічної ініціативи та реалізації амбітних інтересів.

Загальновідомо, що стійка ідейна переконаність населення, вплив на психологічний стан і поведінку людей здебільшого забезпечуються шляхом використання інформаційної інфраструктури та медійного простору, деструктивний вплив на які має руйнівні наслідки на формування національної свідомості. Отже, саме завдяки впливу на морально-психологічний стан суспільства і досягається перемога в інформаційно-мережевих війнах.

Інформаційно-психологічна зброя як основний інструмент ведення інформаційно-психологічних війн використовується при проведенні інформаційно-психологічних заходів та операцій і може спрямовуватися на придушення, знищення, дезорганізацію, дезорієнтацію, дезінформацію, дезадаптацію об'єкта впливу; вона може порушувати психічне здоров'я, спонукати до спонтанних, немотивованих, агресивних (чи антисоціальних) дій, спричиняти тимчасові чи незворотні зміни в свідомості особистості, а то й повне її самознищення [3, с. 144].

Можемо констатувати, що перевага в таких війнах надається нелетальним засобам війни, здатним шляхом використання новітніх досягнень психології та механізмів управління їх мотиваціями чинити вплив на великі групи людей, при цьому не завдаючи шкоди життю населення та не руйнуючи об'єкти інфраструктури. Отже, здійснюється скореговане, тактично прораховане маніпулю-

вання інформаційними потоками в інформаційному просторі, що призводить до руйнування традиційних цінностей у суспільстві.

Крім того, на нашу думку, основними реальними і потенційними загрозами є поширення кіберзлочинності в інформаційній сфері та невідповідність національного законодавства сучасним викликам і загрозам інформаційній безпеці України. Вважаємо, що одним із основних напрямів діяльності нашої держави у сфері забезпечення інформаційної безпеки має стати своєчасне виявлення, запобігання і припинення злочинів у інформаційній сфері.

З огляду на зазначене вище, вбачається за необхідне вироблення системного, наступального підходу до питань протидії та нейтралізації результатів дестабілізуючої діяльності в інформаційній сфері.

Той факт, що інформаційна агресія здійснюється приховано, значно ускладнює не лише протидію її проявам на належному рівні, а й виявлення інформаційно-психологічних впливів і суб'єктів їх здійснення. Таким чином, можна зробити висновок, що сучасна інформаційно-психологічна війна наразі перетворюється в основну форму протиборства між державами, для ведення якого використовуються різноманітні технології, мета яких – деструктивний вплив на духовно-ідеологічну сферу життя суспільства. Своєю чергою, дезінформація і відверта брехня є класичними елементами інформаційно-психологічного протистояння.

Підсумовуючи, зауважимо, що відмінною рисою сьогодення є інформаційно-психологічна війна, яка торкається і зовнішньополітичної, і внутрішньополітичної сфери. Очевидно, що несвоєчасне розпізнавання замаскованих деструктивних впливів у інформаційному просторі та відсутність відповідних навиків для протистояння і нейтралізації інформаційної агресії в об'єктів інформаційно-психологічної обробки в майбутньому можуть стати причиною небажаної поразки. Отже, країни, котрі матимуть гармонійно розвинуте та надійно захищене інформаційне суспільство матимуть більші шанси на успіх у відстоюванні своїх позицій в інформаційному просторі.

Література

1. Про основи національної безпеки України : Закон України від 19.06.2003 № 964-IV [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/964-15.

2. Манойло А. В. Государственная информационная политика в особых условиях : монография / А. В. Манойло. – М. : МИФИ, 2003. – 388 с.

3. Воробйова І. В. Інформаційно-психологічна зброя як самостійний засіб ведення інформаційно-психологічної війни // І. В. Воробйова // Системи озброєння і військова техніка. – 2010. – № 1(21). – С. 141–144.

УДК 681.3+519.83

Крайнов В. О.
кандидат технічних наук, доцент
Національний університет оборони
України імені Івана Черняховського

ПЕРСПЕКТИВНІ НАПРЯМИ УДОСКОНАЛЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА ОРГАНІВ УПРАВЛІННЯ ВІЙСЬКАМИ

Розвиток світової спільноти наочно демонструє, що останнім часом критично важливим державним ресурсом, що робить найбільший вплив на національну безпеку, стає інформація, циркулююча в автоматизованих системах управління і зв’язку. Дані системи є невід’ємним компонентом структури управління державою, економікою, фінансами і обороною. Прискорений розвиток комп’ютерних технологій не тільки значною мірою сприяв підвищенню ефективності їх функціонування, але і відкрив додаткові можливості для навмисної деструктивної дії на них протилежної сторони.

У основу концепції інформаційного протиборства закладена спільна залежність (уразливість) держави та їх потенційних супротивників від інформації і інформаційних систем. У зв’язку з цим при її реалізації розглядаються два аспекти діяльності – дія на інформаційну інфраструктуру супротивника і захист свого власного інформаційного середовища.

Підготовка і проведення інформаційних операцій пов’язані з узгодженням і дозволом на рівні національного військово-політичного керівництва країни комплексу питань законодавчого і політичного характеру. Інформаційні операції проводяться на всіх рівнях військових дій, межі між якими часто носять умовний характер.

На стратегічному рівні такі операції проводяться за рішенням військово-політичного керівництва країни і покликані забезпечити досягнення національних стратегічних цілей. В ході їх здійснюється дія на всі елементи державного устрою потенційних супротивників (політичні, військові, економічні і інформаційні) при одночасному захисті своїх державних структур. Для досягнення цілей інформаційні операції на цьому рівні повинні забезпечувати високий ступінь координації між військовими органами і урядовими установами і відомствами, а також союзниками і партнерами по коаліції.

На оперативному рівні інформаційні операції (ІО) проводяться для забезпечення успішного ходу операції або кампанії в цілому або рішення головних задач операції. Їх мета – дія на лінії зв'язку, системи тилового забезпечення і бойового управління озброєнням сил противника при одночасному захисті аналогічних систем, як своїх ЗС, так і союзників. ІО, що проводяться на цьому рівні, можуть сприяти досягненню стратегічних цілей.

ІО на тактичному рівні проводяться з метою забезпечення рішення тактичних задач. Вони зосереджені на дії на інформацію та інформаційні системи, такі, як системи зв'язку, бойового управління, розвідки і інші, що безпосередньо забезпечують ведення бойових дій з'єднань і частин противника, при одночасному захисті своїх систем, та союзників.

Відповідно всі ІО підрозділяються на наступальні і оборонні.

Наступальні ІО є комплексним проведенням по єдиному задуму і плану заходів щодо оперативного маскування, радіоелектронної боротьби, програмно-математичної дії на інформаційно-управляючи системи (ІУС), фізичному знищенню (виведення з ладу) об'єктів інформаційної інфраструктури, а також психологічних і спеціальних ІО. В ході таких операцій вживаються заходи, що надають дію на свідомість людей і направлені на зрив процесу ухвалення рішень, а також дії з метою порушення роботи або знищення елементів інформаційної інфраструктури. Новим елементом наступальних інформаційних операцій порівняно з концепцією боротьби з системами управління є спеціальні ІО та заходи щодо програмно-математичної дії на комп'ютерні мережі супротивника.

Оборонні ІО є взаємозв'язаними процесами по захисту інформаційного середовища, розкриттю ознак нападу, відновленню

боєздатності і організації у відповідь дій на агресію (напад). Їх основними елементами є: забезпечення фізичної безпеки інформаційної інфраструктури, безпеки інформації і скритності дій військ (сил); розкриття заходів щодо оперативного маскування супротивника; контрпропаганда; контррозвідка; радіоелектронний захист і спеціальні інформаційні дії.

Оборонні ІО повинні забезпечувати своєчасність і точність передачі даних, гарантований доступ до них користувачів в умовах інформаційної дії противника. В ході їх передбачається проведення заходів щодо відновлення боєздатності інформаційних систем.

Наступальні і оборонні ІО можуть проводитися по єдиному задуму і плану і взаємно доповнювати один одного. Вони орієнтовані на одні і ті ж об'єкти дії, якими можуть виступити:

- органи управління держави та збройних сил;
- ІУС цивільної інфраструктури (телекомунікаційні, включаючи засоби масової інформації, транспортні, енергетичного комплексу, фінансового і промислового секторів);
- управляючі елементи військової інфраструктури (системи зв'язку, розвідки, бойового управління, тилового забезпечення, управління зброєю);
- лінії, канали зв'язку і передачі даних;
- інформація, що циркулює або зберігається в системах управління;
- суспільство в цілому (як цивільне населення, так і особовий склад збройних сил), його державні, економічні і соціальні інститути;
- керівний склад і персонал автоматизованих систем управління, що бере участь в процесі ухвалення рішень.

В період проведення миротворчих операцій об'єктами дії можуть бути також воєнізовані, партизанські і політичні організації, релігійні і соціальні групи, окремі особи, які відкрито чи таємно виступають проти збройних сил і перешкоджають виконанню завдань.

За оцінкою американських експертів, ефект цільової інформаційної дії на противника можна порівняти із застосуванням ЗМУ і загроза піддатися такій дії може стати важливим чинником при впливі на потенційного агресора. На їх думку, ефективність цієї загрози прямо пропорційна рівню технологічного розвитку і масштабам використання комп'ютерної техніки в системах управління державою.

Будучи по своєму характеру комплексним процесом, інформаційна операція є інтегрованим, узгодженим за часом використання різних засобів і методів, орієнтованих на досягнення певної загальної мети.

Програмно-математична дія на комп'ютерні мережі (комп'ютерна атака) визначається як дії із застосуванням апаратно-програмних засобів, направлених на використання, спотворення, підміну або знищення інформації, що міститься в базах даних комп'ютерів і інформаційних мереж.

Тому, на підставі викладеного, можна сказати, що питання безпеки інформації – важлива частина концепції впровадження нових інформаційних технологій в військову справу. "Той, хто володіє достовірною і повною інформацією, – той володіє ситуацією, а той, хто володіє ситуацією, – той здатен управляти нею у своїх інтересах, а той, хто здатен управляти, – той здатен перемагати". Тому захист інформації у системах управління військами на теперішній час є дуже актуальною проблемою, яка потребує свого вирішення.

Література

1. Домарев В. В. Защита информации и безопасность компьютерных систем. –К.: Диасофт, 1999, – 325с.

2. Медведовский И. Д., Семьянов П. В., Леонов Д. Г. Атака на Internet. –М: ДМК, 2000, –220 с.

3. Перспективи застосування інформаційних технологій в збройній боротьбі. Аналітичний матеріал кафедри інформатизації штабів. НАОУ. – Київ: 2003, –20 с.

УДК 341.824:338.47 (043.2)

Кудрявцев Г. В.
Національна академія СБ України
Управління правового забезпечення СБ України

ОКРЕМІ ПИТАННЯ ДІЯЛЬНОСТІ ВІЙСЬКОВО-ЦИВІЛЬНИХ АДМІНІСТРАЦІЙ

4 лютого 2016 року Верховною Радою України було прийнято Закон України "Про внесення змін до деяких законів України щодо діяльності військово-цивільних адміністрацій", яким було

внесено зміни до законів України “Про місцеве самоврядування в Україні”, “Про місцеві державні адміністрації” та “Про військово-цивільні адміністрації”.

Зміни до частини дев’ятої статті 3 та частини другої статті 6 Закону України “Про військово-цивільні адміністрації” передбачають, що у разі якщо відповідні обласні військово-цивільні адміністрації не утворені, керівник Антитерористичного центру при Службі безпеки України наділятиметься повноваженнями зокрема щодо:

- загального керівництва діяльністю військово-цивільних адміністрацій населених пунктів, районних військово-цивільних адміністрацій;

- призначення на посаду та звільнення з посади керівників військово-цивільних адміністрацій населеного пункту (населених пунктів) [1].

Ще до внесення відповідних змін передбачалося, що загальне керівництво діяльністю військово-цивільних адміністрацій населених пунктів, районних військово-цивільних адміністрацій здійснюють керівники відповідних обласних військово-цивільних адміністрацій. Закон спочатку не визначав хто буде здійснювати функцію загального керівництва діяльністю військово-цивільних адміністрацій населених пунктів та районних військово-цивільних адміністрацій, якщо відповідні обласні військово-цивільні адміністрації не будуть утворені. До внесення змін приписи частини дев’ятої статті 3 Закону України “Про військово-цивільні адміністрації” передбачали, що керівник Антитерористичного центру при СБУ здійснює керівництво діяльністю лише обласних військово-цивільних адміністрацій у сфері забезпечення громадського порядку та безпеки [2].

На нашу думку, покладення на Антитерористичний центр при СБУ повноважень щодо управління всією діяльністю військово-цивільних адміністрацій не відповідає його завданням, визначеним спеціальним законодавчим актом у сфері боротьби з тероризмом – Законом України “Про боротьбу з тероризмом”, адже цей нормативно-правовий акт визначає Службу безпеки України як головний орган у загальнодержавній системі боротьби з терористичною діяльністю та вказує, що координацію діяльності суб'єктів, які залучаються до боротьби з тероризмом, здійснює Антитерористичний центр при СБУ (абзац четвертий статті 4) [3].

До того ж, Положенням про Антитерористичний центр та його координаційні групи при регіональних органах Служби безпеки України (затверджене Указом Президента України від 14.04.99 № 379) наділення керівника Антитерористичного центру при Службі безпеки України повноваженнями здійснювати загальне керівництво обласними військово-цивільними адміністраціями (далі – ВЦА) не передбачено.

Подібну позицію Головне науково-експертне управління Верховної Ради України висловлювало ще 27.01.2015 року до законопроекту № 1855, який пізніше було прийнято в цілому як Закон України "Про військово-цивільні адміністрації".

Законодавство визначає сферу повноважень СБУ, як спеціалізованого органу, який здійснює захист державного суверенітету, конституційного ладу, територіальної цілісності, економічного, науково-технічного і оборонного потенціалу України, законних інтересів держави та прав громадян від розвідувально-підривної діяльності іноземних спеціальних служб, посягань з боку окремих організацій, груп та осіб, а також забезпечення охорони державної таємниці (ст. 1 Закону України «Про Службу безпеки України»)[4]. Діяльність Антитерористичного центру, як постійно діючого органу при Службі безпеки України, спрямована безпосередньо на здійснення координації діяльності суб'єктів боротьби з тероризмом у запобіганні терористичним актам щодо державних діячів, критичних об'єктів життєзабезпечення населення, об'єктів підвищеної небезпеки, актам, що загрожують життю і здоров'ю значної кількості людей та не стосується управління комунальним господарством, соціального забезпечення населення населеного пункту, району тощо [5].

Ідея покладання на Антитерористичний центр при СБУ повноважень органів влади загальної компетенції (місцевих державних адміністрацій та органів місцевого самоврядування) по суті означає надання спеціалізованому правоохоронному органу абсолютно невластивих йому функцій, для виконання яких цей орган не пристосований за своєю структурою, особовим складом, характером професійної підготовки його службовців.

Загалом, логіка побудови правової системи України, імперативні приписи Конституції України, принцип верховенства права передбачають можливість наділення структурних підрозділів тих чи інших органів лише тими повноваженнями, які охоплюються

сферою компетенції та завданнями відповідних органів. У зв'язку з цим у структурі Антитерористичного центру при СБУ можуть створюватися підрозділи лише для виконання завдань, що на нього покладені. А той факт, що військово-цивільні адміністрації, які по суті наділені повноваженнями органів місцевого самоврядування, діють у складі Антитерористичного центру при СБУ, може призвести в майбутньому до неналежного виконання завдань з протидії терористичним загрозам та спричинить появу нових колізій у законодавстві.

Література

1. Закон України «Про внесення змін до деяких законів України щодо діяльності військово-цивільних адміністрацій» від 04.02.2016 №995-VIII [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/995-19

2. Закон України «Про військово-цивільні адміністрації» від 03.02.2015 №141-VIII [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/141-19

3. Закон України «Про боротьбу з тероризмом» від 20.03.2003 № 638-IV [Електронний ресурс]. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/638-15

4. Закон України «Про Службу безпеки України» від 25.03.1992 №2229-XII [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/2229-12

5. Положення про Антитерористичний центр та його координаційні групи при регіональних органах Служби безпеки України : Указ Президента України від 14.04.1999 №379/99 [Електронний ресурс]. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/379/99

УДК 005.3

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

ОБМЕЖЕННЯ ІНФОРМАЦІЙНИХ ПРАВ ГРОМАДЯН У ЗВ'ЯЗКУ З ВИКОНАННЯМ ФУНКЦІЙ ДЕРЖАВИ

У попередніх дослідженнях обґрунтовано, що під інформаційними правами варто розуміти гарантовані державою можливості людини задовольняти її потреби в отриманні, використанні,

поширенні, охороні і захисті необхідного для життєдіяльності обсягу інформації [1].

Основою інформаційних прав людини визначено право на інформацію, яке включає право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб — на свій вибір. Ключовою складовою права на інформацію є право людини на доступ (отримання) інформації, а свободу вираження поглядів і переконань, свободу обміну інформацією [2, ст. 2] включено до обсягу поняття «право на інформацію».

Революція гідності відкрила перед Україною можливості для побудови нової системи відносин між громадянином, суспільством і державою на основі цінностей свободи і демократії. Однак окупація Росією частини території України – Автономної Республіки Крим, розв'язання воєнної агресії на Сході України, ставить перед Україною додаткові завдання, зокрема в питаннях забезпечення інформаційної безпеки: протидію інформаційним операціям проти України, маніпуляціям суспільною свідомістю і поширенню спотвореної інформації, створення і розвиток інститутів, що відповідають за інформаційно-психологічну безпеку [3, п. 4.11.].

У таких умовах нормативно-правове регулювання реалізації інформаційних прав громадян тісно пов’язане із закріпленням права людини на. інформаційну безпеку, зокрема в частині захищеності людини від неповноти,, невчасності та невірогідності інформації, що використовується, від негативних інформаційних впливів. Тому першочергового значення набуває питання «реагування» держави на поширення недостовірної інформації з метою забезпечення інформаційної безпеки як людини, так і держави. Адже Конституція України передбачає, що забезпечення інформаційної безпеки — це одна із найважливіших функцій держави, справа всього народу [4, ст. 17], а інформаційна безпека класично визначалася як «стан захищеності життєво важливих інтересів людини, суспільства, держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації» [5, п. 13, розділ ІІІ].

У цьому напрямі держава змінює правове регулювання суспільних відносин, пов'язаних із безпосереднім виконанням оборонних функцій громадянами України. Так, наприклад, «порядок зберігання і користування особистими фотоапаратами, магнітофонами, радіоприймачами, мобільними телефонами, іншими засобами мобільного зв'язку та передачі інформації, комп'ютерною та іншою побутовою радіоелектронною технікою для військовослужбовців, які виконують обов'язки військової служби, встановлюється командиром військової частини» [6, ст. 143]. Така норма, хоча формально й обмежує інформаційні права військовослужбовців, однак спрямована на забезпечення їх безпеки під час бойових дій у процесі захисту територіальної цілісності України.

Практичного значення набуває питання діяльності журналістів телерадіокомпаній, друкованих та Інтернет ЗМІ. Формально вони безпосередньо не виконують інформаційної функції держави, пов'язаної із організацією системи одержання, використання, поширення і збереження інформації, однак журналісти і ЗМІ є важливою складовою забезпечення відповідної функції.

Непоодинокі факти дискредитації органів державної влади України, розкриття інформації з обмеженим доступом або «чутливої» (за категоріями НАТО) відкритої інформації про розташування, склад, плани, військове оснащення українських Збройних Сил тощо зумовлюють актуалізацію проблеми упорядкування діяльності ЗМІ в особливий період та в умовах воєнного часу.

Доцільно започаткувати громадське обговорення питання внесення змін до законодавства про друковані засоби масової інформації (пресу) в Україні та телерадіомовлення у частині закріплення норм про попереднє погодження повідомлень і матеріалів, які поширюються ЗМІ і є «чутливими» для національної безпеки, у особливий період та в умовах воєнного часу.

Безумовно, мова не має йти про створення аналогічного тоталітарному Головліту органу. Найоптимальнішим рішенням має бути поєднання зусиль держави, громадськості і ЗМІ у напрямку встановлення дієвих механізмів протидії інформаційної агресії, а саме: інформаційним операціям проти України, маніпуляціям суспільною свідомістю і поширенню спотвореної інформації, розвитку інститутів, що відповідають за інформаційно-психологічну безпеку громадян.

Література

1. Марущак А. І. Визначення поняття «інформаційні права людини» / А. І. Марущак // Інформація і право. — 2011. — № 2. — С. 21-26.
2. Закон України від 01.07.2015 р. «Про внесення зміни до статті 143 Статуту внутрішньої служби Збройних Сил України» // Відомості Верховної Ради України. – 2015. – № 33. – Ст. 326.
3. Указ Президента України від 26.05.2015 р. № 287/2015 «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» // Офіційний вісник України. – 2015. – № 43. – Ст. 1353.
4. Конституція України від 28 червня 1996 року // Відомості Верховної Ради України. — 1996. — № 30. — Ст. 141.
5. Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки, затверджені Законом України від 9 січня 2007 року // Відомості Верховної Ради України. — 2007. — № 12. — Ст. 102.
6. Закон України від 01.07.2015 р. «Про внесення зміни до статті 143 Статуту внутрішньої служби Збройних Сил України» // Відомості Верховної Ради України. – 2015. – № 33. – Ст. 326.

УДК 32.019.5: 316.422

Лашкет С. В.
Національна академія СБ України
Матяш О. І.
кандидат технічних наук, старший науковий співробітник
Національна академія СБ України

ГРОМАДСЬКА ДУМКА – ІНФОРМАЦІЙНИЙ КРИТЕРІЙ ЕФЕКТИВНОСТІ РЕФОРМ В УКРАЇНІ

На тлі загострення соціально-економічної та політичної ситуації спостерігається стійка тенденція до зростання занепокоєння населення станом реформ в Україні, посилюється недовіра громадян до органів державної влади та управління, зокрема щодо спроможності виведення країни з кризи, оскільки громадянське суспільство передусім цікавлять кінцеві результати реформ.

Оцінка будь-яких процесів передбачає встановлення відповідних критеріїв, під якими розуміється найвищий, практично досягнутий показник того чи іншого роду діяльності, який є мірилом її оцінки й подальшого поліпшення.

Однак для оцінки діяльності державних інституцій суспільство має бути проінформоване, якими методами, засобами, способами набуті перелічені досягнення. Якщо вони були протиправними, антигуманними, тоді кінцевий результат, незалежно від його значущості, не може бути позитивним. За таких умов актуалізується потреба у дослідженні особливостей громадського контролю за діяльністю державних гілок влади, а також громадської думки як одного із критеріїв оцінки ефективності їх роботи.

Серед законодавців, представників владних і правоохоронних структур, науковців та громадськості відсутня єдина думка стосовно того, якою має бути загальна система критеріїв оцінки реформ в Україні. Зважаючи на це, та спираючись на результати досліджень вітчизняних і зарубіжних учених, а також власні наукові доробки спробуємо розширити спектр наукових поглядів на громадський контроль за діяльністю органів державної влади та громадську думку як один із інформаційних критеріїв оцінки ефективності їх роботи.

Соціологічні дослідження громадської думки в Україні відбуваються з різних напрямків та показують падіння рівня громадської довіри до всіх органів влади та інших соціальних інституцій [1].

Громадська думка – складне соціальне явище. Вона є складовою частиною суспільної свідомості, що відображається у міркуваннях і вчинках людей з приводу соціально значимих фактів суспільного життя. Як масова, колективна думка, вона свідчить про те, що певна кількість осіб виказала однакове міркування щодо одного й того ж актуального факту суспільного життя чи приєдналася до думки, яка вже склалася з цього приводу [2].

Носіями, суб’єктами громадської думки є суспільство в цілому та різні соціальні спільноти, групи, колективи. Будь-яка соціальна спільнота складається з окремих індивідів, тому і громадська думка не може сформуватися інакше, як на підставі сукупності індивідуальних думок.

На практиці розрізняють активний і пасивний підходи до виявлення громадської думки. Активний зводиться до з’ясування суб’єктами громадської думки за власною ініціативою. Суб’єкт самостійно визначає мету і завдання вивчення громадської думки, використовуючи при цьому такі форми, як анкетування, опитування і т.п. Одне з провідних місць при використанні активного

методу належить інститутам прямого народовладдя – загальнодержавним референдумам, регіональним обговоренням, зборам (сходам) за місцем проживання, роботи тощо.

Суть пасивного підходу полягає у тому, що суб'єкт отримує уявлення про суспільні реакції й оцінки в міру надходження до нього відповідної інформації. Ініціатива у застосуванні такого підходу належить різним соціальним спільнотам і окремим громадянам, які безпосередньо беруть участь в управлінні справами держави і суспільства, голосують на виборах, заслуховують звіти посадових осіб, звертаються до державних органів з пропозиціями, заявами, скаргами, дискутують на сторінках преси тощо. Громадяни, у такий спосіб виражаючи певну суспільну думку, впливають на державі інституції. В контексті викладеного принципового значення набуває гарантоване ст. 34 Конституції України право на свободу думки і слова, а також на вільне вираження громадянами своїх поглядів і переконань.

Відзначимо, що в Україні люди сміливо висловлюються з гострих і злободенних проблем діяльності виконавчої, законодавчої та судової влади, результати опитувань публікуються і транслюються засобами масової інформації, політичні партії активно виступають в ролі виразників думок соціальних шарів, помітний вплив партійних парламентських фракцій на прийняття законодавчих рішень тощо. Можливість гласного, публічного висловлювання населення щодо злободенних проблем суспільного життя і вплив оприлюдненої позиції на розвиток суспільно-політичних відносин відображає суть громадської думки як соціального інституту.

Для оптимального формування і функціонування громадської думки необхідні відповідні умови, до яких належить можливість отримання інформації, що відповідає основним вимогам до неї (об'єктивність, повнота, систематизованість, комплексність, оптимальність, оперативність), змога обмінюватися думками всередині цієї спільноти в цілому і значущих її груп, право й реальна можливість публічно висловлювати весь діапазон думок з даної проблеми.

Формування громадської думки проходить три етапи. Першим етапом становлення громадської думки є отримання певною аудиторією необхідної інформації про події, факти тощо. Другий етап – осмислення отриманої інформації, яка здебільшого є інди-

відуальною. На третьому етапі відбувається обговорення різних індивідуальних позицій і точок зору з метою прийняття якогось рішення та виявлення з приводу цього загальної думки.

Найбільш вагомий чинник формування громадської думки – безпосередній власний досвід людей набутий під час зіткнення з повсякденними ситуаціями, на перший погляд, суто особистими, але які насправді є відображенням проблем спільноти, всього соціуму в цілому. Цей процес ґрунтується на життєвому досвіді, він не є заздалегідь програмованим згори та здебільшого не спрямований суб'єктами, зацікавленими у його кінцевому результаті. Отже, сьогодні громадська думка щодо діяльності органів державної влади та управління складається здебільшого з власного досвіду людей, які з тих чи інших причин вступали в контакт з їх співробітниками.

Серед інших чинників важливе місце посідає суспільна ситуація, під якою розуміється сукупність взаємодіючих соціально-економічних, політичних, духовних, ідеологічних і соціально-психологічних умов життєдіяльності людей. Суспільна ситуація – це ті реалії повсякденної життєдіяльності людей, факти, явища і процеси, в умовах яких реалізуються їхні потреби та інтереси. Відображаючи й усвідомлюючи певну суспільну ситуацію, люди мимоволі співвідносять конкретні життєві реалії з тими можливостями, які вони мають для реалізації власних потреб та інтересів. У результаті цього виникає широкий спектр індивідуальних, групових, колективних уявлень, поглядів, оціночних суджень, з яких потім і викристалізовується громадська думка щодо актуальних проблем економічного, соціально-політичного або духовно-ідеологічного життя в умовах конкретної суспільної ситуації [2].

Громадська думка як інститут громадянського суспільства нині формується переважно за допомогою засобів масової інформації, котрі висвітлюють ситуацію в країні, регіоні або місті. І від того, як своєчасно, правдиво та об'єктивно інформується населення, здійснюється роз'яснювальна робота, залежить, наскільки надійним, об'єктивним і безпечним буде інформаційне середовище, а громадська думка захищена від різних маніпуляцій.

Узагальнюючи викладене, зазначимо, що активізація формування засад громадянського суспільства сприятиме його впливу на якість реформ в Україні, посиленню його нагляду та конт-

ролю за діяльністю усіх гілок державної влади. Тому пріоритети їх діяльності мають визначатися не лише державою, а в першу чергу громадськістю, оскільки динамічний розвиток сучасної соціально-політичної ситуації вимагає узгодження інтересів суспільства та державних інституцій.

Найважливішим напрямом підвищення якості роботи усіх владних структур у будь-якій державі вважається їх орієнтація на задоволення потреб громадян. Певно, й у вітчизняній практиці особливу увагу варто приділити проблемі громадської думки щодо їх діяльності. Потрібен перегляд самої концепції врахування громадської думки в механізмі державної влади та управління. Вважаємо, що поряд з оцінюванням поглядів населення на діяльність цих інституцій, необхідне чітке визначення того, що очікує людей від їх діяльності, які проблеми у сфері охорони прав, свобод та законних інтересів громадян, на думку населення, вони мусять вирішувати.

Література

1. Черненко Т. Громадська думка як чинник ефективності діяльності правоохоронних органів в Україні. Аналітична записка / Т. Черненко [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/articles/468/.

2. Мурашин О. Г. Громадська думка як інститут громадянського суспільства / О. Г. Мурашин [Електронний ресурс]. – Режим доступу: http://naiau.kiev.ua/tslc/pages/biblio/visnik/nomer3/murash.html.

УДК 005.3

Петров В. В.
кандидат політичних наук
РНБО України

ДО АСПЕКТІВ СТАНОВЛЕННЯ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ У СФЕРІ ДЕРЖАВНИХ ОРГАНІВ

Інформаційна складова є одним із ключових елементів під час ведення гібридної війни Російською Федерацією проти України. Зазначене обумовлює необхідність вдосконалення підходів до формування та реалізації державної інформаційної політики.

Саме тому гостро постає питання побудови цілісної системи скоординованої взаємодії органів влади, зокрема у проведенні інформаційних та психологічних операцій, удосконалення комплексу заходів протидії та наповнення українського та всесвітнього медіапростору якісним інформаційним продуктом. Система стратегічних комунікацій являє собою дієвий механізм реалізації окреслених вище завдань.

Довідково: стратегічні комунікації, за термінологією НАТО, – скоординоване і належне використання комунікативних можливостей на всіх рівнях державної політики – публічної дипломатії, зв'язків із громадськістю, військових зв'язків, інформаційних та психологічних операцій, заходів, спрямованих на просування цілей держави.

Першочерговим кроком до розбудови Партнерства у сфері стратегічних комунікацій став офіційний запит Апарату Ради національної безпеки і оборони України до Департаменту громадської дипломатії НАТО з пропозицією підтримати українське керівництво у галузі стратегічних комунікацій.

За результатами переговорів щодо започаткування програми Партнерства у сфері стратегічних комунікацій, в якій на Апарат Ради національної безпеки і оборони України покладені обов'язки координаційного центру та головного партнера з української сторони, Секретар РНБО України Олександр Турчинов разом з Генеральним Секретарем НАТО Єнсом Столтенбергом 22 вересня 2015 року у м. Києві підписали Дорожню карту Партнерства зі стратегічних комунікацій між Радою національної безпеки і оборони України та Міжнародним секретаріатом НАТО.

Партнерство у сфері стратегічних комунікацій спрямоване на розвиток спроможностей українських органів влади у галузі стратегічних комунікацій. Саме тому за результатами підписання Дорожньої карти Партнерства Апаратом РНБО України був розроблений та затверджений Секретарем РНБО України чіткий алгоритм дій - План заходів з реалізації Дорожньої карти Партнерства у сфері стратегічних комунікацій.

Реалізація зазначеного плану розпочалася із проведення аудиту та функціонального аналізу наявних ресурсів – роботи підрозділів державних органів, відповідальних за спеціальні інформаційні, інформаційно-психологічні операції, операції сприяння, публічну дипломатію та сферу зв'язків з громадськістю.

Результатом такого дослідження стали пропозиції щодо організаційного, методичного та практичного вдосконалення згаданих вище сфер.

Враховуючи той факт, що програма Партнерства передбачає розроблення та запровадження механізму взаємодії державних органів у сфері стратегічних комунікацій щодо проведення інформаційно-психологічних операцій та інших спеціальних заходів, а також реалізації зв'язків з громадськістю, планом заходів передбачене створення постійно діючої міжвідомчої робочої групи з питань координації зазначеної діяльності.

Окремим заходом має стати впровадження практичного механізму ефективного використання комунікацій у кризовий період.

З огляду на високий рівень актуальності питання інформування населення, особливо тимчасово окупованих територій та тих, що межують з ними, в рамках розбудови системи стратегічних комунікацій запланована підготовка Стратегії інформаційної присутності України на окупованих та звільнених територіях, а також проведення спільних наукових досліджень з питань стратегічних комунікацій, спрямованих на впровадження досвіду НАТО в Україні.

З метою забезпечення оперативної взаємодії, проведення спільних заходів, а також анонсування запланованих міжвідомчих заходів передбачене створення єдиної інформаційної бази даних ЗМІ.

Важливим напрямом роботи Партнерства є формування системи підготовки спеціалістів у галузі стратегічних комунікацій – створення єдиної навчальної бази та системи для підготовки фахівців у сфері стратегічних комунікацій, зокрема шляхом унесення змін до навчальних програм ВНЗ та проведення цільових курсів.

Заходи Партнерства у сфері стратегічних комунікацій сприятимуть розвитку здатності України здійснювати ефективні комунікації, забезпеченню системної взаємодію між усіма зацікавленими суб'єктами урядового та неурядового сектору, а також реалізації ефективних заходів протидії російській пропаганді та інформуванню громадськості про події в Україні.

УДК 005.3

Пилипчук В. Г.
доктор юридичних наук, професор, член-кореспондент Національної академії правових наук України, заслужений діяч науки і техніки України
Науково-дослідний інститут інформатики і права Національної академії правових наук України

СИСТЕМА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ПРОБЛЕМИ ФОРМУВАННЯ І ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ

Протягом 2014 – 2015 років в Україні, зокрема, в ході проведених конференцій та інших заходів, організованих Національною академією СБ України, НДІ інформатики і права НАПрН України та іншими закладами і установами, було розроблено низку цікавих пропозицій і рекомендацій з проблем інформаційної безпеки.

За останні роки в Українському суспільстві значно змінилося розуміння важливості проблем розвитку інформаційної сфери та необхідності забезпечення інформаційної безпеки. На державному рівні у цій сфері вжито низку правових, організаційних, оперативно-службових та інших заходів.

Водночас, як свідчить аналіз, система забезпечення інформаційної безпеки ще залишається недостатньо ефективною і такою, що не повною мірою відповідає національним інтересам України.

Враховуючи зазначене звернімо увагу на деякі актуальні проблеми, що стосуються інформаційної сфери і потребують правового врегулювання.

Насамперед, актуальною залишається ***проблема розробки та реалізації ефективної державної інформаційної політики***. Певною мірою це можна пояснити низкою об'єктивних і суб'єктивних чинників, починаючи від задекларованого внесення відповідних змін до Конституції України і закінчуючи питаннями кадрового та іншого ресурсного забезпечення.

Поряд з цим, варто зауважити, що *інформаційна сфера* включає *інформаційні технології, інформаційні ресурси, інформаційну продукцію та послуги*.

До ***функціональних напрямів інформаційної діяльності***, за нашими оцінками, підтриманими наказом МОН України від 29.09.2014 № 1081, слід віднести:

– адміністративні послуги (електронне урядування) і доступ до публічної інформації;

– телекомунікації, зв'язок, інформатизацію;

– засоби масової інформації, глобальні інформаційні мережі, рекламу;

– видавничу, бібліотечну, архівну і музейну справи;

– державну статистику і документообіг (електронний документообіг, електронний підпис тощо);

– інформаційну діяльність в галузях освіти і науки, культури і мистецтв;

– інформаційну діяльність в економічній, фінансовій, банківській та інших сферах (е-торгівля, е-комерція, е-банкінг тощо).

Тобто, мова йде про комплексний характер інформаційної сфери, який стосується різних напрямів життєдіяльності людини, суспільства і держави. За цих умов державну інформаційну політику має визначати Верховна Рада України, а пропозиції щодо неї повинні розробляти та реалізовувати в межах компетенції центральні органи виконавчої влади під загальним керівництвом Кабінету Міністрів України.

Не менш ***складною залишається ситуація*** з питань ***забезпечення інформаційної безпеки*** України, де існує низка політико-правових, організаційних, оперативно-службових, кадрових та інших проблем.

Насамперед, звернімо увагу, що згідно з чинним законодавством *сфера інформаційної безпеки є складовою національної безпеки* України, а до с*уб'єктів забезпечення інформаційної безпеки* (або суб'єктів забезпечення національної безпеки в інформаційній сфері), за нашими оцінками, можуть бути віднесені:

1) Президент України, Верховна Рада України, Кабінет Міністрів України, Рада національної безпеки і оборони України;

2) Міністерство з питань інформаційної політики України, Державний комітет телебачення і радіомовлення України, Національна рада з питань телебачення і радіомовлення, Державна служба спеціального зв'язку і технічного захисту інформації України та інші центральні органи виконавчої влади, державні адміністрації та органи місцевого самоврядування, Національна

поліція і Державне бюро розслідувань, що формуються, органи прокуратури та судові органи;

3) Служба безпеки України, Служба зовнішньої розвідки України, Державна прикордонна служба України, Збройні Сили України та інші військові формування України;

4) державні і недержавні засоби масової інформації, підприємства, заклади, установи та організації різних форм власності, що здійснюють інформаційну діяльність;

5) наукові установи і навчальні заклади України, які здійснюють наукові дослідження та підготовку фахівців за різними напрямами інформаційної діяльності, в галузі інформаційного права та інформаційної безпеки;

6) громадяни України та інші особи, за їх згодою, громадські організації та інші інститути громадянського суспільства.

З огляду на викладене актуальною постає ***проблема протидії сучасним викликам і загрозам інформаційній безпеці*** та ***координації діяльності*** у цій сфері.

Для вирішення вказаної проблеми ще 2014 року у проекті *Закону України «Про засади інформаційної безпеки України»* (реєстр. № 4949) пропонувалося створити центральний орган виконавчої влади зі спеціальним статусом у сфері інформаційної безпеки та його міжрегіональні підрозділи. Але вказаний орган так і не було сформовано. Як свідчить аналіз, окрім правового забезпечення, реалізація цієї пропозиції потребувала б певного часу і необхідних організаційних, кадрових, фінансових та інших ресурсів.

Також слід зауважити, що основні завдання з питань запобігання, виявлення, попередження і припинення чи нейтралізації реальних і потенційних викликів і загроз інформаційній безпеці, протидії кіберзлочинності та іншим правопорушенням в інформаційній сфері нині в межах компетенції переважно реалізуються Службою безпеки України, розвідувальними органами України, Державною службою спеціального зв'язку і технічного захисту інформації України та Національною поліцією України. Водночас, за нашими оцінками, їх зусилля значною мірою залишаються розпорошеними і не поєднаними єдиними організаційними та оперативно-службовими задумами, а функції подекуди дублюються.

За цих умов, безперечно, більш вагомою щодо координації діяльності державних і недержавних суб'єктів забезпечення інформаційної безпеки, насамперед, з політико-правових питань, має бути роль Ради національної безпеки і оборони України.

Поряд з цим, заслуговують на увагу пропозиції стосовно надання Службі безпеки України правового статусу головного органу або спеціально уповноваженого державного органу у сфері забезпечення інформаційної безпеки. На користь цієї пропозиції може слугувати наступне:

– відповідно до ст. 17 Конституції України забезпечення інформаційної безпеки віднесено до основних функцій держави. Події останніх років свідчать, що застосування «інформаційної зброї» у т.зв. «гібридній війні» проти України та наявні виклики і загрози в інформаційній сфері створюють реальні загрози конституційному ладу та державній безпеці України, забезпечення якої згідно з чинним законодавством покладено на Службу безпеки України;

– в Центральному управлінні та регіональних органах СБ України функціонує розгорнута система інформаційно-аналітичних підрозділів, підрозділів контррозвідувального захисту інтересів держави у сфері інформаційної безпеки, підрозділів захисту національної державності та підрозділів забезпечення охорони державної таємниці. На базі останніх, за оцінками вітчизняних та іноземних експертів, розгорнуто досить ефективну систему охорони державних секретів та конфіденційної інформації, що є власністю держави;

– практика надання правового статусу спеціально уповноваженого державного органу або головного органу у різних сферах вже апробована чинним законодавством. Зокрема, відповідно до законів України «Про державну таємницю», «Про контррозвідувальну діяльність» та «Про боротьбу з тероризмом» СБ України є спеціально уповноваженим державним органом у сфері забезпечення охорони державної таємниці та у сфері контррозвідувальної діяльності, а також головним органом у загальнодержавній системі боротьби з терористичною діяльністю;

– надання СБ України правового статусу головного органу або спеціально уповноваженого державного органу у сфері забезпечення інформаційної безпеки, на відміну від створення нового центрального органу виконавчої влади, не потребуватиме значних кадрових, фінансових та інших ресурсних витрат.

В цілому, зазначені пропозиції, а також функції з питань забезпечення інформаційної безпеки, які можуть покладатися на СБ України, за нашими оцінками, потребують додаткової експертної оцінки, опрацювання і правового врегулювання.

Крім зазначеного, ***актуальною залишається проблема законодавчого забезпечення у сфері інформаційної безпеки***. Зокрема, основні нормативно-правові акти у цій сфері, насамперед, «Концепція інформаційної безпеки України», як це передбачено коаліційною угодою парламентських фракцій, а також закони України «Про засади інформаційної безпеки України» та «Про кібернетичну безпеку» так і залишилися не опрацьованими та не прийнятими Верховною Радою України.

Загалом, підсумуємо викладене такими основними **висновками і пропозиціями:**

1) *інформаційну сферу* можна визначити як сукупність інформаційних технологій, ресурсів, продукції і послуг, інформаційної інфраструктури, суб'єктів інформаційної діяльності та системи регулювання суспільних інформаційних відносин; а *забезпечення інформаційної безпеки* – як діяльність, спрямовану на запобігання, своєчасне виявлення, припинення чи нейтралізацію реальних і потенційних загроз інформаційній безпеці України;

2) державну інформаційну політику має визначати Верховна Рада України, а пропозиції щодо неї повинні розробляти в межах компетенції центральні органи виконавчої влади під керівництвом Кабінету Міністрів України. Водночас, основи політики держави у сфері інформаційної безпеки визначаються законодавством про основи національної безпеки, а пропозиції щодо формування та реалізації державної політики у цій сфері мають розроблятися, насамперед, суб'єктами забезпечення національної безпеки в інформаційній сфері;

3) функції Ради національної безпеки і оборони України щодо координації діяльності державних і недержавних суб'єктів забезпечення інформаційної безпеки, насамперед, з політико-правових питань, можуть бути посиленими. Водночас, заслуговують на увагу і потребують опрацювання пропозиції стосовно надання СБ України правового статусу головного органу або спеціально уповноваженого державного органу у сфері забезпечення інформаційної безпеки;

4) у законодавчих актах з питань інформаційної безпеки, що потребують першочергового опрацювання та прийняття, мають бути врегульовані питання функціонування системи забезпечення інформаційної безпеки, а також реалізовані принципи захисту прав, свобод і безпеки людини та законних інтересів суспільства і держави в інформаційній сфері.

УДК 681.384

Пилипчук В. В.
кандидат технічних наук
Воєнно-дипломатична академія імені Євгенія Березняка

КОМПЛЕКСНИЙ ПІДХІД ДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

В умовах сьогодення все гостріше постає питання забезпечення інформаційної безпеки в сучасних автоматизованих системах (АС) Вирішення зазначеного питання може бути успішним лише за умови використання комплексного підходу до побудови системи забезпечення інформаційної безпеки, що охоплює всі аспекти життєдіяльності організації.

Комплексна система захисту інформації повинна будуватися з урахуванням чотирьох рівнів будь-якої інформаційної системи:

1. Рівень прикладного програмного забезпечення (ПЗ), що відповідає за взаємодію з користувачем. Прикладом елементів АС, які працюють на цьому рівні, можна назвати текстовий редактор WinWord, редактор електронних таблиць Excel, поштова програма Outlook, браоузер Internet Explorer.

2. Рівень системи управління базами даних (СКБД), що відповідає за зберігання і обробку даних інформаційної системи. Прикладом елементів АС, які працюють на цьому рівні, можна назвати СКБД Oracle, MS SQL Server, Sybase, MS Access.

3. Рівень операційної системи (ОС), що відповідає за обслуговування СКБД і прикладного ПЗ. Прикладом елементів АС, які працюють на цьому рівні, можна назвати ОС Microsoft Windows NT, Sun Solaris, Novell Netware.

4. Рівень мережі відповідає за взаємодію вузлів інформаційної системи. Прикладом елементів ІС, які працюють на цьому рівні можна назвати протоколи TCP / IP, IPS / SPX і SMB / NetBIOS.

Забезпечення інформаційної безпеки має починатися з аналізу автоматизованої системи і технології обробки інформації. Даний етап дозволить не тільки виявити і проаналізувати можливі шляхи реалізації загроз безпеці, але й оцінити ймовірність і збиток від їх реалізації. За результатами цього етапу розробляються рекомендації щодо усунення виявлених загроз, правильно-

го вибору і застосування засобів захисту. Разом із проведенням аналізу існуючої АС, повинна здійснюватися розробка організаційно-розпорядчих документів, що дають необхідну правову базу службам безпеки і відділам захисту інформації для проведення всього спектру заходів, пов'язаних із захистом інформації, взаємодії з зовнішніми організаціями, залучення до відповідальності порушників, та інше.

Наступним етапом побудови комплексної системи інформаційної безпеки служить установка і настройка рекомендованих на попередньому етапі засобів захисту інформації. До таких засобів можна віднести системи захисту інформації від несанкціонованого доступу, системи криптографічного захисту, мережні екрани, засоби аналізу захищеності.

Для правильного і ефективного застосування встановлених засобів захисту АС необхідний кваліфікований персонал. Однак ситуація, що склалася у державі вказує на те, що поки таких фахівців мало. Виходом з ситуації, що склалася, можуть стати курси підвищення кваліфікації, на яких співробітники відділів захисту інформації та служб безпеки отримають всі необхідні практичні знання для використання наявних засобів захисту, виявлення загроз безпеки АС і запобігання таким загрозам.

Однак на цьому процес забезпечення безпеки інформації не закінчується. З плином часу наявні засоби захисту застарівають, виходять нові версії систем забезпечення інформаційної безпеки, постійно розширюється список знайдених вразливостей і атак. Тому фахівцям в області захисту інформації необхідна своєчасна, а також повна інформація про такі події.

Оскільки технології оброблення інформації, програмні і апаратні засоби повсякчас змінюються, існує необхідність періодично переглядати розроблені організаційно-розпорядчі документи, проводити обстеження автоматизованої системи або її підсистем, навчати новий персонал, підвищувати його кваліфікацію, оновлювати засоби захисту АС.

Література

1. Петренко С.А. Политики безопасности компании при работе в интернет – М.: ДМК Пресс, 2011. – 396 с.

2. Блинов А.М. Информационная безопасность: Учебное пособие. Часть 1. – СПб.: Издательство СПбГУЭФ, 2010. – 96 с.

3. ISO/IEC 27001:2005, Information technology – Security techniques – Information security management systems.
4. ISO/IEC 38500:2008, Corporate governance of information technology.
5. Комплексная система защиты информации на предприятии: учеб. пособие для студентов / В.Г. Грибулин, В.В. Чудовский. – М.: Издательский центр «Академия», 2009. – 416 с.

УДК 355.34:94[477]

Сідак В. С.
доктор історичних наук, професор, член-кореспондент
Національної академії педагогічних наук України
Національна академія СБ України

ІСТОРИЧНІ АСПЕКТИ ПРОБЛЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ

Сучасний період життя суспільства характеризується всезростаючою роллю інформаційної сфери, яка являє собою сукупність інформації, інформаційної інфраструктури, суб'єктів, що здійснюють збір, формування, поширення й використання інформації, а також системи регулювання суспільних відносин, що виникають при цьому. А отже, проблеми інформаційної безпеки набувають особливої ваги.

Незважаючи на те, що інформаційна безпека, як окрема проблема була сформульована і названа тільки в період інтенсивної комп'ютерно-телекомунікаційної інформатизації, вона, по суті, має загальний у часі й просторі характер. Вона існує стільки, скільки існує людство, і проявлялася у всіх сферах діяльності людей, суспільств і держав. Тож осмислити проблеми, що нині постали перед нами у сфері забезпечення інформаційної безпеки ми можемо лише розглянувши їх еволюцію.

Передусім зауважимо, що з огляду на управлінські проблеми, слід вести мову не лише про стан захищеності систем обробки і зберігання даних, але й у широкому контексті захищеності інформаційного поля держави. Зрештою, як свідчить вивчення історичного досвіду, саме захищеність інформаційного поля слугувала основною гарантією захищеності і конфіденційності інформації.

Інформаційна безпека держави характеризується ступенем захищеності і, отже, стійкістю її основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи, суспільної свідомості і т. д.) по відношенню до небезпечних інформаційних впливів, причому як до впровадження, так і до вилучення інформації [1].

Появу такого поняття, як інформаційна безпека, а отже й перші кроки на шляху до його врегулювання, включно з управлінськими, ми можемо простежити ще з додержавного періоду історії – часу появи інформаційних комунікацій в суспільстві, та з усвідомленням наявності інтересів, що можуть зазнати шкоди шляхом впливу на засоби інформаційних комунікацій.

Інформація, як відомо, є засобом, що забезпечує можливість адаптації людини й суспільства до умов існування, засобом нагромадження знань про навколишній світ, на основі яких люди й суспільство реалізують свої інтереси. Людина господарювала й годувала себе завдяки систематизації знань, розвивалася під впливом інтелектуального раціоналізму науки, створювала дедалі досконаліші технології, а тому масиви змістовних інформаційних ресурсів із часом стали невід'ємною частиною багатства окремих людей, монастирів, університетів і взагалі держав. Тисячі років знадобилося для того, щоб послідовно перейти від примітивних засобів комунікації до сучасних.

З огляду на невисокий практичний інтерес, недоцільно розглядати діяльність, спрямовану на захист інформації від архаїчних часів до феодального суспільства через вкрай нечітке категорування інформації, невизначеність об’єкту захисту. Загалом, тривалий час основним методом захисту таємниць та інформаційного поля була ксенофобія, виведена в абсолют. В подальші епохи, домінантною стала клерикальна складова. Основне завдання інформаційної безпеки полягало в захисті відомостей про події, факти, майно, місцезнаходження і інші дані, що мають для людини особисто або співтовариства, до якого вона належала, життєве значення. Водночас, якщо вести мову про Україну, то вже в цей час можна зауважити боротьбу за окремішність інформаційного простору, укоріненість розуміння спільності поставлених інформаційних завдань.

З певними застереженнями появу інформаційного суспільства можна констатувати з часу завершення Наполеонівських війн.

Умовно є підстави вважати, що цей період протривав до початку XX ст., коли поява індустріального суспільства продемонструвала нові, небачені до того інформаційні можливості, що й були використані у світових війнах. Водночас, вдосконалювався захист нових технічних засобів зв'язку, використовувався досвід першого періоду інформаційної безпеки на вищому технологічному рівні.

Провідні, передусім воєнні мислителі починають розрізняти внутрішні та зовнішні джерела інформаційної безпеки. Під внутрішніми джерелами розуміють наявність історичного, політичного та соціального досвіду життя у правовій державі, що торкається процесу практичної реалізації прав та свобод громадян, в тому числі в інформаційній сфері. До зовнішніх джерел належать здатність протидіяти діяльності іноземних політичних, військових, економічних та розвідувальних структур в інформаційній сфері; політиці домінування деяких країн в інформаційній сфері; діяльності міжнародних терористичних груп; іншим диверсифікаційним явищам [2, 3].

Важливо відзначити, що з терміном інформаційної безпеки тісно зв'язані інші поняття. Це, зокрема, захист інформації, інформаційні ресурси, інформаційні ризики, інформаційний продукт, інформаційна сфера, інформаційна діяльність, інформаційне середовище й ряд інших.

З’являється і таке поняття, як інформаційна війна. Тривалий час вона виступала складовою концепції тотальної війни. Особливо слід зауважити, що практичне застосування напрацьованих теоретичних розробок у сфері інформаційного протиборства вперше широко були застосовані у роки Кримської війни 1853-1856 рр., основні події якої були пов’язані з Україною. На даний час, ця ідея еволюціонувала до поняття гібридної війни, вийшовши на якісно новий рівень розвитку.

Тривалий час визначення інформаційної війни здійснювалось у вузькому розумінні, відбиваючи суто воєнну спрямованість. Та вже наприкінці століття мова стала вестись в широкому розумінні, відбиваючи спрямованість на забезпечення національних інтересів в будь-якій життєво важливій сфері державної і суспільної діяльності.

Ключовою подією, що ознаменувала собою початок нової епохи інформаційного протиборства, цілеспрямованого використання інформаційних ресурсів та управління інформаційною без-

пекою, як складової загальнодержавної діяльності, є Перша світова війна. Інформація тут остаточно перетворюється на вид зброї, а інформаційні процеси виступають основою реалізації інформаційних загроз інтересам країни в будь-якій сфері і заходів з їх нейтралізації.

Метою інформаційної боротьби у вузькому розумінні проголошується захоплення й утримання інформаційної переваги над противником під час підготовки й в ході воєнних дій. Правлячі кола починають цілеспрямований і комплексний вплив на свідомість і підсвідомість населення, на інформаційні ресурси на всіх фазах їх продукування, розповсюдження й використання, а також на інші складові інформаційного середовища. Особливої ваги набуває не так руйнівний, як цілеспрямований вплив саме на зміст інформації для забезпечення своїх інтересів у різних сферах діяльності особистості, суспільства, країни [4].

Вдосконалюються і методи протидії. Не зменшуючи важливості виконання завдань технічного захисту інформації, спрямованого в основному на забезпечення її конфіденційності, слід підкреслити особливу значущість завдань захисту власне змісту інформації від навмисного його спотворення чи перекручення, у тому числі й завдань виявлення дезінформації.

Задля справедливості, слід зауважити, що фахівці з власне, технічного захисту інформації виділяють період з 1935 по 1946 рр. – час стрімкого розвитку засобів радіолокації і гідроакустики. Основним способом забезпечення інформаційної безпеки в цей період було поєднання організаційних і технічних заходів, направлених на підвищення захищеності засобів технічного зв’язку [5].

З початком інформаційної ери (1946 р.) завдання інформаційної безпеки вирішувалися, в основному, методами і способами обмеження фізичного доступу до устаткування засобів добування, переробки і передачі інформації. Розвиваються нові інформаційно-комунікаційні мережі. Завдання інформаційної безпеки вирішувалися, в основному, методами і способами фізичного захисту засобів добування, переробки і передачі інформації, об'єднаних в локальну мережу шляхом адміністрування і управління доступом до мережевих ресурсів. Інформаційний ресурс став найважливішим ресурсом держави, а забезпечення його безпеки – найважливішою і обов'язковою складовою національної безпеки.

З 1985 р. починається новий етап управління інформаційною безпекою. Закінчується «холодні війна», що була визначальним чинником пріоритетів захисту інформаційного поля держави. Розвиваються глобальні інформаційно-комунікаційні мережі. Починається епоха, що завершилась трансформацією засобів масової інформації у засоби масової комунікації. Для вирішення завдань інформаційної безпеки на цьому етапі необхідним є створення макросистеми інформаційної безпеки людства під егідою ведучих міжнародних форумів [5].

Таким чином, ми бачимо, що тривалий час управління інформаційною безпекою здійснювалось у контексті ведення воєнного ти політичного протиборства. Певні зрушення в усвідомленні інформаційної безпеки припадають на час т.зв. «холодної війни». І, нарешті, зараз ми вже можемо вести мову про інформаційну безпека держави – стан захищеності життєво важливих інтересів людини, суспільства і держави [6].

На жаль, нині, навіть в умовах боротьби з агресією РФ нам доводиться констатувати несистемну політику держави у сфері інформаційних продуктів та інформаційних послуг, що зумовлює витіснення українського продукту та поступове заміщення його не просто неукраїнським, а часто антиукраїнським за сутністю.

Література

1. Князев А.А. Информационная война // Энциклопедический словарь СМИ // [Електронний ресурс]. — Режим доступу: — http://voluntary.ru/dictionary/1105/word/informacionaja-voina.

2. Свечин А.А. Стратегия. – М.-Л.: Государственное военное издательство, 1926. – 400 с. 3. Батюшин Н.С. У истоков русской контрразведки. Сборник документов и материалов / Вступ. ст. И.И. Васильева, А.А.Здановича; Комент., подбор док. и ил. В.К.Былинина. – М.: Икс – Хистори; Кучково поле, 2007. – 496 с.

4. Блументаль Ф. Л. Буржуазная политработа в мировую войну 1914–1918 гг. : обработка общественного мнения. – М.-Л.: Государственное издательство, 1928. – 360 с.

5. Історія виникнення інформаційної безпеки // // [Електронний ресурс]. — Режим доступу: — http://bsit10.at.ua/publ/istorija_viniknennja_informacijnoji_bezpeki/1-1-0-1.

6. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» від 09.01.2007 № 537-V // http://zakon3.rada.gov.ua/laws/show/537-16 [електронний ресурс].

УДК 35:303:004

Соснін О. В.
доктор політичних наук, професор, заслужений діяч науки і техніки України,
член-кореспондент Української академії політичних наук
Національний авіаційний університет

ПРОБЛЕМИ БЕЗПЕКИ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ ДІЯЛЬНОСТІ ДЕРЖАВИ

Сучасне суспільство постійно і всюди живе в ситуації глобальних викликів, ризиків і загроз. Поступово долаючи їх, зокрема і в сфері управління, людство здобуває досвід на шляху цивілізаційного розвитку. Фундаментальних знань і характеристик щодо процесів управління в постіндустріальному світі ми поки що не сприймаємо повною мірою, а лише активно ревізуємо запропоновані в минулому методи. Як наслідок, ніякого серйозного аналізу і шляхів щодо вирішення проблем управління Україною в постіндустріальну добу ніхто не пропонує, а коло гострих і невирішених питань неухильно зростає. Просто на наших очах стрімко виникає багато, глобальних за виміром, проблем, зокрема в інформаційно-комунікаційній сфері, які вимагають не просто термінового реформування управлінських вертикалей, а взагалі кардинальної перебудови влади і суспільства.

Важливою характеристикою й конкурентним фактором в процесах розвитку країн наприкінці XX століття стала динаміка і форми управління інформаційно-комунікаційними процесами в суспільстві, їх швидкість і спрямованість до новизни і креативності рішень, що приймаються. Стрімкий розвиток інформаційних і комунікаційних технологій, проникнення їх в усі сфери суспільно-політичного життя, сам по собі обумовив потребу більшості громадян залучитися до процесів управління на всіх рівнях. Як наслідок, зросли вимоги громадян до «відкритості» влади. Тобто розуміння своїх прав і свобод тощо і це стало викликом часу рівня доступності інформації. Реагуючи на такий виклик суспільство швидко усвідомило, що інформаційно-комунікаційна сфера являє собою найменш формалізоване середовище життєдіяльності людини, як в силу природи інформації, так і властивостей людської

свідомості. Вони дійсно важко піддаються жорстким зовнішнім алгоритмам управління, за виключенням тих випадків, коли людина, як носій свідомості, перебуває у стані несвободи.

В природному процесі відображення проблем, свободи людини і її прав на інформацію завжди необхідно співставляти два категоріальних поняття, як відображають загальнолюдські цінності: «свобода» і «необхідність», «свобода» і «відповідальність». Як свідчить досвід в сфері інформаційно-комунікаційної діяльності людини, суспільства і держави завжди має бути досягнуто їх розумне співвідношення заради безпеки існування. Воно традиційно було присутнє і в нашій культурі, однак, із розвитком інформаційно-комунікаційних технологій (ІКТ) об'єктивні і суб'єктивні обставини постійно заважають нам скористатися досвідом в організації на таких засадах інформаційно-комунікаційної функції держави і в розбудові інформаційно-комунікаційної сфери країни взагалі. Проблема постійно поглиблюється, експотенціально зростає, як рівень загроз так і рівень відповідальності влади за її ефективне вирішення. Нам постійно не вистачає фаховості і можливостей генерувати тут якісні і збалансовані в часі сценарії і стратегії, які були би адекватні стратегічним прогнозам і планам розвитку країни, і саме тут сьогодні визріває в нашому суспільстві підґрунтя для нових конфліктів економічного, геополітичного, етнічного тощо характеру.

Під впливом соціально-економічних і політичних процесів активної участі в них ТНК ознака доступності інформації стає взагалі домінуючою світовою тенденцією в інформаційно-комунікаційній і інформаційно-аналітичній роботі. Все це впливає на розвиток нашого і суспільств різних країн і таким чином питання прав і свобод громадян в інформаційно-комунікаційній сфері стрімко набуває ознак головної проблеми суспільного розвитку. Право народу знати, свобода на висловлювання у своїй сукупності утворюють і кристалізують саму ідею створення громадянських суспільств і одночасно виносять на поверхню питання безпеки інформації, кібернетичної безпеки і взагалі інформаційної безпеки людини, суспільства і держави в постіндустріальну добу. Наразі в нашому суспільстві йде активне їх обговорення.

Сьогодні зокрема актуальними є питання щодо того, що являє собою те, що окреслюється терміном «кібернетична безпека» (кібербезпека), і як вона співвідноситься з існуючими в націона-

льному законодавстві поняттями, зокрема такими, як «захист інформації в інформаційно-телекомунікаційних системах»? Розуміючи, що кібернетична безпека (кібербезпека) взагалі – це стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в світовому кібернетичному просторі (кіберпросторі) – ми маємо постійно і прискіпливо вивчати це середовище. Воно виникло в новітню добу в результаті функціонування комп'ютеризованих засобів зв'язку і пов'язаних з ними комп'ютерних технологій, реєстрації, збереження і поширення інформації в комп'ютерних мережах на основі єдиних принципів і за загальними правилами. Звідси виникло і надважливе питанню щодо того, хто в державі повинен займатися цим, опікуватися питаннями захисту інформації? Безумовно, можна вважати, що таким органом в Україні є Державна служба спеціального зв'язку та захисту інформації, яка була утворена в часи набуття незалежності і постійно розвивається, її призначення, по-перше, безумовно полягає у формуванні та реалізації державної політики у сфері захисту інформації, однак, комплекс питань, які пов'язано із цим при виконанні державою інформаційно-комунікаційної функції в умовах зростання темпів інформації комп'ютеризованого світу, вимагає залучення до цієї роботи всього державно-управлінського апарату країни і структур громадянського суспільства. Складна сукупність проблем означає, що ми повинні знати і вміти ефективно користуватися накопиченими людством інформаційними ресурсами і захищати його при користуванні новітніми ІКТ, відкритими і утаємниченими знаннями, проводити якісну і успішну кадрову політику.

Всі провідні країни світу відверто і прагматично, навіть агресивно захищають тут свої інтереси, а сьогодні іноді і за межами кордонів своїх держав. Вони давно почали розглядати іноземні об'єкти інформаційно-комунікаційних інфраструктур як власні і критичні, а їх безпеку своїм найважливішим завданням. Оприлюднені останнім часом факти про витоки інформації за допомогою технічних і інших засобів іноземних розвідок свідчать про те, що розвідка стала невід'ємним компонентом систем ведення бізнесу і державного управління.

Україні катастрофічно не вистачає фахівців для інформаційно-комунікаційної, аналітичної, інформаційно-пропагандистської та управлінської роботи. В умовах домінування цифрових техно-

логій, проблема об'єктивно не може бути розв'язана риторикою політичних лідерів, політологів, соціологів і інших фахівців гуманітарних наук. Ситуація змушує нас зокрема по новому і більш прискіпливо оглянути всю проблематику створення, зберігання і ефективного використання інформаційних ресурсів і, як насідок, аналітичної роботи з великими масивами даних, в системі управління державою і суспільством. Аналітика, без сумніву, є для нас найбільш критичною. В циклі управління вона більш за все вимагає від владних структур активної розумової високопрофесійної праці фахівців і опанування технологіями стратегічного аналізу, інформації, включаючи і роботу із автоматизованими мережевими інформаційно-керуючими системами.

Осягнути ситуацію і точно визначати тут коло проблем, які нам сьогодні треба знати і вирішувати, ми поки що не змогли повною мірою. Для цього, крім досягнення відповідного науково-технічного рівня, потрібна постійна відверта і публічна дискусія фахівців із поверненням до витоків самої проблеми щодо гуманістичних методів управління суспільством і інформаційно-комунікаційною сферою. Особливо прискіпливо ми маємо оглянути проблему в контексті вирішення проблем розбудови в Україні мережевого інформаційно-комунікаційного середовища в умовах, коли проти нас розгорнута повномасштабна інформаційна і військова агресія.

Розриваючи коло накопичених проблем, Україна, безумовно, має піти на безпрецедентні реформи в інформаційно-комунікаційній сфері, науці, освіті, про що ми багато говоримо протягом усіх років незалежності. Корупція та винайдена бюрократами формальна імітація тут корисної діяльності набула в нас масштабу справжнього лиха. Все це знецінює найцікавіші і розумні ідеї креативно мислячих громадян України, перетворює їх корисні починання у щось зовсім протилежне задумам. Слід визнати, що внаслідок цього і багатьох інших причин у нас відбувся провал всіх моделей інноваційного розвитку суспільства, і стався він тому, що не було враховано повною мірою ані нашим законодавством, ані свідомістю громадян, цінність і могутність сучасних інформаційно-комунікаційних чинників. Сам термін «інновація» став у нас лише найбільш популярною оцінкою стану й перспектив розвитку суспільства, а не базовим принципом нашого сучасного світогляду, який би визначав місце людини у світі, мотиви й мету її діяльності.

Література

1. Соснін О. В. До питання організації інноваційного оновлення України /О.В. Соснін // Віче, громадсько-політичний і теоретичний журнал Верховної Ради України. – № 22 (378). - листопад 2014. – С.14-19.

УДК 341.824:338.47 (043.2)

Тиква В. Л.
Національна академія СБ України

СУТНІСТЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ, СУСПІЛЬСТВА ТА ОСОБИСТОСТІ

Перш ніж розкривати сутність і зміст поняття «Інформаційна безпека», необхідно спочатку визначитися, що слід розуміти під безпекою як такою.

Існує досить багато визначень поняття «безпеки». Найчастіше безпеку трактують як такий стан, коли немає небезпеки, тобто «чинників і умов, загрозливих існуванню безпосередньо індивідові або його співтовариству у формі сім'ї, населеного пункту або держави». А. Бурьяк трактує національну безпеку як «показник стану нації, що означає, що сукупна дія внутрішніх і зовнішніх шкідливих чинників не може значно понизити якість її життя і не створює загрозу її існуванню». І. Л. Прохоренко дає таке визначення: «Національна безпека – це таке поєднання внутрішніх і зовнішніх обставин, що впливають на життя держави, при якій відсутні загрози критичного характеру і в той же час зберігається повноцінна здатність держави адекватно реагувати на ці загрози, якщо вони виникнуть». Безпека досить часто трактується як здатність об'єкта зберігати за наявності деструктивних, дезорганізуючих дій (зовнішніх і внутрішніх) свої найважливіші, системотворчі властивості, основні характеристики і параметри, втрата яких може привести до того, що об'єкт втрачає свою сутність, перестає бути самим собою. Ряд дослідників під безпекою розуміє систему гарантій, що забезпечує явищу його нормальний розвиток. У Законі Російської Федерації «Про безпеку» вміст поняття «безпеки» трактується як «стан захищеності життєво важливих інтересів особи, суспільства і держави від внутрішніх і зовнішніх загроз».

Практично всі приведені вище визначення піддавалися і продовжують піддаватися критиці як з боку фахівців-практиків, так і з боку вчених. Звичайно, що безпека не може існувати без своєї діалектичної протилежності – небезпеки. Більш того, деякий комплекс небезпек присутній завжди. Поняття «небезпека» в найзагальнішому плані характеризує такий стан об'єкту, при якому загроза його буттю за рахунок розриву або спотворення найбільш істотних зв'язків і стосунків в системі перевищує деяку гранично допустиму суб'єктивно встановлену величину. Небезпека виникає тоді, коли об'єкт піддається впливу (зсередини або ззовні) такого вигляду і такої сили, що механізми його життєзабезпечення стають нездатні підтримувати нормальний режим функціонування, унаслідок чого об'єкт може бути частковий або повністю зруйнований (піддатися деструкції) і перестати виконувати свої основні функції (піддатися дисфункції). Варто відзначити, що не кожна загроза деструкції і дисфункції повинна сприйматися як небезпека, а та і лише та, реалізація якої може привести до такого порушення структури об'єкту, при якій він перестає бути структурно цілісним, втрачає власну ідентичність, або порушується його функціональна цілісність. Відповідно, безпека виникає лише як подолання, зняття цієї ситуації.

Безпеку соціального об'єкта слід розуміти як такий стан, при якому забезпечується його стійке існування в межах встановлених параметрів, зберігається можливість і здатність постановки і досягнення вигідних самому об'єкту цілей. При цьому об'єкт може змінюватися у межах допустимого (заходи або норми), ускладнюватися, міняти структуру, властивості, але при цьому він повинен зберігати свої цілі, функції і власну ідентичність (зберегти структурну цілісність і функціональну цілісність).

Визначивши таким чином поняття «безпека», перейдемо тепер до аналізу сутності та змісту поняття «Інформаційна безпека».

Очевидно, що поняття «Інформаційна безпека» взаємозв'язане з поняттям «Безпека інформації». Досить часто їх використовують як синоніми. Але, як відомо, «безпека» не існує сама по собі, безвідносно до об'єкту, «без визначення об'єкту поняття «безпека» є невизначеним, позбавленим внутрішнього сенсу». Вибір об'єкта безпеки зумовлює зміст поняття «безпеки». Тому, якщо об'єктом захисту виступає власне інформація, то поняття «Інформаційна безпека» і «безпека інформації» дійсно ста-

ють синонімами. Але, якщо як об'єкт захисту розглядається деякий об'єкт (суб'єкт) – учасник інформаційних стосунків, то слово «інформаційна» в терміні «інформаційна безпека» вказує на напрям діяльності, за допомогою якої може бути причинена шкода об'єкту захисту і поняття «Інформаційна безпека» в цьому випадку слід трактувати як стан захищеності даного об'єкта від загроз інформаційного характеру. С.П.Расторгуєв, характеризуючи сучасний стан проблеми, пише: «В результаті проблема захисту інформації, яка раніше була як ніколи актуальна, перекинулася подібно до монети, що викликало до життя її протилежність – захист від інформації. Тепер уже саму інформаційну систему і, в першу чергу людини, – необхідно захищати від інформації, що поступає «на вхід», тому що будь-яка інформація, що поступає на вхід самонавчальної системи неминуче змінює систему. Цілеспрямований деструктивний інформаційний вплив може привести систему до безповоротних змін і, за певних умов, до самознищення». Безпека інформації при цьому повинна розглядатися як складова частина загальної проблеми забезпечення безпеки об'єкта захисту, причому не найголовнішою, а лише в тій частині, в якій незабезпечення безпеки інформації, що має відношення до об'єкта захисту, може завдати йому шкоди, яка, у свою чергу, може привести до порушення його структурної і функціональної цілісності.

У нашій країні основна увага громадськості сконцентрована виключно на проблемі захисту інформації. Таке положення склалося з огляду на багато обставин. В першу чергу, це обумовлено очевидністю. Інформація стала товаром, а товар потрібно захищати. Цілком природно, що першими на собі це відчули представники кредитно-фінансової сфери, де інформація – це гроші, а гроші – це інформація. Витекла інформація – витекли гроші. Все гранично просто і вочевидь і, що важливо, збиток має матеріальне вираження, що підлягає рахунку. Наявність фінансових можливостей дозволила кредитно-фінансовому сектору залучити до вирішення питань забезпечення захисту своєї інформації кращих фахівців, сконцентрувавши їх увагу на вузькоспеціалізованих напрямах. У другу чергу – професійною підготовкою фахівців, першими що усвідомили гостроту проблеми. Переважна більшість з них – представники технічних спеціальностей. Але і цими фахівцями безпека самої інформації розуміється неоднозначно. Як

правило, вона трактується як захищеність встановленого статус-кво інформації від внутрішніх і зовнішніх загроз; від витоку, розкрадання, втрати, несанкціонованого знищення, спотворення, модифікації (підробки), несанкціонованого копіювання, блокування інформації і т.п.; від випадкових чи навмисних несанкціонованих впливів на інформацію чи несанкціонованого її здобуття; від випадкового або навмисного доступу осіб, що не мають права на здобуття інформації, її розкриття, і ін. Значно рідше безпека інформації розглядається з точки зору початкової повноти і надійності інформації.

Сутність інформаційної безпеки більшістю фахівців бачиться в неможливості нанесення шкоди об'єкту захисту, його властивостям або діяльності по виконанню своїх функцій. У засадничому документі в цій сфері – Доктрині інформаційної безпеки – під інформаційною безпекою «розуміється стан захищеності її національних інтересів в інформаційній сфері, що визначаються сукупністю збалансованих інтересів особи, суспільства і держави». Таке формулювання знайшло своє місце в Доктрині не дивлячись на те, що терміни «захищеність», «інтереси» та інші є невизначеними і розпливчатими. До цього можна додати, що некоректно розглядати як об'єкти захисту в законі не лише «інтереси», але і «особу», і «суспільство», та і «держава» теж. Перш за все тому, що вони не є суб'єктами права. Як відомо, суб'єктами права є фізичні і юридичні особи (в крайньому випадку – громадяни, особи без громадянства, організації) і виконавчі органи влади. «Особа», «суспільство», «держава» є категоріями соціології, соціальної філософії і використання цих понять в законодавчому акті недоречно. Крім того, поняття ці непорівнянні (різносуттєві) та украй розпливчаті.

Література

1. Інформаційна безпека (соціально-правові аспекти): Підручник / Остроухов В. В., Петрик В. М., Присяжнюк М. М. Жарков Я.М. та ін. За заг. ред. Скулиша Є. Д. – К.: КНТ 2010. – 776 с. (Затверджено МОН України).

2. Історія інформаційно-психологічного протиборства : підруч. / [В.М.Петрик, М.М.Присяжнюк, Я.М.Жарков, Є.Д.Скулиш, Л.Ф.Компанцева, В.В.Остроухов та ін.] ; за заг. ред. Є.Д.Скулиша. – К. : Наук.-вид. відділ НА СБ України, 2011. – 212 с. (Затверджено МОіН,МтаС України).

3. Основи інформаційної безпеки України: навч. посіб. / [кол.авторів; за заг. ред. А.І. Марущака]. – К.: Наук.-вид. центр НА СБ України, 2013. – 388 с.

4. Сугестивні технології маніпулятивного впливу : навчальний посібник / [В.М.Петрик, М.М.Присяжнюк, Л.Ф.Компанцева, Є.Д.Скулиш, О.Д.Бойко, В.В.Остроухов]; за заг. ред. Є.Д.Скулиша. – 2-ге вид. – К.: ЗАТ «ВІПОЛ», 2011. – 248 с.

УДК 005.3

Шопіна І. М.
доктор юридичних наук
Львівський державний університет внутрішніх справ
МВС України

ВЗАЄМОДІЯ ГРУП ЦИВІЛЬНО-ВІЙСЬКОВОГО СПІВРОБІТНИЦТВА ЗСУ ТА СУБ'ЄКТІВ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА У СФЕРІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Забезпечення інформаційної безпеки в районах проведення антитерористичної операції потребує консолідації зусиль держави і громадянського суспільства. Без ефективної взаємодії між ними за сучасних умов обмеження фінансових, людських та технологічних ресурсів перемога в інформаційній війні залишиться недосяжною метою. Одним з основних суб'єктів забезпечення інформаційної безпеки в районах проведення АТО є сьогодні Збройні Сили України, які, внаслідок їх численності та ролі у встановленні миру і відновленні нормальної життєдіяльності регіону, мають потужні важелі впливу для формування довіри місцевого населення до інститутів Української держави.

Разом з тим, внаслідок свідомого, тривалого та цілеспрямованого знецінення ролі військової організації держави Збройні Сили України довгий час знаходилися в процесі стагнації, не мали змоги змінюватися, удосконалювати свою діяльність у відповідності з викликами часу. Наслідком такого стану стало зниження їх боєздатності, що, у поєднанні з відсутністю з політичної волі з боку керівництва держави, призвело до трагічних людських та територіальних втрат. Крім того, невміння та небажання ефек-

тивно використовувати ресурси та потенціал громадянського суспільства для досягнення загальної мети – захисту територіальної цілісності та суверенітету України – ледве не спричинило ще більш тяжкі наслідки, ніж ми маємо сьогодні.

Слід відзначити, що позитивну роль у формуванні нового підходу до взаємодії з громадськістю у вирішенні завдань інформаційної безпеки відіграли і відіграють представники Збройних Сил України, які проходили службу у складі міжнародного контингенту під егідою НАТО. Ознайомлення на практиці з концепцією цивільно-військового співробітництва (Civil-Military Cooperation), запровадженого у діяльність НАТО у другій половині 80-х років XX століття, дозволила виступити з ініціативою започаткування вказаного виду діяльності збройних сил з урахуванням національних реалій. Ініціатива була підтримана керівництвом Генерального Штабу Збройних Сил України, і у другому півріччі 2014 року перші групи цивільно-військового співробітництва (далі - ЦВС) розпочали свою діяльність на території Донецької і Луганської областей.

Не зупиняючись на висвітленні особливостей функціонування груп ЦВС, які вже знайшли своє відображення у наукових публікаціях [1; 2; 3 та ін.], розглянемо їх унікальність з точки зору проблеми організації сумісної діяльності громадянського суспільства і Збройних Сил України в інформаційній сфері. Така діяльність побудована на трьох рівнях і включає до себе етапи підготовки, моніторингу та безпосереднього здійснення інформаційних впливів.

Етап підготовки груп ЦВС охоплюється межами курсів цивільно-військового співробітництва та включає в себе ознайомлення з принципами та стандартами Civil-Military Cooperation, застосовуваними НАТО, отримання знань щодо особливостей менталітету цивільного населення Донбасу, роботи з представниками різних національних груп та релігійних конфесій, вразливими верствами населення, побудови ефективної співпраці з представниками міжнародних організацій, волонтерами, місцевими активістами, навичок інтерв'ювання місцевого населення щодо актуальної ситуації в населених пунктах, мирного врегулювання конфліктів тощо. До підготовки груп ЦВС активно залучаються представники громадянського суспільства, які складають значну частину інструкторів вказаних курсів. Консолідація зусиль військо-

вих і цивільних на етапі підготовки дозволяє уникнути вузьковідомчої спрямованості, притаманної навчальним курсам багатьох силових структур, розширити діапазон знань, вмінь та навичок членів груп ЦВС, отримати необхідні контакти для надання консультативної допомоги у майбутньому. Проведення професійного психологічного відбору осіб, найбільш придатних за своїми особистісними якостями здійснювати діяльність у галузі цивільно-військового співробітництва, дозволяє своєчасно відсіювати військовослужбовців, ефективність роботи яких за даним напрямом викликає сумніви.

Взаємодія між Збройними Силами України та громадянським суспільством в контексті діяльності груп ЦВС на етапі моніторингу базується на принципі об'єктивності, сутність якого полягає у максимальному нівелюванні можливого впливу представників військових підрозділів на достовірність отриманих відомостей про відношення населення до військової організації та інститутів держави в цілому. Для цього було обрано стратегію, яка передбачає максимальну включеність керівництва ЦВС на етапі постановки завдань такого моніторингу та повну відсутність втручання військових в проведення самих опитувань та обробку їх результатів. Завдяки цьому було отримано змогу відстежувати динаміку настроїв населення в районах проведення АТО та використовувати отриману інформацію як у діяльності самих груп ЦВС, так і у роботі з представниками підрозділів Збройних Сил України, дислокованих в Донецькій і Луганській областях.

Безпосередня діяльність груп ЦВС щодо здійснення інформаційних впливів базується на їх співпраці як із представниками волонтерських та благодійних організацій всіх регіонів України, так і в залученні активних представників місцевої громади, формальних та неформальних лідерів, до вирішення завдань у сфері забезпечення інформаційної безпеки. Таке тісне співробітництво мало своїми передумовами не надлишок, а жорсткий дефіцит власних ресурсів Збройних Сил України для допомоги місцевому населенню на початку антитерористичної операції. Втім, на відміну від інших державних структур, для яких обмеження у фінансуванні автоматично означають призупиненя діяльності, керівництво проекту ЦВС знайшло можливість перетворити проблему на перевагу. При цьому знову-таки додержується вимога спільного планування дій і розмежування функцій суб'єктів: допомога надається представниками громадянського суспільства, а групи

ЦВС здійснюють виявлення потреб в ній та забезпечують безпеку бенефеціарів та волонтерів під час її надання. Поєднання зусиль військових та цивільних, серед яких є і місцеві волонтерські та благодійні організації, у вирішенні проблем життєдіяльності регіону дозволяє населенню Донецької та Луганської областей наочно переконатися у відсутності протиставлення держави і суспільства і отримати позитивний досвід переваг від такої співпраці. Інформація щодо конкретних результатів вказаної діяльності активно висвітлюється у соціальних мережах, засобах масової інформації та на веб-сайті ЦВС.

Безумовно, наданням допомоги мешканцям районів проведення АТО інформаційні впливи у діяльності груп ЦВС не вичерпуються. Окремі блоки їх роботи складають взаємодія з представниками органів державної влади та місцевого самоврядування, пропаганда національних цінностей серед учнів загальноосвітніх шкіл, студентів, вихованців музичних, спортивних та інших навчальних закладів, протидія викривленню фактів та інших засобів інформаційної війни з боку протиборчої сторони тощо. Включення у таку діяльність цивільних осіб, врахування їх думки та уявлень щодо оптимальної побудови роботи дозволяє говорити про створення продуктивного співробітництва з метою забезпечення інформаційної безпеки.

Але, зрозуміло, що ситуація є ще далекою від ідеальної. На жаль, принципи комплектування груп на основі відряджень військовослужбовців з їх основного місця служби не дозволяють створити надійний і достатній кадровий резерв груп ЦВС, оскільки керівництво військових підрозділів цілком закономірно намагається залишити кращих військовослужбовців для виконання завдань у пунктах їх постійної дислокації. Значні перешкоди створюють нормативні прогалини у діяльності ЦВС, спроби подолати які майже рік здійснюються на рівні законотворчої роботи, поки що безрезультатно. Разом з тим, за будь-якого варіанту розвитку подій у зоні проведення АТО, спільні зусилля Збройних Сил України та громадянського суспільства, втілені у діяльності груп ЦВС, будуть потрібні ще багато років. Вони вже принесли конкретні результати, напрацьована певна методологія, плани на майбутнє, і від уваги та розуміння керівництва держави та Збройних Сил України залежить підвищення їх впливу на актуальний стан інформаційної безпеки як в Донецькій та Луганській областях, так і в країні в цілому.

Література

1. Ноздрачов О. О. Особливості діяльності груп цивільно-військового співробітництва Збройних Сил України /О.О.Ноздрачов // Актуальні проблеми взаємодії громадянського суспільства і Збройних Сил України: матеріали міжнародної науково-практичної конференції. – Старобільск, 2015. – С.64-66.

2. Коропатнік І. М. Актуальні проблеми розвитку цивільно-військового співробітництва /І.М.Коропатнік // Актуальні проблеми взаємодії громадянського суспільства і Збройних Сил України: матеріали міжнародної науково-практичної конференції . – Старобільск, 2015. – С.43-45.

3. Шопіна І. М. Розвиток досліджень проблем цивільно-військового співробітництва як виду взаємодії держави та громадянського суспільства / І. М. Шопіна //Наука і правоохорона. – 2014. - №4. – С.308-312.

ПРАВОВІ ТА ОРГАНІЗАЦІЙНО-ТАКТИЧНІ АСПЕКТИ ПРОТИДІЇ РОСІЙСЬКІЙ ІНФОРМАЦІЙНІЙ АГРЕСІЇ ЯК СКЛАДОВІЙ ГІБРИДНОЇ ВІЙНИ

УДК 159.9:316.776.23

Андрусишин Ю. І.
кандидат психологічних наук
Національна академія СБ України
Радкович І. М.
Департамент контррозвідки СБ України

ПСИХОЛОГІЧНИЙ ЗАХИСТ ОСОБИСТОСТІ ВІД МАНІПУЛЯТИВНИХ ВПЛИВІВ В СУЧАСНИХ УМОВАХ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА

У сучасному інформаційно перенасиченому суспільстві існує значна кількість найрізноманітніших способів поширення повідомлень, що впливають на свідомість особистості. Для реалізації сучасних технологій інформаційно-психологічного впливу на індивідуальну, групову і масову свідомість людей використовуються [5]: засоби масової інформації та спеціальні засоби інформаційно-пропагандистської спрямованості; глобальні комп'ютерні мережі і програмні засоби розповсюдження в них пропагандистських інформаційних матеріалів; засоби, що нелегально модифікують інформаційне середовище, на підставі чого людина приймає рішення; засоби створення віртуальної реальності; чутки; засоби підпорогового психосемантичного впливу; засоби генерування акустичних і електромагнітних полів тощо. Відповідно, сучасна особистість не може уникнути прихованого психологічного впливу.

До актуальних питань маніпуляції зверталися дослідники різних наукових сфер, зокрема Г. Грачов, С. Кара-Мурза, Г. Ковальов, Л. Компанцева, І. Мельник, В. Петрик, А. Підлісний, В. Толубко, О. Хлоп'єв, Г. Шиллер та ін. Широке охоплення різнобічних проблем інформаційно-психологічного впливу на особистість не дало змоги вченим зупинитися на засобах психологі-

чного захисту від маніпулятивних впливів, що й визначає важливість представленої публікації.

Науковці слушно зазначають [4; 6], що засоби масової інформації є найбільш ефективним інструментом для здійснення інформаційно-психологічного впливу на великі групи людей і тому їх можна вважати складовою частиною стратегічних сил інформаційного протиборства.

Крім того, масова комунікація фактично контролює нашу свідомість, пропускаючи її через свої фільтри, виокремлює певні елементи із загальної маси культурних явищ і надає їм особливої ваги, підвищує цінність однієї ідеї, знецінює іншу. Те, що не потрапило до масової комунікації, в наш час майже не впливає на розвиток суспільства [6].

Найголовнішою обставиною та характеристикою маніпулятивного інформування є те, що, через використання зазначених технологій створюється лише ілюзія незалежності, об'єктивності, можливості вибору певного виду інформації [1, с. 81]. При цьому, виокремлюють три основні родові ознаки маніпуляції [3, с. 12-13]:

- по-перше, це вид духовного, психологічного впливу (а не фізичне насильство чи загроза насильства), об'єктом дій маніпулятора є психічні структури особистості (мотивація, ціннісні орієнтації, пізнавальні процеси тощо);

- по-друге, маніпуляція – це прихований вплив, факт якого не повинен бути помічений об'єктом маніпуляції;

- по-третє, маніпуляція – це вплив, який вимагає значної майстерності та знань.

Психологічний захист від прихованого впливу реалізується особистістю через антиманіпулятивні механізми (методи, прийоми та способи), спрямовані на забезпечення конструктивної поведінки на основі розвиненої емоційно-вольової саморегуляції. Протидія маніпулятивним впливам передбачає здійснення таких основних заходів: регулювання інформаційних потоків (обмеження або ініціацію розповсюдження певної інформації); розширення способів і засобів обробки й оцінки інформації; організацію колективного або групового психологічного захисту; індивідуальне використання антиманіпулятивних механізмів з метою самозахисту від прихованого впливу.

Організація психологічного захисту особистості від маніпуляцій відбувається на трьох рівнях [1; 2; 3]:

1) соціальному (у масштабах суспільства в цілому) – за допомогою регулювання і організації інформаційних потоків (системи розповсюдження інформації в суспільстві) і розповсюдження способів і засобів, певних алгоритмів обробки і оцінки інформації у процесі соціальної взаємодії (від міжособистісного спілкування до масової комунікації);

2) груповому (в рамках різних соціальних груп і різноманітних форм соціальних організацій) – через розповсюдження і використання внутрішньогрупових інформаційних потоків і джерел, а також специфічних для конкретних соціальних груп й організацій способів соціальної взаємодії, обробки і оцінки інформації (групових норм, орієнтацій, переваг певних комунікаторів, регламентація правил та процедур роботи і взаємодії із зовнішніми інформаційними джерелами тощо);

3) особистісному – шляхом формування та розвитку емоційно-вольової стійкості, комплексу захисних механізмів і алгоритмів поведінки, що пов’язане із відмовою від використання певної інформації, джерел її отримання, каналів розповсюдження (наприклад, відмова від рекламної інформації тощо) або повторною перевіркою важливої інформації.

Ураховуючи зазначені рівні, заходи та інші психологічні аспекти протидії маніпулятивним впливам, особистість матиме змогу оптимізувати власну антиманіпулятивну поведінку та успішно організувати роботу щодо реалізації психологічного захисту за будь-яких умов впливу.

Таким чином, із викладеного вище слідує, що в сучасних умовах розвитку інформаційного суспільства засоби масової інформації є найбільш ефективним інструментом для здійснення інформаційно-психологічного впливу на особистість. Психологічний захист, при цьому, реалізується через антиманіпулятивні механізми та передбачає здійснення низки заходів (регулювання інформаційних потоків; розширення способів обробки й оцінки інформації; організація групового та (або) індивідуального захисту тощо). Протидія маніпулятивним впливам на соціальному, груповому та особистісному рівнях забезпечить успішність організації психологічного захисту особистості, що зумовить конструктивність її дій та адекватність поведінки за будь-яких умов.

Література

1. Грачев Г. Манипулирование личностью: Организация, способы и технологии информационно-психологического воздействия / Г. Грачев, И. Мельник. – М. : Из-во РАГС, 1998. – 162 с.

2. Доценко Е.Л. Психология манипуляции / Е.Л. Доценко. – М., 1997. – 344 с.

3. Кара-Мурза С. Манипуляция сознанием / С. Кара-Мурза. – М. : Алгоритм, 2004. – 528 с.

4. Моль А. Социодинамика культуры / А. Моль ; пер. с фр. ; предисл. Б.В. Бирюкова. – Изд. 3-е. – М. : Изд-во ЛКИ, 2008. – 416 с.

5. Толубко В.Б. Складові інформаційної боротьби / В.Б. Толубко, А.О. Рось // Наука і оборона. – 2002. – № 2. – С. 23-28.

6. Толубко В.Б. Інформаційна боротьба (концептуальні, теоретичні, технологічні аспекти) / В.Б. Толубко. – К. : НАОУ, 2003. – 320 с.

УДК 004.2:004.6

Блавацька Н. М.
кандидат технічних наук, доцент
Національна академія СБ України
Юрх Н. Г.
Національна академія СБ України
Хохлачова Ю. Є.
кандидат технічних наук
Національний авіаційний університет
Іванченко Є. В.
кандидат технічних наук, професор
Національний авіаційний університет

УПРАВЛІННЯ ІНФОКОМУНІКАЦІЯМИ

Технологічна революція на межі XX-XXI сторіччя забезпечила передумови переходу людства до принципово нової фази свого розвитку – інфокомунікаційного суспільства. Це стає можливим внаслідок поступового створення глобальної інфокомунікаційної інфраструктури, яка складається з регіональних та національних інформаційних інфраструктур. Однією із найважливіших складових інформаційних інфраструктур є інфокомунікації. Що ж таке інфокомунікації? Інфокомунікації – це сукупність мереж, за допомогою яких служби операторів задовольняють потреби користувачів у послугах.

З погляду сукупності процесів, які супроводжують функціонування такої складової системи, як інфокомунікації, поняття управління інфокомунікаціями є узагальнюючим терміном, який охоплює множину видів діяльності, а саме експлуатацію, технічне обслуговування засобів мереж інфокомунікацій, управління процесами, зв'язаними з наданням послуг, планування, проектування нових мереж і послуг, забезпечення введення та доступності їх.

Метою управління інфокомунікаціями взагалі та автоматизації зокрема є забезпечення оптимального функціонування мереж інфокомунікації відповідно до їх призначення, при якому інфокомунікації виконують необхідні завдання при мінімумі матеріальних, фінансових, фізичних, інтелектуальних витрат.

Основними завданнями управління інфокомунікаціями є забезпечення тривалої якісної роботи засобів і мереж інфокомунікацій у процесі їх постійного вдосконалення та розвитку в умовах різноманітних змінних впливів.

Управління – це багатофункціональний процес, основними функціями якого є: прогнозування (науково обґрунтоване передбачення перспектив розвитку об'єкта управління та можливих його станів до певного моменту); планування (визначення мети розвитку об'єкта управління, методів і шляхів її досягнення); організація роботи (вибір та формування структури виробничого об'єкта й організаційної структури управління, визначення співвідношення між структурними елементами системи); координація та регулювання (забезпечення погодженості дій виконавців та забезпечення підтримки або зміни показників, суттєвих для функціонування об'єкта управління); активізація та стимулювання (спонукання до дії людей за рахунок матеріальних та моральних стимулів); облік (фіксація стану об'єкта управління); контроль (порівняння фактичного та заданого стану об'єкта управління); аналіз (виявлення та аналіз причин відхилень фактичного стану об'єкта управління від заданого). У загальному вигляді відповідно до функціонального призначення види управління мережами та послугами інфокомунікацій можна згрупувати як технічне, функціональне, оперативне та координаційне (адміністративне управління й управління розробками та розвитком) управління.

Переваги, які забезпечуються застосування систем управління, стимулюють їхню розробку і впровадження. Однак існу-

ють певні чинники, які перешкоджають широкому впровадженню систем управління. Вони зумовлені не тільки складністю технічної реалізації цих систем, а й психологічними причинами, тобто людським чинником.

Література

1. Александров В.В. Цифровая технология инфокоммуникации: передача, хранение и семантический анализ текста, звука, видео / В.В.Александров, С.В.Кулешов, О.В.Цветков. – Санкт-Петербург. : Наука, 2008. – 244 с.

2. Средства анализа и управления сетями [Электронный ресурс] Сайт Compnets. – Режим доступа: http://compnets. narod.ru/.

УДК 342.95

Благодарний А. М.
кандидат юридичних наук, старший науковий співробітник
Національна академія СБ України

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ЗАХОДІВ АДМІНІСТРАТИВНОГО ПОПЕРЕДЖЕННЯ ПРАВОПОРУШЕНЬ В ІНФОРМАЦІЙНІЙ СФЕРІ

Одним із актуальних завдань реформування українського адміністративного права є втілення в життя належного і ефективного правового регулювання діяльності органів державної влади, зокрема, діяльності посадових осіб правоохоронних органів, спрямованої на протидію правопорушенням в інформаційній сфері.

Заходи адміністративного попередження можна визначити як комплекс заходів організаційного, психологічного, фізичного та іншого впливу, спрямованих на виявлення та недопущення правопорушень, забезпечення безпеки держави, громадського порядку та особистої безпеки громадян [1, с. 100]. Як зазначав В. Б. Авер’янов, заходи адміністративного попередження виконують особливі правоохоронні функції, які відрізняють їх від інших заходів адміністративного примусу. Окремі запобіжні заходи за своїм характером наближені до заходів адміністративного припинення, у зв'язку з чим у літературі не завжди однозначно

вирішується питання про віднесення певних конкретних заходів до відповідного виду примусу. Основним і єдиним критерієм відмінності є наявність або відсутність правопорушення.

Заходи адміністративного попередження не виконують функції покарання особи, до якої вони застосовуються, що характерно для адміністративних стягнень, тому не потребують встановлення вини порушника як обов'язкової умови застосування [2, с. 421].

Ці заходи є різноманітними, застосовуються у різних галузях суспільного життя й різними суб'єктами (поліцією, органами охорони державного кордону, органами доходів і зборів, СБ України, контрольно-наглядовими органами (державними інспекціями) тощо). Законодавчою базою застосування таких заходів є КУпАП та Митний кодекс України, закони України: "Про Національну поліцію", "Про оперативно-розшукову діяльність", "Про контррозвідувальну діяльність", "Про Службу безпеки України", "Про боротьбу з тероризмом", "Про Державну прикордонну службу України", "Про дорожній рух" тощо.

Для попередження правопорушень в інформаційній сфері найбільше значення, на наш погляд, має застосування таких адміністративно-попереджувальних заходів:

- профілактика правопорушень, яка реалізується із використанням комплексу оперативних та адміністративних заходів. Проект закону України "Про профілактику правопорушень" визначає профілактику як обов'язкову діяльність органів державної влади, місцевого самоврядування, підприємств, установ, організацій незалежно від форм власності, зокрема громадських організацій, спрямовану на виявлення та усунення причин і умов, які сприяють учиненню правопорушень, а також виявлення осіб, схильних до вчинення правопорушень, та застосування заходів до їх виправлення [1, с. 112];

- огляд (особистий огляд і огляд речей, багажу, транспортних засобів, різних об'єктів) як захід адміністративного попередження може застосовуватись різними органами: органами доходів і зборів – у формі огляду та переогляду товарів і транспортних засобів, перевірки системи звітності та обліку товарів, що переміщуються через митний кордон України; Державною прикордонною службою України – огляду в межах прикордонної смуги, контрольованих прикордонних районів транспортних засобів та ін.

Метою огляду є попередження та виявлення правопорушень, забезпечення громадської безпеки. Суть даного заходу по-

лягає у законодавчо закріпленому обов'язку громадян пред'явити на вимогу уповноваженої особи певні предмети (речі), документи. У разі відмови, особу може бути піддано особистому огляду або огляду його речей, транспортних засобів;

- офіційне застереження про неприпустимість протиправної поведінки. Даний захід застосовується до осіб, які систематично порушують громадський порядок, у випадках, коли немає достатніх підстав для притягнення особи до кримінальної чи адміністративної відповідальності. Метою офіційного застереження є не тільки реакція на протиправну поведінку, але й недопущення її продовження в майбутньому. Правові підстави цього заходу встановлені законами України "Про Службу безпеки України", "Про контррозвідувальну діяльність" тощо, порядок застосування визначається відомчими нормативними актами;

- відвідування підприємств, установ та організацій, входження на земельні ділянки, у житлові та інші приміщення громадян. Загалом, здійснювати даний захід уповноважені посадові особи багатьох державних органів для виконання контрольних та наглядових функцій, при цьому мета та об'єкти застосування суттєво різняться, але суть завжди полягає у входженні, проникненні на відповідну територію, об'єкт чи у приміщення [1, с. 102];

- внесення подання про усунення причин і умов, які сприяють вчиненню правопорушень, відрізняється від інших адміністративно-запобіжних заходів головним чином тим, що його мета полягає в запобіганні вчиненню правопорушень не шляхом їх виявлення і наступного припинення чи встановлення особи порушника, а шляхом запобігання вчиненню правопорушень конкретним органом чи посадовою особою в майбутньому завдяки впливу на обставини, які їх породжують [3, с. 95]. Щодо адміністративних правопорушень таке правило встановлено у ст. 282 КУпАП, відповідно до якої орган (посадова особа), який розглядає справу, встановивши причини та умови, що сприяли вчиненню адміністративного правопорушення, вносить у відповідний державний орган, громадську організацію або посадовій особі пропозиції про вжиття заходів щодо усунення цих причин та умов. Про вжиті заходи протягом місяця із дня надходження пропозиції слід повідомити орган (посадову особу), який вніс пропозицію.

Підсумовуючи викладене, слід зазначити, що до основних заходів адміністративного попередження, які мають право застосовувати посадові особи правоохоронних органів України для

протидії правопорушенням в інформаційній сфері, слід віднести такі заходи як: профілактика правопорушень; огляд (особистий огляд і огляд речей, багажу, транспортних засобів, різних об'єктів); офіційне застереження про неприпустимість протиправної поведінки; відвідування підприємств, установ та організацій, входження на земельні ділянки, у житлові та інші приміщення громадян; внесення подання про усунення причин і умов, які сприяють вчиненню правопорушень.

Література

1. Адміністративне право України : підруч. / [А.М. Благодарний, Ю.П. Бурило, І.М. Гриненко та ін. ; за заг. ред. Є.Д. Скулиша]. – К. : Наук.-вид. центр НА СБ України, 2012. – 560 с.

2. Адміністративне право України. Академічний курс: Підр.: У двох томах: Том 1. Загальна частина /Ред. колегія: В.Б.Авер'янов (голова (та інш.) – К.: ТОВ "Видавництво "Юридична думка", 2007. – 591 с.

3. Комзюк А.Т. Заходи адміністративного примусу в правоохоронній діяльності міліції: поняття, види та організаційно-правові питання реалізації / А.Т.Комзюк, О.М.Бандурка (заг. ред.) ; МВС України ; Національний ун-т внутрішніх справ. – Х. : Вид-во Національного ун-ту внутрішніх справ, 2002. – 355 с.

УДК 005.3

Воскресенський В. Б.
Український науково-дослідний інститут спеціальної техніки та судових експертиз СБ України
Скакун О. В.
Український науково-дослідний інститут спеціальної техніки та судових експертиз СБ України
Сивобородько А. В.
Український науково-дослідний інститут спеціальної техніки та судових експертиз СБ України

ПОРТАТИВНІ АНАЛІЗАТОРИ СПЕКТРУ РЕАЛЬНОГО ЧАСУ, ЯК АПАРАТНІ ІНСТРУМЕНТИ ЗАБЕЗПЕЧЕННЯ КОНТРОЛЮ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ТАКТИЧНОМУ РІВНІ

Оперативно-тактичний рівень забезпечення протидій протиправній діяльності в інформаційному просторі потребує належно-

го апаратного контролю [1]. Апаратний контроль загроз несанкціонованого «зняття» конфіденційної службової інформації – це одна із найбільш актуальних задач у сфері інформаційної безпеки держави [2].

В зоні проведення антитерористичної операції контррозвідувальні підрозділи потребують вибору та застосування адекватних засобів контролю та захисту каналів передачі інформації. Таким обладнанням, наприклад, можуть вважатися такі сучасні прилади, як портативні аналізатори спектру реального часу універсального призначення виробництва провідних світових фірм у комплекті з необхідними (в залежності від діапазону робочих частот) антенно-фідерними пристроями [3, 4, 5, 6]. Адже при вкрай обмеженому фінансуванні постає питання найбільш оптимального вибору засобів вимірювальної техніки (ЗВТ) не тільки по критерію «ціна/якість», але і по градації «універсальне призначення/вузькоспеціалізоване призначення».

Необхідно зазначити, що сучасні засоби зняття інформації здійснюють передачу радіосигналів короткими імпульсними пакетами. Формати модуляції, частота та потужність сигналу змінюються в залежності від подій протоколу під управлінням програмного забезпечення. Радіосигнали з’являються нерегулярно. Для цифрового управління радіочастотними пристроями потрібно враховувати не тільки нелінійний характер сигналів, але також, що ці флуктуації відбуваються за дуже короткі проміжки часу.

Отже, потрібно аналізувати радіочастотні сигнали одночасно по часовому проміжку, частоті та модуляції в єдиному скоординованому процесі. Як результат, зростає потреба в ЗВТ, можливості яких відтворюють швидкоплинний характер сучасних сигналів. Необхідні ЗВТ, що працюють в режимі реального часу, які дозволяють виявляти проблему одночасно із зміною сигналу, синхронізуватись по варіаціям сигналу, вести безперервну реєстрацію сигналу та аналізувати вплив змін у всіх областях. Аналізатори спектру в реальному масштабі часу, що виготовляються компанією Aaronia AG (Німеччина) [7], повністю вирішують проблеми подібних вимірювань.

Портативний (з автономним живленням) аналізатор спектру високочастотного та надвисокочастотного діапазонів SPECTRAN HF – XFR розроблений для експлуатації в жорстких умовах. Цей прилад є поєднанням високопродуктивного, надзвичайно міцного

портативного комп'ютера та надчутливого портативного аналізатора в одному корпусі.

SPECTRAN HF – XFR – перший суперпортативний аналізатор реального часу із діапазоном робочих частот від 1 МГц до 9,4 ГГц та смугою пропускання до 200 МГц.

ЗВТ SPECTRAN HF – XFR дає можливість апаратно знаходити спектр радіочастот, що приймається приладом, також апаратно виконується паралельна фільтрація.

Аналізатори спектру Aaronia AG SPECTRAN HF – XFR встановлюють нові стандарти в технології фільтрації. Там де звичайні аналізатори спектру реального часу будуються на використанні аналізу Фур'є, серія XFR базується на запатентованому методі прийому сигналів за допомогою двох налагоджених із зміщенням гребінчастих фільтрів, які створюють багатофазний фільтр. На відміну від звичайного аналізу Фур'є, багатофазний фільтр перекриває декілька інтервалів значень виборок, спираючись на ряд значень частоти. Отже, завдяки попередньо встановленому інтервалу довільна крива фільтра (наприклад, фільтр Гауса) може бути реалізована без обмеження крутизни характеристики.

Іншою особливістю аналізаторів спектру SPECTRAN XFR є функція потокової передачі в реальному часі. На відміну від інших існуючих аналізаторів спектру реального часу, які не можуть виконувати безперервну реєстрацію даних, серія приладів XFR може передавати дані безперервно і зберігати їх постійно в пам'яті комп'ютера, наприклад через високошвидкісний інтерфейс USB.

ЗВТ SPECTRAN HF – XFR має дуже низький рівень власних шумів, що дає можливість ефективно виконувати аналіз надслабких сигналів – до мінус 170 дБм/Гц. Прилад оснащений кольоровим дисплеєм TFT високої розподільної здатності 1366x768 пікселів із сенсорним екраном та потужним 2,5 ГГц центральним процесором Intel Core i5 - 2520M з nVidia Quadro NVS 4200M (512 МБ DDr3) та дактилоскопічним сканером. Обробка сигналів виконується програмованою логічною інтегральною схемою (ПЛІС), яка, крім іншого, має в своєму складі векторний процесор для аналізу та демодуляції сигналів на 150 мільйонів операцій в секунду. Максимальний рівень вхідного сигналу – плюс 40 дБ. ЗВТ оснащений апаратним цифровим фільтром конвертера DDC.

Прилад також відповідає нормам стандартів на випромінювання (ICNIRP, BGV B11, BlmSchV та інше.). Конструкція

SPECTRAN HF-XFR витримує прямий вплив граничних температур, слабкого дощу, пильових бурь, випадкових падінь та багато іншого, наприклад, в бойових умовах, на будівельному майданчику, в шахтах, в навігації, в авіації і т.п. Аналізатор відповідає вимогам стандарту MIL-STD-810F: падіння 4ft Transit Drop, сильний дощ, пильова буря, вибрація, ударостійкість, вологість, соляний туман, висота над рівнем моря, вибухонебезпечна атмосфера, тепловий удар та граничні температури (робоча: від мінус 29 до 63 °C; неробоча: від мінус 50 до 71 °C). Прилад сертифікований по UL1604 на експлуатацію у вибухонебезпечних зонах (класс 1, раздел 2, зоны A, B, C, D).

Після постачання замовнику прилад відразу готовий до функціонування, так як в ньому вже встановлена професійна програма аналізу LCS.

До стандартного комплекту поставки входять: аналізатор спектру для функціонування в польових умовах SPECTRAN HF – XFR, направлена антена HyperLOG 60100, радіальна ізотропна антена OmniLOG 90200, рукоятка пістолетного типу, SMA-кабель (1 м), інструменти (роз'єми) SMA, зарядний пристрій та джерело живлення з адаптерами, детальні настанови з експлуатації.

Зазначений ЗВТ SPECTRAN HF – XFR є повністю інноваційним продуктом та по своїм характеристикам є кращим серед приладів подібного класу.

Аналізатори спектру високочастотного та надвисокочастотного діапазонів SPECTRAN серії HF ідеально пристосовані для вимірювань випромінювання радарів, пристроїв сотового зв'язку, пристроїв несанкціонованого запису («зняття») інформації, UMTS, DECT, WLAN, Wi-Fi, WiMAX, Bluetooth, об'єктів радіо- та телепередаючих центрів, мікрохвильових печей та інше.

Література

1. Полевий В.І. Інструменти забезпечення інформаційної безпеки: стратегічний, функціональний та оперативний рівні. С. 170 – 173. Актуальні проблеми управління інформаційною безпекою держави. Збірник матеріалів науково-практичної конференції (Київ, 19 березня 2015 року). У двох частинах. Київ, Центр навчальних, наукових та періодичних видань Національної академії СБ України, 2015. Ч. 2, 256 с.

2. Воскресенський В.Б., Сивобородько А.В., Ковальчук В.А. Використання аналізаторів спектру реального часу для апаратного контролю у сфері інформаційної безпеки. С. 44 – 48. Актуальні проблеми управління інформаційною безпекою держави. Збірник матеріалів науково-практичної

конференції (Київ, 19 березня 2015 року). У двох частинах. Київ, Центр навчальних, наукових та періодичних видань Національної академії СБ України, 2015. Ч. 2, 256 с.

3. Анализаторы спектра реального времени. Каталог продукции. [Электронный ресурс] // Режим доступу: www.tektronix.com/rsa.

4. Countering threats early on. Каталог продукции. [Электронный ресурс] // Режим доступу: http://www.rohde-schwarz.com.

5. Анализаторы спектра SPECTRAN. [Электронный ресурс] // Режим доступу: http://www.tovsvs.com.ua.

6. Измерительные приборы. Каталог продукции, поставляемой фирмой VD MAIS. Часть 2. Hameg, Micronix. К., 2009, 40 с., издатель НПФ VD MAIS.

7. Realtime spectrum analyzer. [Электронный ресурс] // Режим доступу: www.aaronia.com.

УДК 316.774:355.40:654.1:341.324(477)

Гнатюк С. Л.
кандидат історичних наук
Національний інститут стратегічних досліджень

ВІДНОВЛЕННЯ НАЦІОНАЛЬНОГО ТЕЛЕРАДІОМОВЛЕННЯ НА ТИМЧАСОВО ОКУПОВАНИХ ТА ЗВІЛЬНЕНИХ ТЕРИТОРІЯХ СХОДУ УКРАЇНИ

За даними соціологічних опитувань, телебачення продовжує залишатися основним джерелом отримання медіа-інформації для 83 % мешканців південного сходу України [1]. Тим часом, від моменту початку окупації (весна 2014 р.) й донині під контролем угрупувань «ЛНР-ДНР» перебуває основна частина матеріально-технічного, інфраструктурного і подекуди кадрового ресурсу державного телерадіомовлення Донецької та Луганської областей, а також місцеві оператори кабельного телебачення.

На цій базі на територіях, підконтрольних «ЛНР-ДНР» замість українського контенту налагоджена ретрансляція російських телевізійних каналів та радіостанцій, а також трансляція власних програм. Це стало одним з вирішальних чинників значного розповсюдження серед населення антиукраїнських настроїв та сепаратистської риторики (за різними підрахунками – в межах

70 %) [5, 6]. Повернення контролю над телерадіопростором окупованих територій Сходу країни є обов'язковою умовою їх звільнення та реінтеграції.

Українській державі на даний момент вдалося лише частково виконати завдання повернення контролю над телерадіопростором окупованих та звільнених територій [2], що мають мінімальний ефект через гострий брак матеріально-технічних, фінансових, кадрових ресурсів, бюрократичні перепони, саботаж окремих посадових осіб та працівників, недостатню кількість та якість необхідного для спеціального мовлення контенту, а також через відсутність чіткої, адекватної масштабам проблеми і узгодженої між профільними відомствами та організаціями програми дій. Результатом є фрагментарність й очевидна недостатність заходів, що вживаються.

Нині найбільш затребуваною в зоні конфлікту є інформація про зниклих родичів і знайомих, втрати серед мирного населення і військових, отримання допомоги від місцевої та державної влади благодійних організацій, волонтерів тощо [5]. Очевидно, що за будь-якого сценарію подальшого розвитку подій на Донбасі [3] ця тенденція до зміщення преференцій в бік нагальних питань повсякденного життя залишиться актуальною аж до повної реінтеграції регіону і відновлення в ньому нормального життя.

Відтак, на задоволення саме цих інформаційних запитів в першу чергу має бути зорієнтоване українське мовлення на окупованих територіях. Достатня кількість (і якість) такого контенту на українських каналах вже сама по собі (а) справлятиме позитивний вплив на гуманітарну ситуацію в зоні, (б) підвищуватиме довіру до каналів, (в) збільшуватиме їхній рейтинг і (г) працюватиме на покращення іміджу української держави та уряду серед населення окупованих територій.

У такому контексті більш позитивно будуть сприйматися аудиторією матеріали, присвячені роз'ясненню намірів та політики українського уряду, дій українських військ та ЦВА, різним аспектам життя в Україні, її історії, культури, стосункам з США та ЄС, а також міжнародним темам, які є предметом маніпуляцій у російському пропагандистському дискурсі. Необхідно ретельно слідкувати за якістю і політкоректністю такого контенту, долучаючи до його вироблення тільки перевірених журналістів, медіафахівців та експертів-коментаторів. Контент має бути в основно-

му російськомовним, але орієнтованим при цьому на загальноукраїнське примирення за своєю тональністю та змістом.

Окремим важливим напрямком подальшої роботи має стати розвиток вітчизняної воєнної журналістики. На даний момент розпочато підготовку відповідних кадрів, у тому числі з урахуванням міжнародного досвіду. Зокрема, у травні 2015 року спільними зусиллями Міністерства оборони, Генерального штабу Збройних сил та Міністерства інформаційної політики було запущено програму «Embedded journalism» («Вбудована журналістика»).

З урахуванням того, що територія проведення АТО: а) є зоною воєнно-політичного конфлікту і гострої всебічної кризи; б) знаходиться у фокусі високоефективної пропаганди супротивника; в) значна кількість її населення вже зараз негативно сприймає як українську державу та уряд, так і перспективу реінтеграції; г) самий процес реінтеграції та відновлення обіцяє бути довгим і складним – пропонується:

Розглянути можливість створення у складі НСТУ окремої редакції (робочої групи) програм для Донбасу з покладанням на неї функцій з розробки унікальної програмної концепції мовлення, вимог до контенту з урахуванням специфіки цільової аудиторії, підготовки пропозицій щодо менеджменту, кадрового складу, логістики та інституційно-організаційної моделі закладів спеціального телерадіомовлення на територіях Донбасу.

Розглянути питання щодо створення на юридичній та матеріально-технічній базі Донецької та Луганської ОДТРК єдиної державної регіональної телерадіоорганізації (ТРО), спеціально призначеної для національного мовлення на тимчасово окупованих та суміжних територіях. Провести консультації та переговори з регіональними ТРО іншої форми власності, українськими та зарубіжними мовниками і неурядовими організаціями щодо співпраці та допомоги в сфері обміну контентом, кадрами, досвідом.

Профільним державним відомствам провести спільні консультації з представниками професійних та експертних медіаорганізацій з метою розробки єдиних принципів та правил роботи журналіста в зоні проведення АТО, а також рекомендації загальнонаціональним та регіональним мовникам щодо висвітлення подій на окупованих територіях і в зоні бойових дій.

Розглянути доцільність та можливість фізичного блокування (або виведення з ладу) ключових інфраструктурних та матеріаль-

но-технічних об’єктів і ресурсів, без яких є неможливим організація мовлення на окупованих територіях та використання радіочастотного ресурсу України в їх межах.

Література

1. Звіт Національної ради України з питань телебачення і радіомовлення за 2014 рік. Затверджено рішенням Національної ради від 22 січня 2015 року за № 73 [Електронний ресурс]. - Режим доступу : http://www.nrada.gov.ua/userfiles/file/2014/Zvitna%20informacia/Zvit_2014.pdf

2. Міністерство інформаційної політики України. Звіт щодо відновлення мовлення в зоні АТО. Лютий 2016 року. [Електронний ресурс]. - Режим доступу : http://mip. gov.ua/files/ Presentation/MIP_ vidnovlennya_movlennya_ljutiy2016.pdf

3. Горбулін В. П'ять сценаріїв для україно-російських відносин [Електронний ресурс]. - Режим доступу : http://gazeta.dt.ua/internal/p-yat-scenariyiv-dlya-ukrayino-rosiyskih-vidnosin-_.html

5. Протидія російській інформаційній агресії: спільні зусилля задля захисту демократії. .Аналітичний звіт. – К.: Телекритика, 2015. – С. 41 : [Електронний ресурс]. - Режим доступу : https://dl.dropboxusercontent.com/u/30479341/Telekritika_analytics_propaganda_2015.pdf

6. Донбас Медіа Форум: інформаційний простір та інформаційна політика в умовах війни [Електронний ресурс]. - Режим доступу : http://www.isdpa.org.ua/news/donbas-media-forum-informaciyniy-prostir-ta-informaciyna-politika-v-umovah-viyni

УДК 94(477)

Горєлов В. І.
кандидат історичних наук
Національний університет оборони України
імені Івана Черняховського
Грицюк В. М.
кандидат історичних наук, доцент
Національний університет оборони України
імені Івана Черняховського

ІНФОРМАЦІЙНИЙ ВИМІР «ГІБРИДНОЇ ВІЙНИ»

Нові воєнно-політичні виклики та умови розвитку інформаційного суспільства на зламі тисячоліть змусили військово-політичне керівництво провідних країн світу, військових теоре-

тиків звернутись до розробки такої потужної і складної форми розв'язання сучасних політичних, економічних, воєнних конфліктів як гібридної війни. Комбінації інформаційно-психологічного, економічного та військового протиборства використовувались і раніше. Але гібридність сучасного конфлікту в тому, що питома вага факторів принципово інша. Набагато потужнішою також є використання засобів та особливостей інформаційного суспільства.

До війни такого типу державне та військове керівництво Російської Федерації готувалося завчасно. Теоретичні та прикладні розробки зі стратегії і тактики війни «гібридного» типу здійснювались та здійснюються на основі власного унікального досвіду масштабного збройного конфлікту з потужними, іррегулярними збройними формуваннями. В їх числі перша та друга чеченські війни 1994–2001 рр. («контртерористична операція») на Північному Кавказі, які проходили в умовах загальної ситуації миру у державі та інтенсивного ідеолого-інформаційного супроводження.

Доктринальні документи Російської Федерації не містять терміну «гібридна війна». Російська військово-теоретична думка заперечує власні розробки та використання теорії «гібридної війни», як, зрештою, і військово-політичне керівництво Російської Федерації заперечувало факти військового втручання збройних сил у Криму та на Сході України. Однак реалії свідчать про інше.

Сучасний військовий конфлікт, згідно з новою воєнною доктриною Російської Федерації, є «комплексним застосуванням військової сили, політичних, економічних, інформаційних та інших заходів невоєнного характеру, що реалізуються разом із широким використанням протестного потенціалу населення і сил спеціальних операцій» [6].

Ще на початку 2013 року погляди росіян на зміни в формах і методах ведення бойових дій виклав начальник ГШ ЗС РФ генерал Валерій Герасимов. Інформаційне протиборство взагалі визначалося як наскрізна діяльність на всіх етапах конфлікту [1]. Багато з того, на що звертав увагу генерал Герасимов знайшло практичне відображення у подіях які відбувалися спочатку в Криму, а потім і на Сході України. Тож можна констатувати, що проти України ведеться повноцінна війна: "гібридна" за своєю формою.

Інформаційний складник займає центральне місце серед чинників досягнення ефективності при веденні гібридної війни

[4, 8, 9]. Безперечно, до війни такого типу Росія готувалась давно. Власне, Україна стала полем бою для розгортання гібридних дій. В українському випадку маємо справу не просто з ворожою пропагандою, а з тим, що фахівці-інформаційники слушно характеризують як "війну смислів/сенсів" (початок якої можна умовно віднести до 2006–2007 рр.). Для ретрансляції цих смислів задіяно всю множину каналів донесення інформації. Основним структурним елементом у цій війні стають симулякри — образи того, чого в реальності не існує. Прикладами таких симулякрів є: "фашисти в Києві", "звірства каральних батальйонів", "розіп'яті хлопчики", використання Україною заборонених озброєнь. Стратегічна мета експлуатації цих симулякрів — замінити об'єктивні уявлення цільових груп про характер конфлікту тими "інформаційними фантомами", які потрібні агресору.

Відповідно, чи не перше, що зробили різноманітні "ополченці" та "зелені чоловічки" на окупованих територіях, — це відключили українські телеканали і масовано включили російські. Формування єдиного й повністю контрольованого інформаційного простору – очевидна стратегія розгортання інформаційного складника конфлікту з боку агресора.

Важливо відзначити, що Російська Федерація розгорнула один із фронтів "гібридної війни" і проти громадян своєї держави, формуючи там модель поведінки, яка багато в чому улягає месиджам федеральної преси. Небажання значної кількості громадян Росії подивитися на речі під іншим кутом зумовлене і страхом виникнення когнітивного дисонансу між дійсністю, формованою російськими ЗМІ, та реальними подіями.

Ще один важливий інформаційний фронт – зовнішній. Масштаби діяльності "фондів", "культурних товариств", "аналітичних центрів" і просто "експертів" проросійської спрямованості в Європі, а також діяльність каналу RT справді значні. Навіть тут загальна концепція "гібридної війни" "по-російськи" дається взнаки: частину таких експертів просто вигадують, а від їх імені публікують необхідні коментарі та висновки.

Важливим трансграничним простором ведення інформаційного протиборства стала мережа Інтернет. Різноманітні реальні й удавані "хактивісти", "кіберпартизани", "кіберополчення", а також спеціальні підрозділи різних безпекових відомств для ведення протистоянь у кіберпросторі — всі вони стають важливим

елементом кібератак, а також ведення спеціальних психологічних операцій у соціальних мережах та в мережі Інтернет загалом. Однак повністю завоювати інформаційний простір Росії не вдалося, — чимало пропагандистських заяв із боку російського телебачення з української тематики швидко спростовували самі інтернет-користувачі, які дедалі частіше стають "рядовими інформаційних воєн".

Висновки. Протистояти Росії в "гібридній війні" буде важко. Противник до ведення інформаційної війни проти України задіяв значні ресурси, готувався до цього протистояння роками. Однак ми мусимо навчитися асиметрично протидіяти викликам гібридної війни. Більш цілісною має стати реакція і на інформаційну агресію.

Література

1. Герасимов В. Ценность науки в предвидении [Електронний ресурс] / В. Герасимов. – Режим доступу: http://vpk-news.ru/articles/14632
2. Горбулін В. "Гібридна війна" як ключовий інструмент російської геостратегії реваншу [Електронний ресурс] / Володимир Горбулін – Режим доступу: http://gazeta.dt.ua/internal/gibridna-viyna-yak-klyuchoviy-instrument-rosiyskoyi-geostrategiyi-revanshu-_.html
3. Іващенко А.М., Шпура М.І. Еволюція поглядів на стратегію сучасного гібридного конфлікту та сценарії протидії гібридним загрозам / Іващенко А.М., Шпура М.І. // Збірник наукових праць ЦВСД НУОУ. – 2015. – №1(53). – С. 18–23.
4. Корнієнко С. Путін веде в Україні гібридну війну – генерал Каппен [Електронний ресурс] / С. Корнієнко. – Режим доступу: http://www.radiosvoboda.org/content/article/25363591.html
5. Леонов В.В. Війни XXI століття: технології “гібридної війни” / Леонов В.В., Ворович Б.О., Сівоха І.М. // Збірник наукових праць ЦВСД НУОУ. – 2015. – №1(53). – С. 24–30.
6. Воєнна доктрина Російської Федерації / Затверджена президентом Російської Федерації 25 грудня 2014 року
7. Телелим В.М. Планування сил для виконання бойових завдань у “гібридній війні” / Телелим В.М., Музичинеко Д.П., Пунда Ю.В. // Наука і оборона. – 2014. – №3. – С. 30–35.
8. FT: «Новое российское искусство войны» [Електронний ресурс]. – Режим доступу: http://www.vedomosti.ru/politics/news/32774201/ft-novoe-rossijskoe-iskusstvo-vojny
9. Vandiver John. SACEUR: Allies must prepare for Russia ‘hybrid war’ [Електронний ресурс] / John Vandiver. – Режим доступу: http://www.stripes.com/news/saceur-allies-must-prepare-for-russia-hybrid-war-1.301464.

УДК 004.946

Грищук Р. В.
доктор технічних наук, старший науковий співробітник
Житомирський військовий інститут імені С. П. Корольова

СПОСІБ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ СТАРТАПУ ВІРТУАЛЬНИХ СПІЛЬНОТ У СОЦІАЛЬНИХ ІНТЕРНЕТ-СЕРВІСАХ ЗА ПРИНЦИПОМ КРИТИЧНОЇ МАСИ

Постановка проблеми в загальному вигляді. Роль соціальних інтернет сервісів (СІС) у процесі становлення громадянського суспільства постійно зростає [1]. Особливе місце в СІС займають віртуальні спільноти (ВС) – групи агентів, комунікація яких здійснюється за особистісними або груповими інтересами їх учасників [2, 3]. Останнім часом великий та малий бізнес також успішно використовує СІС для просування на ринок власних брендів [4]. Але в умовах жорсткої ринкової конкуренції не зважаючи на бізнес потужність бренду, проблема стартапу його віртуальної спільноти у СІС залишається актуальною.

Аналіз останніх досліджень і публікацій показав, що концепція стартапу ВС у СІС залежить від багатьох умов. До основних з них можна віднести: правильність підготовки ВС до розкручення; підтримання стабільної кількості агентів, які вступають до ВС за визначений проміжок часу; обов’язкове утримання 10% бар’єру носіїв ідеї ВС; своєчасне розміщення якісного контенту тощо та досягнення ВС критичної маси. При чому, додержання останньої із зазначених умов, зокрема, і визначає успіх стартапу ВС у СІС. Аналіз академічної літератури за темою дослідження показав, що проблема стартапу ВС у СІС за принципом критичної маси до сьогодні не опрацьована ні теоретично, ні методично. Переважна більшість досліджень, зосереджена на вивченні питань розробки, дослідження та аналізу моделей СІС. Також у ряді наукових публікацій, увага акцентується на вивченні питань, пов’язаних з суспільно-гуманітарною роллю СІС. Таким чином, тема, що досліджується, залишається не розкритою.

Метою дослідження є підвищення ефективності стартапів ВС у СІС за рахунок розроблення відповідного способу оцінювання ефекту за принципом критичної маси.

Викладення основного матеріалу дослідження. Дамо такі дефініції критичній масі ВС у СІС та стартапу [4, 5]: критична маса M ВС $c \in C$ у СІС $g \in G$ – це мінімально необхідна кількість агентів $a_{\min} \in A$, що споживають та генерують новий контент $k \in K$, внаслідок чого забезпечується активізація віральної (вірусної) петлі v й саморозвиток e ВС; стартап ВС у СІС – це новостворена віртуальна спільнота $c' \in C$ у СІС $g \in G$, яка розкручується в умовах жорстких ресурсних обмежень; віральна петля v – це швидкість розповсюдження контенту між агентами $a \in A$ ВС $c' \in C$ у СІС $g \in G$; критичний стан ВС – це стаціонарний стан ВС $c' \in C$ у СІС $g \in G$, за якого кількість агентів $a_{const} \in A$ не змінюється в часі $t \in T$; критичність – умови, за яких у віртуальній спільноті $c' \in C$ у СІС $g \in G$ підтримується механізм саморозвитку e. Таким чином, проблема стартапу ВС у СІС виникає тоді, коли виникає потреба швидкої активації віртуальної петлі, що забезпечить саморозвиток спільноти в умовах жорстких ресурсних обмежень. Але на практиці, вирішення означеної проблеми пов'язане з вирішенням протиріччя, яке полягає в задоволенні потреби щодо приведення у відповідність високих вимог, які висуваються до темпів активізації віртуальної петлі новостворюваної ВС при залученні мінімальної кількості агентів, до жорстких ресурсних обмежень, що встановлюються. Тому, вирішити виявлене протиріччя пропонується на онові принципу критичної маси. Оскільки на сьогодні не існує універсального способу для визначення критичної маси для стартапу ВС у СІС, то в першому наближенні принцип критичної маси у формалізованому вигляді, сформулюємо наступним чином:

$$\left\langle \min(M) : a \geq a_{\min}, o \geq o_{\min} \right\rangle, \tag{1}$$

де $a_{\min}$ – мінімально необхідна кількість агентів, що забезпечують вдалий стартап ВС c у СІС g, $a_{\min} \in A$, $c' \in C$, $g \in G$; $o_{\min}$ – мінімальні витрати ресурсів, яких достатньо для вдалого стартапу ВС c' у СІС g, $o_{\min} \in O$.

У прямій постановці задача визначення критичної маси (1) ВС є некоректною. Для її регуляризації скористаємося метрикою самоподібності – показником Херста [6]

$$H = \frac{\log(R/S)}{\log(m * \pi/2)}, \tag{2}$$

де H – показник Херста; S – середньоквадратичне відхилення ряду спостережень; R – розкид накопиченого відхилення; m – кількість спостережень.

Величина показника (2) опосередковано відповідає на питання чи досягла ВС критичної маси $\min(M)$ за мінімальної кількості агентів $a_{\min}$ та виділених ресурсів $o_{\min}$, чи ні.

У доповіді наводяться приклади застосування розробленого способу для оцінювання ефективності стартапу ряду ВС у CIChttps://ru.wikipedia.org/wiki/Facebook. Приведено аналіз одержаних результатів, сформульовано відповідні рекомендації. Показано приклади вдалого та невдалого стартапів [7, 8].

Висновки та перспективи подальших досліджень. Вперше для оцінювання ефективності стартапу ВС у СІС запропоновано використовувати принцип критичної маси. З цією метою розроблено відповідний спосіб та розкрито його теоретичні й методологічні засади. Доведено, що додержання принципу критичної маси забезпечує стабільний розвиток динаміки ВС, що в майбутньому виключає зменшення кількості їх агентів.

Таким чином, стартап ВС у СІС за принципом китичної маси, виступає запорукою вдалого просування нових бізнес-проектів. У подальшому планується дослідити залежність критичної маси ВС від різних умов, які впливають на ефективність її розкручення.

Література

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

2. Грищук, Р. В. Технологічні аспекти інформаційного протиборства на сучасному етапі / Р. В. Грищук, І. О. Канкін, В. В. Охрімчук // Захист інформації. – 2015. – Том 17. – № 1 – С. 80–86.

3. Грищук Р. В. Мобільні соціальні інтернет-сервіси як один із різновидів масової комунікації на сучасному етапі / Р. В. Грищук, Ю. Г. Даник, О. В. Самчишин // Безпека інформації – 2015. – Том 21. – № 1. – С. 16–20.

4. Путь от 0 до критической массы пользователей в стартапах : как набрать критическую массу пользователей и не провалиться? [Электронный ресурс] / А. Завялов. – Режим доступа к мат. : https://medium.com/@azavyalov/0-d563fd2f2bab.

5. Грищук Р. В. Стартап віртуальних спільнот у соціальних мережах за принципом критичної маси / Р. В. Грищук // Захист інформації. – 2015. – Спеціальний випуск – С. 19–25.

6. Найман, Э. Расчет показателей Херста с целью выявления трендовости (персистентности) финансовых рынков и макроэкономических индикаторов /Э. Найман // Економіст. –2009. – №10. – С. 18–28.

7. Грищук Р. В. Особливості організації та ведення моніторингу електронних засобів масової комунікації / Р. В. Грищук, О. В. Манько, І. О. Орищук // Інформаційна безпека. – Луганськ : СНУ ім. В. Даля. – 2014. – С. 10–15.

8. Грищук Р. В. Прогнозування динаміки поширення контенту й запитів на нього, за даними контент-аналізу повідомлень у соціальних інтернет-сервісах / Р. В. Грищук, К. В. Молодецька // ІІ Міжнар. наук.-практ. конф. ["Актуальні питання забезпечення кібербезпеки та захисту інформації"] (Закарпатська область, Міжгірський район, село Верхнє Студене, 24-27 лют. 2016 р.). – К. : Видавництво Європейського університету, 2016. – С. 58–59.

УДК 94 (477)

Гуз А. М.
доктор історичних наук, професор
Національна академія СБ України

ФАЛЬСИФІКАЦІЯ ІСТОРІЇ ЯК ЗАСІБ ІНФОРМАЦІЙНОЇ ВІЙНИ РОСІЇ ПРОТИ УКРАЇНИ

Події, які нині відбуваються в Україні, нікого не залишають байдужими. Розуміння того, що одним із потужних засобів агресії є інформаційна зброя, спонукало до розвіюванню історичних міфів російської пропаганди.

Патріотизм кожного українця має спиратися на стійкі переконання, фундаментом якого є знання власної історії. Озброєні знаннями людини і, зокрема, студенти, ніколи не піддадуться на ганебні й цинічні провокації проросійських ЗМІ та ідеологів, і завжди зможуть під машкарою «братньої турботи» викрити хижацьку політику Росії стосовно України. Науковці та викладачі на даному етапі спроможні зробити те, що на інформаційному фронті допоки, на превеликий жаль, не вдається журналістам і політикам, а саме: переконливо й вичерпно, спираючись на історичні дослідження та факти, донести до молодого покоління правду про вельми непростий шлях України до власної незалежності.

Уважне й неупереджене вивчення наукових джерел, особливо не пов'язаних з офіційною Московською (чи то часів Російської імперії, чи то періоду СРСР) переконливо засвідчує, що упродовж усієї історії співжиття Росія вела проти України та українства інформаційну війну. На жаль, Україна у ній часто програвала і програє досі, чому сприяють і вигадані росіянами історичні міфи, спрямовані, насамперед, на маніпуляцію суспільною свідомістю. Результат саме цього деструктивного впливу ми нині наочно бачимо у Криму та на Донбасі. Фальсифікація історії - ось засіб інформаційної війни Росії проти України. Прикладів фальсифікації історії України російськими вченими безліч – від походження Київської Русі до подій Революції Гідності, анексії Криму та агресії на Донбасі. У нашому дослідженні ми спробуємо розвінчати хоча б деякі з побрехеньок російської пропаганди.

Відома давня російська мантра про те, що Україна – це «Окраина» Росії. Уперше Русь називають Україною 1187 року в Іпатіївському літописі. В ньому йдеться саме про Україну, а не «Окраїну». Сучасна Україна є правонаступницею давньоруської держави слов'ян Київська Русь (історію і назву, якої вкрали північні сусіди, бо власної не мали аж до середини XVIII ст.). Саме про неї в Іпатіївському літописі читаємо: ...«и плакашеся по нем все Переяславце ... бе бо князь добр и крепок на рати ... и в нем же Украина много постона...». Описується загибель переяславського князя Володимира Глібовича під час походу на половців. Цей же літопис оповідає про князя Ростислава Берладника, котрий відвідав «Україну Галицьку». В Галицько-Волинському літописі є такі рядки про князя Данила Галицького: «забрал Берестье, и Угровск, и Верещин, и Столпье, и Комов, и всю Украину» [1].

Назва Україна походить від українського дієслова «вкривати» – «вкрити» – «покривати», «вкраина» і свідчить про те, що в той час міста-поліси могли забезпечити захист, «укрити» певну територію. Тобто, та частина території, землі, яка була «вкрита» містом, і ставала україною. Тобто, слово «Україна» – це стародавнє «Держава», яке походить від дієслова держати (утримувати). В німецькій мові існує слово «Inland», яке дослівно переводиться «Вкраїна» і означає «своя земля».

Стосовно «окраїни», варто зазначити, що Київ – культурний центр Русі, не міг бути «окраїною» за визначенням. Інша справа Залісся, Московія на той час дійсно була окраїною відомого Руського світу. Назва «Україна» стала часто вживатися в побуті, коли в українців виникла можливість задуматися про свою краї-

ну, про відновлення Русі, своєї країни, держави, державності, країни – України! Однак, політичну назву Русь – Україна отримала лише в XVII-XVIII ст. Творець першої у світі конституції Пилип Орлик писав: «Ucraina», «inUcrainam», «на Украйне», «Киев и иные украинские городы». Українці не стали «малороссами», не стали і «хохлами» в XIX столітті, бо були найбільшою національною общиною, найбільш густонаселеною колонією Російської імперії.

Ще одна брехня про те, що української мови не існує, а є лише малоросійське «нарєчіє» великоросійської. Цю брехню розвіюють такі тези: «Наслідком єдності походження всіх східнослов'янських мов від «руської», «русьской» – від «Русь» мови, їх близькості став той факт, що «руськими» тривалий час продовжували називати кожну із східнослов'явнських мов… У заголовку Острозької біблії зазначається: «Біблія… по языку словенску», але в розмовній мові її дуже часто називали «руською». Як бачимо йшлося про руську мову (не «русскую»), під якою розуміли саме українську, тому що ця мова, яку ми знаємо сьогодні, і є: руська мова, якою написаний статут Великого Князівства Литовського і Руського; руська мова Мелетія Смотрицького, українського просвітителя, котрий працював у Вільно і Києві, автора виданої в 1619 році в Єв'ї «Грамматіки славєнскія правильноє синтагма»; руська мова «Грамматіки словенска» Лаврентія Зизанії, який відрізняв московську церковно-словянську мову, а насправді – болгарську від нашої руської (тобто української). «Словенски переводимъ: Удержи языкъ свой от зла и устнъ своъ же не глатилсти. Руски истолковуемъ: Гамуй языкъ свой от злого и уста твои нехай не мовятъ здрады». Тобто, «гамуй», «нехай», «мовять», «здрады» – це українські слова («руські») [1]. Очевидно, що автор «Грамматіки словенска» руською мовою вважав сучасну українську, в той період спільну для українців і білорусів.

Варто зазначити, що найчисельнішою етнічно-мовною групою після 1569 року, яка виразно домінувала на теренах Великого Литовського Князівства було населення, яке розмовляло руською (українською) мовою, поляки їх називали русини. Мовознавці доводять, що процес поділу давньоруської мови на окремі мови – білоруську й українську розпочався в кінці середньовіччя. Саме тоді руська (українська) мова була урядовою мовою Великого Литовського Князівства, основна маса населення якого розмовляло цією мовою [2]. Її використовували у канцелярії великих князів, в судочинстві в XVI-XVII ст. Руською мовою також про-

ведено кодифікацію права Великого Князівства, тобто три Литовські статути – 1529, 1566 і 1588 р. Правлячі еліти в Литві довгий час вважали руську мову критерієм власної державності в рамках федеративної Речі Посполитої. В тексті ІІІ Литовського статуту, що діяв у Великому Литовському Князівстві до кінця XVIII ст. «не чужою якоюсь мовою, але своєю власною (руською) права списані маємно» [2]. А ІІ Литовський статут (руський) діяв в українських воєводствах до поділів Речі Посполитої. Шляхта руського походження часто боронили урядовий статус руської мови від наступу польської (1606, 1632, 1638). Польську мову визнали на теренах Великого Литовського Князівства лише в 1697 р. Навіть після цього шляхта довгий час залишається двомовною.

Крім того, варто зазначити, що попри невтілену в життя Гадяцьку угоду 1658 року, аж до кінця існування Речі Посполитої її володарі користувалися титулатурою «короля Польщі, великого князя литовського, руського… та ін..», що походила з пізньосередньовічної офіційної назви Литовської держави – Великого Князівства Литви, Русі і Жмуді.

Сучасна російська мова справді є результатом серйозної роботи, підсумок якої нам відомий, сучасною російською заговорили тільки на початку XX століття.

І останній закид російським фальсифікаторам і пропагандистам: чому ж Москва забороняла українську мову, якщо її не було? Наводимо у хронологічній послідовності усі приписи щодо заборони української мови: 1627 – указ царя Олексія Михайловича: зібрати усі книжки українською мовою в церквах і спалити; 1690 – указ московского патриарха Іокима про заборону української писемності; 1709 – указ Петра І про заборону друку книг українською мовою; 1748 – указ Синоду про заборону викладання у школах українською мовою (в Україні тоді закрили 866 шкіл, притому, що в Московії їх не було й сотні); 1763 – указ Катерини ІІ про заборону викладання українською мовою в Києво-Могилянській академії; 1863 – Валуєвский (на той час – міністр внутрішніх справ Росії) циркуляр: «Украинского языка нет и не было, а кто этого не признает – враг России»; 1876 – Емський указ Олександра ІІ про заборону ввозити на територію Російської імперії з-за кордону книги українською мовою, видавати українською оригінальні твори й робити переклади з іноземних мов, тексти для нот, друкувати будь-які книги українською мовою, ставити українські театральні вистави, влаштовувати концерти з українськими піснями, викладати українською мовою в початко-

вих школах; 1888 – указ Олександра ІІІ про заборону використання української мови в державних установах і хрещення дітей українськими іменами; 1914 – указ Миколи І про заборону української преси; 1938 – указ наркомосвіти про обов'язкове вивчення в українських школах російської мови; 1958 – постанова пленуму ЦК КПРС про перехід усіх українських шкіл на російську мову навчання [3].

Відновити українську мову, повернути Україні Україну вдалося лише після загибелі імперії. Але знову на заваді розбудови української незалежності стоять імперські амбіції, зброя і пропагандистка машина Москви. А перемогти їх можуть лише правда, лише гідність, мужність, волелюбність і незламність українського народу.

Література

1. Білінський В. Б. Країна Моксель, або Московія. Роман-дослідження / В. Б. Білінський. Кн. 1. – К. : Видавництво імені Олени Теліги, 2009. – 376 с.

2. Польща – нарис історії. – Варшава, 2015. – 366 с.

3. Чеславский О. Законны ли претензии России на наследие Руси-Украины? / О. Чеславский // http://obozrevatel.com/person/oleg-cheslavskij.htm.

УДК 355.011 (477)"2014"

Євсєєв І. Г.
Національний університет оборони України
імені Івана Черняховського
Скрябін О. Л.
кандидат історичних наук
Національний університет оборони України
імені Івана Черняховського

ЩОДО ЗАЛУЧЕННЯ ЗБРОЙНИХ СИЛ УКРАЇНИ В ПРОВЕДЕННІ АНТИТЕРОРИСТИЧНОЇ ОПЕРАЦІЇ В ДОНЕЦЬКІЙ ТА ЛУГАНСЬКІЙ ОБЛАСТЯХ У 2014 РОЦІ: ПРАВОВИЙ АСПЕКТ

Через агресивні дії незаконних збройних формувань в окремих районах Донецької та Луганської областей, їх підтримку Російською Федерацією (далі – РФ), з метою забезпечення терито-

ріальної цілісності України та її державного суверенітету керівництво держави прийняло рішення про проведення антитерористичної операції (далі – АТО) на цих територіях із залученням Збройних Сил України [1]. Керуючись положеннями Конституції України [2], Закону України "Про боротьбу з тероризмом" [3] 14 квітня 2014 року Указом Президента України, було введено в дію рішення Ради національної безпеки і оборони України "Про невідкладні заходи щодо подолання терористичної загрози і збереження територіальної цілісності України" [4]. Для безпосереднього управління силами і засобами, які залучалися до проведення АТО, був створений оперативний штаб на чолі з керівником Антитерористичного центру при Службі безпеки України (далі – АТЦ).

Збройні Сили України на початку проведення антитерористичної операції керувались наявною на той час законодавчою та нормативно-правовою базою: положеннями Конституції України, законів України, указів Президента України та інших нормативно-правових актів [2-7]. Водночас, незважаючи на наявність низки законодавчих та нормативно-правових актів, які регулювали правові засади участі Збройних Сил України в антитерористичній операції, їх практична реалізація виявилася непристосованою до тих реальних та потенційних загроз, що виникали в ході проведення АТО. Так, вже на початку збройного протистояння між силовими структурами держави і незаконними збройними формуваннями (далі – НЗФ) стало очевидним, що чинне законодавство України у боротьбі з тероризмом було орієнтованим переважно на протидію поодиноким терористичним актам щодо окремих об'єктів і осіб з боку невеликих груп терористів.

У подальшому недосконаліть вітчизняного законодавства у цій сфері відчутно проявилась у змісті і обсязі завдань, які мала виконувати українська армія в антитерористичній операції, оскільки вони обмежувались лише забезпеченням захисту від терористичних посягань на її об'єкти, зброю і майно.

У реальності державі треба було простояти масштабній агресії РФ, яка використовувала НЗФ, а також направляла озброєних найманців. Найгіршим стало те, що ця недосконаліть антитерористичного законодавства України не дозволяла проводити Збройним Силам України та іншим суб'єктам боротьби з тероризмом координацію масштабних заходів з бойового застосування їх частин і підрозділів.

Необхідність адекватного протистояння незаконним збройним формуванням вимагала законодавчого розширення меж антитерористичної операції, зокрема, повноважень частин, підрозділів та окремих військовослужбовців Збройних Сил України, інших суб'єктів боротьби з тероризмом при виконанні поставлених завдань або запровадження воєнного стану в районі її проведення.

З метою покращення організаційних засад боротьби з тероризмом, удосконалення взаємодії між Збройними Силами України та іншими суб'єктами цієї діяльності, забезпечення безпеки населення та припинення діяльності НЗФ, підготовці та проведенні інших антитерористичних заходів, посилення персональної відповідальності керівників задіяних державних установ за виконання окремих доручень при проведенні антитерористичних операцій на державному рівні [8, 9] були вжиті наступні заходи:

- внормовано умови залучення і використання сил і засобів органів військового управління, з'єднань, військових частин Збройних Сил України, інших суб'єктів боротьби з тероризмом, а саме: особового складу та спеціалістів окремих підрозділів, військових частин, зброї, бойової техніки, спеціальних і транспортних засобів, засобів зв'язку, інших матеріально-технічних засобів щодо припинення діяльності НЗФ;

- посилено відповідними фахівцями склад МКЦ АТЦ;

- удосконалено до вимог часу організаційні основи боротьби з тероризмом;

- налагоджено повноцінне функціонування АТЦ та МКК. Зокрема, за рішенням керівника АТЦ до широкомасштабних операцій у районі їх проведення стали залучатись та використовуватись всі наявні сили та засоби Збройних Сил України та інших суб'єктів боротьби з тероризмом.

Таким чином, правове регулювання діяльності Збройних Сил України в антитерористичній операції у 2014 році відбувалось поступово (протягом квітня – грудня). Його результатами стали: по-перше, законодавче закріплення додаткових повноважень Збройних Сил України щодо припинення діяльності НЗФ, по-друге, підвищення якості взаємодії та спільних дій Збройних Сил України та інших суб'єктів боротьби з тероризмом в зоні проведення антитерористичної операції, по-третє, збільшення повноважень керівництва АТЦ на залучення та використання сил і засобів суб'єктів боротьби з тероризмом [3, 5, 7].

Література

1. Звернення в.о. Президента України, Голови Верховної Ради України Олександра Турчинова до народу України 13 квітня 2014 року [Електронний ресурс]. – Режим доступу : http://rada.gov.ua/news/Top-novyna/91409.html.

2. Конституція України: від 28 червня 1996 р. // Відомості Верховної Ради України. – 1996. – № 30. – Ст. 141.

3. Про боротьбу з тероризмом : Закон України: від 20 березня 2003 р. // Відомості Верховної Ради України. – 2003. – № 25. – Ст. 180.

4. Про рішення Ради національної безпеки і оборони України від 13 квітня 2014 року "Про заходи щодо посилення боротьби з тероризмом в Україні": Указ Президента України від 14 квітня 2014 р. № 405/2014 // Офіційний вісник Президента України. – 2014. – № 14. – Ст. 745.

5. Про Збройні Сили України: Закон України від 6 грудня 1991 р. // Відомості Верховної Ради України. – 1992. – № 9. – Ст. 108.

6. Про Антитерористичний центр: Указ Президента України: від 11 грудня 1998 р. № 1343/98 // Офіційний вісник України. – 2010. – № 7. – Ст. 300.

7. Про Положення про Антитерористичний центр та його координаційні групи при регіональних органах Служби безпеки України: Указ Президента України від 14 квітня 1999 р. № 379/99 // Офіційний вісник України. – 2010. – № 7. – Ст. 302.

8. Про внесення змін до законів України щодо боротьби з тероризмом : Закон України: від 5 червня 2014 р. // Відомості Верховної Ради України. – 2014. – № 29. – Ст. 946.

9. Про внесення змін до деяких указів Президента України: Указ Президента України: від 16 грудня 2014 р. № 934/2014 // Офіційний вісник України. – 2014. – № 101. – Ст. 2971.

УДК 005.3

Клименко С. В.
кандидат юридичних наук, доцент
Національна академія СБ України

ОКРЕМІ ПИТАННЯ КРИМІНАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ ЗА ПОСЯГАННЯ НА ІНФОРМАЦІЙНИЙ СУВЕРЕНІТЕТ

Постійне зростання впливу інформаційної сфери характерне для сучасного етапу розвитку суспільства. Саме тому дослідженням ефективності державної інформаційної політики із забезпе-

чення інформаційної безпеки останнім часом приділяється значна увагу науковців всього світу.

Останнім часом Україна зіштовхнулася з цілим комплексом заходів інформаційного впливу з боку іноземних держав, які були спрямовані на 1) дезінформування та маніпулювання; 2) пропаганду; 3) диверсифікацію громадської думки; 4) психологічний тиск; 5) поширення чуток.

О. Руснак зауважує, що важливим є обґрунтування відмінностей у правовій кваліфікації втручання іноземних держав та міжнародних організацій у внутрішні справи України з використанням засобів масової інформації та діяльності представників зарубіжних ЗМІ, які здійснюють спеціальні інформаційні операції з метою здійснення вигідного впливу на внутрішню та зовнішню політику нашої держави. У сучасних умовах найпоширенішими ви- дами діяльності з метою завдання шкоди національній безпеці у формі вигідного впливу іноземних держав з використанням зарубіжних ЗМІ є: – намагання маніпулювати суспільною свідомістю шляхом поширення спеціально підібраної, недостовірної, неповної або упередженої інформації. За результатами вдалої маніпуляції формується лояльність населення до політики іноземних держав, спрямованої на завдання шкоди національним інтересам України, досягається пасивність індивідів, введення їх у стан політичної бездіяльності, що нейтралізує потенціал народу у справі захисту його суверенітету [1, с. 148].

Життєва практика переконує, в необхідності запровадження цілого комплексу заходів спрямованих на нейтралізацію суспільно небезпечних посягань, в тому числі і в сфері посягання на інформаційний суверенітет держави. Одним із таких заходів стало створення у 2014 році Міністерства інформаційної політики, який має стати головним органом у системі центральних органів виконавчої влади у сфері забезпечення інформаційного суверенітету України, зокрема з питань розповсюдження суспільно важливої інформації на Україні і за її межами, а також забезпечення функціонування державних інформаційних ресурсів.

Беззаперечно значне місце в системі таких заходів має посісти і кримінально-правова політика держави спрямована на протидію посяганням на інформаційний суверенітет держави. Допомогу в реалізації такої політики може надати досвід окремих зарубіжних країн. Іноземні держави доволі активно застосовують

кримінально-правові засоби протидії посяганню на інформаційний суверенітет держави. Так, КК Швеції в ст. 13 встановлює кримінальну відповідальність особи, яка отримує гроші або інше майно від іноземної держави або від будь-якої особи за кордоном, що діє в інтересах іноземної держави, з метою, за допомогою публікації або поширення письмових документів або іншими способами, вплинути на громадську думку таким чином, щоб порушити будь-яку з основ форми державного правління Королівства або будь-який інше важливе питання безпеки Королівства, рішення якого знаходиться в компетенції Парламенту або Уряду.

Аналогічна норма передбачена і в КК Данії, де в § 102 (глава 12 - злочини проти незалежності та безпеки держави) визначено, що будь-яка людина, яка вчинює пропаганду на користь будь якої ворожої влади з якою Данія перебуває в стані війни, включаючи такі дії, як видавницьку справу, публікування, редагування, для просування ворожих інтересів, оплата істотної фінансової допомоги пропаганди згаданої вище.

Аналогічні кроки в цьому напрямку необхідно здійснити і в Україні. На сьогодні будь-які заклики до повалення чи зміни конституційного ладу, захоплення державної влади, а також до зміни меж державного кордону України вже є кримінально караними відповідно до положень ст. ст. 109 та 110 КК України. Об'єктивною стороною даних злочинів передбачено здійснення публічних закликів чи розповсюдження матеріалів із закликами до зміни меж державного кордону, захоплення державної влади чи повалення конституційного ладу. Проте, в інформаційному полі України, включаючи і соціальні мережі, існує безліч публікацій, які не містять прямих закликів до вказаних дій, проте негативно впливають на формування громадської думки щодо порушення основних положень Конституції України, які стосуються територіальної цілісності та суверенітету держави. Беззаперечно, свобода слова в Україні гарантуються Конституцією. Проте, фінансування таких дій іноземними державами, перетворює їх у надійний механізм посягання на суверенітет та незалежність України.

Вчинення таких дій громадянами України може підпадати під чинну редакцію ст. 111 КК України, де мова йде про надання громадянином України допомоги іноземній державі чи іноземній організації в проведенні підривної діяльності проти України. Проте, як буди із вчиненням таких дій іноземними громадянами, чи особами без громадянства.

На наш погляд вирішити це питання можна за допомогою встановлення кримінальної відповідальності за такі дії в КК України. Зокрема передбачити в КК України кримінальну відповідальність за поширення будь-яким способом в інтересах іноземної держави чи організації інформації, яка формує громадську думку щодо зміни меж території України, зміни чи повалення конституційного ладу України, а також захоплення державної влади.

Література

1. Руснак О. В. Медіа-інформаційна безпека України: правові аспекти / О. В. Руснак // Стратегічні пріоритети. – 2013. – № 3 (28). – С. 147-150.

УДК 005.3

УДК 005.3

Коропатнік І. М.
Військовий інститут
Київського національного університету імені Тараса Шевченка

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ВИКОНАННЯ БОЙОВИХ ЗАВДАНЬ ПІДРОЗДІЛІВ ЗСУ В ЗОНІ АТО ГРУПАМИ ЦИВІЛЬНО-ВІЙСЬКОВОГО СПІВРОБІТНИЦТВА

Інформаційне забезпечення та підтримка бойових дій - це стала практика провідних країн світу, країн-членів НАТО та інших військових союзів. На момент започаткування антитерористичної операції в Луганській та Донецькій областях питання її інформаційної підтримки було, на жаль, проігноровано. Як наслідок, ряд службово-бойових завдань підрозділами ЗСУ були або не виконані або виконані не в повному обсязі, що призвело до неповоротних втрат серед військовослужбовців ЗСУ, СБУ, інших військових формувань. Блокування пересування військових колон, перешкоджання виконанню завдань військових підрозділів, передача розвідувальної інформації протиборчій стороні - це лише деякі видимі наслідки ігнорування інформаційної складової забезпечення бойових дій.

Усвідомлення важливості підтримки військових дій місцевим населенням реалізувалося у створенні пілотного проекту цивільно-військового співробітництва ГШ ЗСУ. Започаткована робота з місцевим населенням, представниками органів місцевої влади, волонтерськими організаціями, міжнародними благодійними організаціями дозволила оперативно вирішувати нагальні проблеми, пов'язані із забезпеченням життєдіяльності мешканців районів проведення АТО. У свою чергу, це сприяло зниженню напруження у відносинах між населенням та військовими підрозділами.

Нормативно-правові засади діяльності груп цивільно-військового співробітництва в Україні було закладено в базових нормативно-правових актах у сфері національної безпеки. Так, відповідно до Закону України «Про основи національної безпеки України» до загроз в інформаційній сфері було віднесено намагання маніпулювати суспільною свідомістю, зокрема шляхом поширення недостовірної , неповної або упередженої інформації. Основним напрямком державної політики в цій сфері було визначено вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії і монополізації інформаційної сфери України.

Фіксація цих положень в Законі «Про основи національної безпеки» є абсолютно логічною, однак їх практична реалізація потребувала цілеспрямованої діяльності суб'єктами, на яких було покладено виконання відповідних завдань.

Ігнорування положень закону призвело до негативних подій на сході України, в Криму та на деяких окремих територіях інших регіонів.

Спроби виправити ситуацію в сфері інформаційної безпеки сприяли затвердженню низки правових документів. Хоч і з запізненням, в них було визначено напрями державної політики у вказаній сфері. У Стратегії національної безпеки, затвердженій Указом Президента України від 26 травня 2015 року № 287/2015, до актуальних загроз національній безпеці віднесено інформаційно-психологічну війну, формування російськими засобами масової комунікації альтернативної до дійсності викривленої інформаційної картини світу та відсутність цілісної комунікативної політики держави. Для забезпечення інформаційної безпеки вважається за необхідне протидіяти інформаційним операціям проти

України, маніпуляціям суспільної свідомості, поширенню спотвореної інформацією та інше. Також передбачена розробка і реалізація скоординованої інформаційної політики органів державної влади.

В Указі Президента України «Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року «Про нову редакцію Воєнної доктрини України» №555/2015 в розділі «Цілі та основні завдання воєнної політики щодо інформаційної безпеки» в якості останніх визначено удосконалення державної інформаційної політики у воєнній сфері; попередження та ефективна протидія інформаційно-психологічним впливам інших держав.

Як ми бачимо, відмінність цих документів в питаннях забезпечення інформаційної безпеки - це закріплення у другому з них термінів «попередження» та «ефективна протидія» інформаційному впливу. Зважаючи на терміни підписання цих документів, цілком логічно виникнення уточнених визначень щодо завдань в сфері інформаційної безпеки.

Також в останньому нормативно-правовому акті з'являється термін «спеціальні інформаційні заходи впливу». Він застосовується до діяльності,що проводиться на території Донецької та Луганської областей.

З позиції реалізації практичних завдань у сфері забезпечення інформаційної безпеки більший інтерес, безумовно, уявляє Указ Президента України №555/2015. В ньому впроваджено дві актуальні позиції, які покладені в основу діяльності груп цивільно-військового співробітництва в зоні АТО, а саме: «З метою переваги над воєнним противником мають бути посилені заходи з реалізації державної інформаційної політики. Забезпечення інформаційної складової воєнної безпеки здійснюватиметься шляхом запровадження ефективної системи заходів стратегічних комунікацій у діяльність органів сектору безпеки» (п.41).

Розглянемо можливість практичної реалізації цих положень детальніше. Як відомо, інформаційний вплив на групи населення здійснюється різними формами і методами та за допомогою різних комунікативних засобів.

Досвід проведення військових та миротворчих операцій НАТО, США та інших держав реалізувався в базові положення концепції цивільно-військового співробітництва, які в подальшому були відображені в більшості керівних документів НАТО. Цікавим для

нас є положення про інформаційне забезпечення діяльності підрозділів НАТО, концепцію якого для кожної операції на окремих територіях готують фахівці CIMIC перед її проведенням.

Загальновизнана практика проведення інформаційного впливу, достатнього для отримання підтримки у місцевого населення (в залежності від специфіки регіону) дозволяє окреслити термін впливу – від трьох до чотирьох місяців. Інформаційний вплив на місцеве населення здійснюється через засоби масової комунікації на кшталт ТВ, Інтернет, радіо, друкованих видань, а також шляхом розповсюдження інформації через ключових суб'єктів комунікації – осіб, які мають вплив на місцеве населення (представники органів місцевої влади, політики, бізнесмени, формальні та неформальні лідери).

На сьогоднішній час, на жаль, запевнення представників Міністерства інформаційної політики України та інших посадових осіб щодо позитивних змін та наявності інформаційного впливу на населення через комунікативні засоби України не відповідають в повній мірі дійсності. В зоні проведення антитерористичної операції на віддаленні 30-40 км від лінії зіткнення супротивник має перевагу у питаннях інформаційного впливу. Моніторинг, здійснюваний групами цивільно-військового співробітництва, дозволяє стверджувати, що у 30 кілометровій зоні інформація з різних джерел комунікації – радіо, ТВ, інтернет - надходить з протилежної сторони. Інтернет-провайдер, який надає послуги фізичним та юридичним особам в Луганській області, знаходиться в м. Луганськ. Укртелеком не спроможний технічно здійснювати підтримку споживачів області, і тому попит на цю послугу задовольняють інші суб'єкти. Єдиним реальним суб'єктом цілеспрямованого інформаційного впливу в зоні антитерористичної операції за таких умов є групи цивільно-військового співробітництва. При цьому заради справедливості необхідно зазначити, що вони користуються не лише ресурсною базою міжнародних організацій, але й всіх підрозділів Збройних Сил України , що виконують завдання в зоні АТО.

На нашу думку, найбільш слабкі місця забезпечення інформаційної підтримки дій Збройних Сил України полягають у неспроможності здійснення превентивних заходів. Майже єдиний структурний підрозділ ЗСУ – Управління цивільно-військового співробітництва - на даний час готує підґрунтя для створення ін-

формаційного продукту, що може бути використаний для впливу на місцеве населення.

Асоціювання людини у формі з позитивними подіями досягається завдяки співпраці з міжнародними благодійними організаціями, представниками волонтерського руху та іншими донорами. Можемо констатувати, що групи ЦВС не мають нині фінансової підтримки з боку держави, і ті результати, яких досягають фахівці CIMIC НАТО за рахунок внутрішніх фінансових можливостей військово-політичного блоку, досягаються в нашому випадку за рахунок доброї волі благодійників та міжнародних благодійних організацій на кшталт Червоного хреста, НСА та ін.

Специфіка роботи груп цивільно-військового співробітництва полягає у тому, що вони працюють на території своєї держави. Це дозволяє уникнути мовного, ментального, релігійного бар'єрів, полегшує можливості впливу на місцеве населення в районі проведення бойових дій. Разом з тим недостатність правового, фінансового та методологічного забезпечення значною мірою утруднює їх функціонування. Однак, на відміну від багатьох інших суб'єктів інформаційної політики, групи ЦВС ЗСУ щоденно і цілеспрямовано здійснюють прозору діяльність з метою зміцнення рівня інформаційної безпеки в районах проведення АТО.

Пролонгація ситуації недостатньої керованості інформаційним полем в зоні АТО може призвести до поступової втрати територій та повзучого наступу антидержавницьких поглядів, що є загрозою вищого рівня для національної безпеки України. Вказане обумовлює необхідність переходу від теоретичних узагальнень до практичної площини реалізації державної інформаційної політики.

Література

1. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»: Указ Президента України від 26 травня 2015 року № 287/2015 // Офіційний вісник України. – 2015. - № 43. – Ст.1353

2. Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року «Про нову редакцію Воєнної доктрини України»: Указ Президента України від 24 вересня 2015 року № 555/2015 // Офіційний вісник України. – 2015. - №78. – Ст.2592.

УДК 35.076

Косиєв О. А.
Львівський державний університет безпеки життєдіяльності
Гриник Р. О.
Львівський державний університет безпеки життєдіяльності

ІНФОРМАЦІЙНА АГРЕСІЯ ЯК НЕВІД'ЄМНА СКЛАДОВА ВЕДЕННЯ ГІБРИДНОЇ ВІЙНИ

Глобальною ціллю гібридної війни є закріплення частини стратегічно важливих ресурсів країни-жертви за агресором. При цьому "передача" таких ресурсів здійснюється елітою "країни-жертви" добровільно, адже сприймається нею не як загарблення, а як рух шляхом розвитку. Це тягне за собою проблеми у розпізнаванні технологій і засобів гібридної війни та, як наслідок відсутність своєчасної та адекватної відповіді на дії агресора. Якщо "гарячі" війни з часом обов'язково підлягають перегляду результатів, то результати гібридної війни перегляду не підлягають, зважаючи на обов'язковість змін ментальності народу, яка в результаті трансформації губить свої основні цілі і духовні цінності, замінюючи їх морально-психологічними ілюзіями і міфами агресора [1].

Під час проведення гібридної війни агресор намагається вплинути на якомога більше число суспільних інститутів держави – об'єкта вторгнення. Це можуть бути засоби масової інформації, конфесійні, приватні і громадські організації, фонди, частина яких може забезпечуватись з-за кордону, а інші – державою з метою розвитку населення та відносин із міжнародними організаціями. Але при цьому всі організації здійснюють так звану розподілену атаку, в результаті якої завдаються масові, точкові удари, які поступово ліквідовують суспільний інститут держави.

Іншою особливістю гібридної війни є відсутність жорсткої ієрархії в структурі агресора. У даній структурі суб'єкт дії керується не наказами керівництва, а власними мотивами і загальними законами, яким характерні спільні світоглядні уявлення того суспільного середовища, за ідеї якого він бореться. Тому те, що відсутня структура побудови мережі та організованих зв'язків

між її одиницями не дає можливості достатньо чітко і конкретно визначити існування і життєдіяльність структур такого роду.

Загалом, гібридна війна включає такі сфери:

- географічну – визначення контролю над частиною чи навіть цілою території країни суперника за допомогою інформаційних і розвідувальних систем, заохочення та підтримка сепаратистських, залучення супротивника у військові та політичні конфлікти;
- економічну – нав'язування кредитів на невигідних для держави умовах, введення різноманітних економічних санкцій, залучення до членства в малоефективних міжнародних економічних організаціях;
- ідеологічну – використання завідомо неправдивої інформації, спотворення інформації, підміни понять, внесення ментальних вірусів і міфологем у свідомість населення супротивника;
- інформаційну – організація атак на інформаційно-телекомунікаційні системи, внесення шкідливого програмного забезпечення різного роду в обчислювальні і телекомунікаційні системи та бази даних ворога [2].

Яка б не була остаточна мета гібридної війни, найважливішим завданням є унеможливлення доступу громадян до об'єктивної і вірної інформації. Важливість цього моменту можна пояснити тим, що швидкість і якість рішень, які приймаються на усіх етапах державного управління, а також формування суспільної думки та настроїв, прямо залежні від повноти та достовірності циркулюючої в країні інформації, засоби спотворення якої можуть бути наступні:

- приховання особливо важливої інформації про стан справ у будь-якій галузі;
- занурення важливої інформації в масив так званого інформаційного сміття;
- підміна термінів або трансформація сенсу;
- відведення уваги на події в інших сферах;
- керування термінами, які легко сприймаються суспільством, але які не мають не тільки чіткого визначення, але і за своєю суттю не відповідають цій предметній галузі;
- заповнення інформаційного простору неприйнятною інформацією;
- посилання на невірно проведені і замовні соціологічні дослідження;

- введення обмеження в ЗМІ на згадку якоїсь інформації, навіть, якщо вона загальновідома з ціллю уникнення усестороннього обговорення шкідливих для влади питань і тем;

- відвертий обман з ціллю створення певної відповіді населення та іноземної громадськості на будь-яку інформацію.

Епоха нових інформаційних воєн ставить завдання масштабного управління інформацією, що надходить по численних каналах, і створення спотвореної інформаційної картини світу. Гібридна війна це війна нового покоління яка ведеться не безпосередніми воєнними діями, а засобами моніторингу за обстановкою в державі суперника, переміщення підконтрольних об'єктів (фізичних осіб) на відповідні позиції в механізмі його державного управління. Моделювання та програмування необхідних процесів та результатів у державі суперника через засоби інформаційного інструментарію. Гібридна війна – багатофункціональне поняття, в яке входить також створення загрози продовольчої, екологічної, політичної, релігійної, інформаційної та інших видів безпеки для суперника невоєнним шляхом.

Література

1. Хамзатов М.М. Влияние концепции сетецентрической войны на характер современных операций / М.М. Хамзатов // Военная мисль. – 2006. – № 7. – С. 13–17.

2. Hoffman Frank G. Hybrid Warfare and Challenges / F.G.Hoffman // Joint Force Quarterly (JFQ). – 2009. – Issue 52, Forth Quarter. – P. 34-39.

УДК 34.096

Красноступ Г. М.

кандидат юридичних наук, старший науковий співробітник
Науково-дослідний інститут інформатики і права
Національної академії правових наук України

ПРОЗОРІСТЬ МЕДІА ВЛАСНОСТІ: СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ ПРАВОВОГО РЕГУЛЮВАННЯ

Більшість громадян України отримують інформацію за допомогою аудіовізуальних медіа. Відсутність відомостей про власників відповідних телерадіоорганізацій не дозволяє визначитись з питанням, наскільки тим чи іншим мовникам можна довіряти.

Саме тому, прозорість відносин медіа власності грає важливу роль для плюралізму аудіовізуальних засобів масової інформації та демократії в цілому.

Частиною п'ятою статті 4 Закону України «Про телебачення і радіомовлення» встановлені основні принципи державної політики у сфері телебачення і радіомовлення. Передбачено, що держава встановлює дієві обмеження щодо монополізації телерадіоорганізацій промислово-фінансовими, політичними та іншими групами чи окремими особами, а також гарантує захист телерадіоорганізацій від фінансового і політичного тиску з боку фінансово-політичних груп та органів державної влади і органів місцевого самоврядування [1].

Підпунктом 12.4 пункту 12 Резолюції Парламентської Асамблеї Ради Європи «Про виконання обов'язків та зобов'язань Україною» від 5 жовтня 2005 р. № 1466 Парламентська Асамблея Ради Європи ще у 2005 році закликала органи влади України гарантувати прозорість власності на засоби масової інформації [2].

Протягом останніх років Верховною Радою України прийнято три закони, спрямовані на виконання зазначених зобов'язань Україною, а саме:

«Про внесення змін до деяких законів України щодо забезпечення прозорості відносин власності стосовно засобів масової інформації» від 4 липня 2013 р. № 409-VII [3];

«Про внесення змін до деяких законодавчих актів України щодо визначення кінцевих вигодоодержувачів юридичних осіб та публічних діячів» від 14 жовтня 2014 р. №1701-VII [4];

«Про внесення змін до деяких законів України щодо забезпечення прозорості власності засобів масової інформації та реалізації принципів державної політики у сфері телебачення і радіомовлення» від 3 вересня 2015 р. № 674-VIII [5].

Не зважаючи на це, наразі відсутня будь-яка достовірна інформація щодо того, кому належать українські аудіовізуальні засоби масової інформації.

Однією з основних позитивних новел прийнятого у 2013 р. Закону України «Про внесення змін до деяких законів України щодо забезпечення прозорості відносин власності стосовно засобів масової інформації» [3] було те, що право аудіовізуальних засобів масової інформації як суб'єкта господарювання на надання інформації про свого власника у відповідь на запит стало

обов'язком [6]. Проте, Закон отримав багато критики з боку медіа спільноти та представників засобів масової інформації.

Закон України «Про внесення змін до деяких законодавчих актів України щодо визначення кінцевих вигодоодержувачів юридичних осіб та публічних діячів» [4] також регулював питання прозорості відносин власності щодо аудіовізуальних засобів масової інформації. Законом передбачено подання юридичними особами державному реєстратору інформації про структуру власності засновників, відомостей про свого кінцевого вигодоодержувача (вигодоодержувачів) у тому числі кінцевого вигодоодержувача (вигодоодержувачів) їх засновника, якщо засновник – юридична особа.

Проте, зазначені положення Закону суб'єкти законодавчої ініціативи визнали недостатніми для належного забезпечення права кожного на інформацію про власників аудіовізуальних засобів масової інформації і 3 вересня 2015 р. Верховною Радою України було прийнято Закон України «Про внесення змін до деяких законів України щодо забезпечення прозорості власності засобів масової інформації та реалізації принципів державної політики у сфері телебачення і радіомовлення» [5].

Слід зазначити, що після прийняття цього спеціального Закону суспільні відносини щодо забезпечення прозорості відносин власності стосовно аудіовізуальних засобів масової інформації вже не регулюються Законом України «Про внесення змін до деяких законодавчих актів України щодо визначення кінцевих вигодоодержувачів юридичних осіб та публічних діячів» [4]. Тобто, працюватиме правило про співвідношення загальної та спеціальної норм.

Законом [5] статтю 1 Закону України «Про телебачення і радіомовлення» доповнено новими визначеннями. Нашу увагу привернуло визначення терміну «публічна компанія», згідно з яким це юридична особа, створена у формі публічного акціонерного товариства, акції якої включені до біржових списків (пройшли процедуру лістингу) фондових бірж, що відповідають критеріям, визначеним Національним банком України. При цьому, вважається, що публічна компанія не має осіб, які мають істотну участь, здійснюють над нею контроль, та є такою, що не має кінцевого бенефіціарного власника (контролера). У результаті цього фактично дія Закону України «Про телебачення і радіомовлення»

щодо визначення структури власності не поширюватиметься на публічні компанії. Таким чином, цим Законом прямо передбачено можливість не надавати інформацію про реальних власників аудіовізуальних засобів масової інформації, якщо їх засновником є публічна компанія.

Крім того, на сьогодні не існує дієвого механізму перевірки Національною радою України з питань телебачення і радіомовлення інформації про структуру власності телерадіоорганізацій і провайдерів програмної послуги. Тому, Законом [5 на вказаний регуляторний орган було покладено обов'язок розробити Порядок подання телерадіоорганізаціями та провайдерами програмної послуги інформації про структуру власності, а також затвердження відповідних форм документів. З метою вирішення порушеного питання Національна рада Україна з питань телебачення і радіомовлення створила робочу групу з питань прозорості медіа власності, що мала розробити відповідні документи [7].

Вважаємо, що сьогодні край необхідно врахувати кращі європейські практики організаційно-правового забезпечення державної інформаційної політики щодо прозорості відносин власності стосовно аудіовізуальних засобів масової інформації, оскільки їх діяльність впливає на інформаційну безпеку нашої країни в цілому.

З огляду на наведене, у новій редакції Закону України «Про телебачення і радіомовлення» необхідно передбачити ефективний механізм обмеження щодо монополізації телерадіоорганізацій промислово-фінансовими, політичними та іншими групами чи окремими особами.

Література

1. Про телебачення і радіомовлення : Закон України від 21 грудня 1993 р. № 3759-XII // Відомості Верховної Ради України. – 2006. – № 18. – ст. 155. – [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/3759-12.

2. Про виконання обов'язків та зобов'язань Україною : Резолюція Парламентської Асамблеї Ради Європи від 5 жовтня 2005 р. № 1466. – [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/994_611.

3. Про внесення змін до деяких законів України щодо забезпечення прозорості відносин власності стосовно засобів масової інформації : Закон України від 4 липня 2013 р. № 409-VII // Відомості Верховної Ради Украї-

ни. – 2014. – № 20-21. – ст. 715. – [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/409-18.

4. Про внесення змін до деяких законодавчих актів України щодо визначення кінцевих вигодоодержувачів юридичних осіб та публічних діячів : Закон України від 14 жовтня 2014 р. №1701-VII // Відомості Верховної Ради України. – 2014. – № 46. – ст. 2048. – [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/1701-18.

5. Про внесення змін до деяких законів України щодо забезпечення прозорості власності засобів масової інформації та реалізації принципів державної політики у сфері телебачення і радіомовлення : Закон України від 3 вересня 2015 р. № 674-VIII. – [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/674-19.

6. Беляева К. В. Европа на страже прозрачности украинских СМИ // Судебно-юридическая газета, 2013. – № 33 (201). – [Електронний ресурс]. – Режим доступу : http://sud.ua/newspaper/2013/08/23/53506-evropa-na-strazhe-prozrachnosti-ykrainskikh-smi.

7. Нацрада створила робочу групу з питань прозорості медіа власності – [Електронний ресурс]. – Режим доступу : http://www.telekritika.ua/kontekst/2015-10-09/112063.

УДК 327.56(478)

Кудрявцев В. О.
Воєнно-дипломатична академія імені Є. Березняка

ВРЕГУЛЮВАННЯ ПОЛІТИЧНИХ КОНФЛІКТІВ В УМОВАХ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА (НА ПРИКЛАДІ ПРИДНІСТРОВСЬКОГО КОНФЛІКТУ)

Ратифікувавши Угоду про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергетики і їхніми державами-членами, з іншої сторони [1], Україна отримала інструмент та дороговказ для своїх перетворень. Виконання вимог цієї Угоди дає можливість Україні в подальшому стати повноцінним членом Європейського Союзу [2].

Проте, на заваді процесу гармонійної інтеграції України до європейських та євроатлантичних структур, створення єдиного континентального простору стабільності, безпеки і стійкого економічного розвитку постала збройна агресія Російської Федерації по відношенню до нашої держави та неврегульованість політичних конфліктів довкола неї.

Тому, одним з основних напрямів державної політики національної безпеки держави у зовнішньополітичній сфері Україною задекларовано таке:

1. Зусилля на регіональному рівні спрямовуватимуться на створення ефективної системи взаємодії у Центральній та Східній Європі з метою забезпечення безпеки та стабільності. Для цього використовуватимуться насамперед інструменти та можливості ОБСЄ та Ради Європи. Особлива увага приділятиметься формуванню механізмів забезпечення безпеки в регіоні Чорного моря.

2. Україна проводитиме спільно з іншими європейськими союзниками політику денуклеаризації та демілітаризації Чорноморського регіону; сприятиме поверненню до режиму оновленого Договору про звичайні збройні сили в Європі; братиме активну участь в опрацюванні існуючих та внесенні нових безпекових ініціатив, спрямованих на зміцнення стабільності і колективної безпеки в Європі [3].

Осторонь процесів, що відбуваються в Україні і довкола неї не залишається і Європейський Союз (ЄС). Так, у підсумковій декларації Ризького саміту Східного партнерства зазначено, що ЄС залишається прихильним своїй підтримці територіальної цілісності, незалежності та суверенітету всіх своїх партнерів. Повне дотримання всіх принципів і зобов'язань, закріплених в 1975 році в Заключному акті в Гельсінкі та в 1990 році в Паризькій хартії всіма учасниками ОБСЄ, а також повна повага до принципів та положень Статуту ООН мають вирішальне значення для спільного бачення вільної, демократичної, мирної і неподільної Європи [4].

Природно, що на тлі анексії Автономної Республіки Крим і збройного вторгнення Російської Федерації у східні області нашої держави, проблема врегулювання політичних конфліктів у суміжних з Україною державах відходить на другий план, проте намагання Москви реалізувати на теренах Донецької і Луганської областей придністровський сценарій зумовлює необхідність наукового осмислення феномену придністровського конфлікту та розроблення заходів з адаптації державної політики України до динамічних змін ситуації в регіоні.

Останнім часом проблема придністровського врегулювання знаходиться під пильною увагою як міжнародних організацій, політичних еліт різних країн, громадських інституцій так і широкого кола зарубіжних та вітчизняних науковців.

Так, питання про надання спеціального статусу Придністров'ю у складі єдиної молдовської держави розглядалось на засіданні Ради міністрів ОБСЄ у Белграді 3-4 грудня 2015 року [5].

Крім того, останніми роками спостерігається активізація досліджень проблем виникнення політичного конфлікту довкола Придністров'я, його перебігу, інтересів ключових гравців та перспектив врегулювання. Найбільш актуальними, ґрунтовними і цікавими з огляду на ситуацію, що склалася в Україні та імовірність реалізації придністровського сценарію на Сході нашої держави є дослідження О. Гетьманчук, М. Дорошка, Є. Єніна, В. Коцура, А. Почобута, Т. Чорновола та ін. [6-10].

Крім того, в сучасній політологічній науці створено достатнє теоретичне підґрунтя для дослідження політичних конфліктів на пострадянському просторі як чинників впливу на національну безпеку держав регіону. Існує значна кількість публікацій, в яких розглянуто конкретні конфлікти, що виникали останнім часом, та проблеми їхнього врегулювання.

Проте, недостатньо дослідженими є методологічні аспекти визначення ризиків і загроз національній безпеці України, зумовлених наявністю неврегульованого придністровського конфлікту. Бракує наукових підходів щодо визначення шляхів мінімізації ризиків нашій державі в процесі врегулювання придністровського конфлікту, ролі і місця силових структур України у цьому процесі.

Тому, особливої актуальності у наш час набувають наукові дослідження з розроблення механізмів реалізації державної політики України з врегулювання політичних та збройних конфліктів в умовах протидії російській інформаційній агресії та визначення шляхів мінімізації загроз національній безпеці нашої держави.

Література

1. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони: ратифікована Законом України № 1678-VII від 16.09.2014 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/984_011.

2. Стратегія сталого розвитку "Україна-2020": схвалена Указом Президента України від 12.01.2015 № 25/2015 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/5/2015.

3. Стратегія національної безпеки України: затверджена Указом Президента України від 26.05.2015 № 287/2015 [Електронний ресурс]. – Режим доступу: http://zakon0.rada.gov.ua/laws/show/287/2015.

4. Итоговая декларация Рижского саммита Восточного партнерства от 22 мая 2015 года [Електронний ресурс]. – Режим доступу: http://eurointegration.com.ua/rus/articles/2015/05/22/7034050/view_print.

5. Constructive spirit at 22nd OSCE Ministerial Council laid solid foundations for continuing dialogue on Europe's security challenges [Електронний ресурс] / OSCE. – Режим доступу: http://osce.org/cio/207056.

6. Чем ДНР-ЛНР отличаются от Приднестровья, и почему РФ не выводит войска с Донбасса [Електронний ресурс] / Апостроф. – Режим доступу: http://apostrophe.com.ua/article/society/2015-09-28/chem-dnr-lnr-otlichayutsya-ot-pridnestrovya-i-pochemy-rf-ne-vyivodit-voyska-s-donbassa/2329.

7. Kijow zmienia strategie wobec Naddniestrza [Електронний ресурс] / Gazeta Wyborcza. – Режим доступу: http://wyborcza.pl/1.75477.19272000.kijow-zmienia-strategie-wodec-naddniestrza.html.

8. Сценарії розвитку придністровського конфлікту: виклики європейській безпеці [Електронний ресурс] / Інститут світової політики. – Режим доступу: http://iwp.org.ua/img/IPW-Transnistria_FULL.pdf.

9. Doroshko M.S. Transdniestrian conflict in the Republic in Moldova: geopolitical implications / М.С. Дорошко // Актуальні проблеми міжнародних відносин: Збірник наукових праць, – Вип. 114. Частина І (у двох томах). – К.: КНУ імені Тараса Шевченка, Інститут міжнародних відносин, 2013. – С. 3-10.

10. Коцур В.В. Забезпечення миру в Придністров'ї: плани, цілі та взаємодія України, Росії, Молдови, ОБСЄ /В.В.Коцур // Гілея. Історичні науки. Філософські науки. Політичні науки: Науковий вісник: Збірник наукових праць. – К.: Вид. НПУ імені М.П. Драгоманова, 2011. – Вип. 45(№ 3). – С. 646-653.

УДК 343.132

Куценко Д. В.
кандидат юридичних наук
Національна академія внутрішніх справ

КРИМІНАЛЬНІ ПРОЦЕСУАЛЬНІ ГАРАНТІЇ ДЕРЖАВНОЇ ТАЄМНИЦІ ПІД ЧАС ІНІЦІЮВАННЯ ПИТАННЯ ПРО ПРОВЕДЕННЯ НЕГЛАСНИХ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ

Проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій вважається основним засобом отримання доказів. Така можливість, відповідно до ст. 93 КПК передбачена для сторони обвинувачення (ч. 2. ст. 93 КПК). Для сторони захисту,

потерпілим, представником юридичної особи, щодо якої здійснюється провадження, можливість проведення слідчих (розшукових) дій не передбачена але передбачена можливість ініціювання їх проведення через подання слідчому, прокурору відповідних клопотань (а. 2 ч. 3 ст. 93 КПК).

Згідно з ч. 1 ст. 246 КПК негласні слідчі (розшукові) дії – це різновид слідчих (розшукових) дій, відомості про факт та методи проведення яких не підлягають розголошенню, за винятком випадків, передбачених КПК. Щодо порядку отримання дозволу по більшості негласних слідчих (розшукових) дій відповідно до ч. 1 ст. 248 розгляд клопотання здійснюється слідчим суддею за участю особи, яка подала клопотання. У випадку коли першочергове клопотання подає сторона захисту, потерпілий, представник юридичної особи, щодо якої здійснюється провадження постає питання, чи необхідно слідчому судді залучати до розгляду клопотання зазначених учасників. У цьому разі з одного боку саме сторона захисту, потерпілий, представник юридичної особи, щодо якої здійснюється провадження є ініціаторами негласної слідчої (розшукової) дії і найбільше зацікавлені у її проведенні та результатах. З іншого боку, якщо питання щодо проведення негласної слідчої (розшукової) дії вже дійшло до слідчого судді значить слідчий або прокурор, виніс клопотання про проведення цієї дії а відповідно і погодився зі всіма або більшістю доводів які наводились ініціаторами. При вирішенні цього питання слід також звернути увагу на ч. 3 ст. 248 КПК відповідно до якої слідчий суддя постановляє ухвалу про дозвіл на проведення негласної слідчої (розшукової) дії, якщо прокурор, слідчий доведе наявність достатніх до того підстав. Отже законодавцем передбачається, що обов'язок доведення необхідності проведення певної негласної слідчої (розшукової) дії лежить саме на слідчому та прокурорі. Окрім цього під час розгляду клопотання про необхідність проведення негласної слідчої (розшукової) дії можуть проговорюватись питання які складають державну таємницю і далеко не факт що у сторони захисту, потерпілого або представника юридичної особи, щодо якої здійснюється провадження буде оформлений допуск до державної таємниці відповідної категорії. У зв'язку із вищенаведеним, з метою дотримання кримінальних процесуальних гарантій державної таємниці та не допущення ускладнення вказаної процесуальної дії вважаємо не доцільним присутність

сторони захисту, потерпілого або представника юридичної особи, щодо якої здійснюється провадження під час розгляду клопотання слідчим суддею про надання дозволу на проведення ініційованої ними негласної слідчої (розшукової) дії. Але, з метою дотримання інтересів згаданих осіб та сприяння засаді змагальності сторін та свободи в поданні ними суду своїх доказів і у доведенні перед судом їх переконливості вважаємо за необхідне обов'язково доводити позицію цих осіб та наведені ними аргументи до відома слідчого судді. У зв'язку з чим вважаємо за доцільне закріпити ч. 6 ст. 248 КПК такого змісту: «Під час розгляду слідчим суддею клопотання про дозвіл на проведення негласної слідчої (розшукової) дії, у разі якщо вона була ініційована стороною захисту, потерпілим, представником юридичної особи, щодо якої здійснюється провадження, слідчий, прокурор зобов'язані довести аргументи зазначених осіб до відома слідчого судді». Таке доповнення буде особливо актуальним у випадку, коли слідчий або прокурор відмовивши стороні захисту, потерпілому, представнику юридичної особи, щодо якої здійснюється провадження у клопотанні про проведення негласної слідчої (розшукової) дії але у зв'язку із оскарженням такої особи до слідчого судді (аб. 2 ч. 3 ст. 93 КПК, п. 7 ч. 1 ст. 303 КПК) та задоволенням цієї скарги (п. 3 ч. 2 ст. 307 КПК), буде змушений аргументувати позицію (наприклад п. 2 ч. 3 ст. 248 КПК) з якою не згодний. Важливим моментом у дотриманні кримінальних процесуальних гарантій державної таємниці під час доказування є те, що процесуальний порядок розгляду клопотання щодо проведення негласних слідчих (розшукових) дій передбачає обов'язкове повідомлення особи, яка заявила таке клопотання про результати його розгляду (ч. 2 ст. 220 КПК). І якщо у разі повної або часткової відмови у задоволенні клопотання з повідомленням особи питань не виникає, то у випадку позитивного рішення з'являються правові труднощі. Як вже вказувалось вище згідно з ч. 1 ст. 246 КПК негласні слідчі (розшукові) дії – це різновид слідчих (розшукових) дій, відомості про факт та методи проведення яких не підлягають розголошенню. Окрім цього відповідно до п. 4.12.4 Зводу відомостей що становлять державну таємницю зазначені відомості становлять державну таємницю ступеню секретності «таємно» [1]. Отже складається ситуація при якій з одного боку посадові особи повинні виконати свій обов'язок та повідомити особу про результа-

ти розгляду її клопотання, з іншого боку у разі задоволення такого клопотання та повідомлення про це заявнику слідчий або прокурор розголосять відомості про факт проведення негласної слідчої (розшукової) дії а отже розголосять відомості що становлять державну таємницю особі, яка не має відповідного допуску. Формально таке діяння охоплюється складом злочину передбаченим ст. 328 КК України. Окрім цього термін «факт проведення негласної слідчої (розшукової) дії» вважаємо не зовсім вдалим. Його пояснення або визначення а ні у КПК а ні у Зводі відомостей що становлять державну таємницю нам знайти не вдалось. У тлумачному словнику української мови слово «факт» означає дійсну, не вигадану подію, дійсне явище; те, що сталося, відбулося насправді [2, с. 552]. Тобто певну дію у минулому часі, дію, яка вже пройшла. У зв'язку з чим вважаємо, що цей термін не зовсім вірно відображає відомості які необхідно тримати у таємниці адже з тактичної точки зору навіть більш важливого значення має тримання у таємниці: 1. самого наміру проведення негласної слідчої (розшукової) дії (з моменту отримання процесуальної згоди на її початок відповідної посадової особи); 2. інформації, що певна негласна слідча (розшукова) дія об'єктивно триває на даний момент, тобто здійснюється у теперішньому часі. До речі вже після проведення негласної слідчої (розшукової) дії відомості про факт її проведення можуть розкриватись під час відкриття матеріалів іншій стороні (ч. 1 ст. 254, ст. 290 КПК) та особам, щодо яких ці негласні слідчі (розшукові) дії проводилися (ст. 253 КПК). Отже вважаємо що у цьому питанні законодавство потребує уточнення термінології яка би відображала не тільки минулий час (факт проведення) а і передбачала би не розголошення інформації у часі майбутньому (намір про проведення) та теперішньому (з моменту початку проведення до моменту закінчення проведення відповідної негласної слідчої (розшукової) дії).

Література

1. Наказ Служби безпеки України від 12 серп. 2005 року № 440 «Про затвердження Зводу відомостей, що становлять державну таємницю» : [Электронний ресурс]. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/z0902-05/print1443623709954988

2. Словник української мови: в 11 томах. — Том 10, Видав-во «Наукова думка» – К., 1979. – 658 с.

УДК 341.824:338.47(043.2)

Лещик Н. В.
Державна наукова установа
«Інститут модернізації змісту освіти»

ВПЛИВ ТЕЛЕВІЗІЙНОЇ ІНФОРМАЦІЇ НА МОРАЛЬНЕ ЗДОРОВ'Я СУСПІЛЬСТВА ТА СВІДОМІСТЬ ГЛЯДАЦЬКОЇ АУДИТОРІЇ

Найголовнішим надбанням людства є свобода слова, яка є і головним постулатом в діяльності засобів масової інформації та необхідною умовою існування демократичного суспільства. Згідно Конвенції про захист прав людини і основоположних свобод «...кожен має право на свободу вираження. Це право повинне включати свободу без втручання і незважаючи на межі» [1].

Вільне поширення інформації будь-якого виду через кордони є важливим чинником міжнародного порозуміння, об'єднання людей та взаємного збагачення культур [2].

Мораль ґрунтується на неписаних законах, що склалися у суспільстві на основі традиційних духовних і культурних цінностей. Велике значення має формування моральної свідомості особистості у підростаючого покоління, адже наскільки молодь засвоїть моральні ціннісні орієнтири, буде залежати майбутнє країни.

Міжнародне і європейське законодавство виважено і обережно ставиться до обмеження свободи слова, але у випадку захисту суспільної моралі прийнято ряд обмежень, які закріплені у відповідних документах.

Завданням журналіста у суспільстві є задоволення прав аудиторії на отримання достовірної і вичерпної суспільно значущої інформації, чесне, точне і збалансоване висвітлення подій, виходячи з позиції професійної відповідальності перед суспільством. Тому на Заході виникло таке поняття як «журналістська відповідальність» – відповідальність конкретного журналіста або цілого медіа перед суспільством та аудиторією.

Але, на жаль, з розповсюдженням телебачення відбулася вульгаризація змісту телепрограм сенсаційними матеріалами, де є секс, смерть, скандали, насилля тощо.

Здатність телебачення одночасно повідомляти про подію і давати її відображення на телевізійному екрані є чи не найбільш

унікальною властивістю телебачення. Про здатність телебачення психологічно впливати на людину зазначає Рада Європи у своїх рекомендаціях «Про силу візуальних образів» і застерігає про хвилю «віртуальної реальності», яку породжують телебачення і комп'ютери [3, с. 2].

Вперше дослідили вплив медіа-насилля на підліткову злочинність А. Лацис і Л. Кейлина в праці «Дети и кино» (1928 р.). Більшість громадян вірять в образи, які бачать, наприклад, у випусках новин, хоча часто вони є певною інтерпретацією якоїсь події. Суть медіа-технологій – вплив на свідомість і поведінку людини. Вчені називають їх психотехнологіями або спеціальними технологіями, здатними навіювати ідеї або маніпулювати свідомістю, поведінкою людини [4, с. 70].

Н. Череповська виділяє наступні види спеціальних технологій: ефект «праймінгу», заміна імен або наклеювання ярликів, буденна розповідь, ефект присутності, відволікання уваги, ефект психологічного шоку. Завдяки їх застосуванню, увага глядачів особливим чином спрямовується на незначні події і відвертається від важливих суспільних проблем [4, с. 70].

Глядач може по різному сприймати інформацію, подану за допомогою психотехнологій. Але приблизно для 10% дорослих телеглядачів під час перегляду телевізора нічого більше не існує. Чим молодший глядач, тим таке захоплення більше і сягає загалом 15% загального числа глядачів. Близько 20% українських глядачів забувають про свої проблеми і труднощі перед телевізором [5, с. 24]. Американська дитина, за дослідженнями медичного факультету Гарвардського університету, до настання 18 років спостерігає на екрані телебачення 180 тис. випадків насилля, з них – 80 убивств. Організація «Mediascope» стверджує, що 66% дитячих програм у США містять сцени насилля, причому у 77% випадків насилля ніяк не карається. Хоча, зауважимо, американський ефір значно менше насичений сценами насилля, ніж український. Чимало американських фільмів, які у нас демонструються, у США заборонені для неконтрольованого дорослими показу [6].

Діти до восьми років майже не розрізняють реальність і фантазію. Підлітки ж більше схильні довіряти матеріалам телебачення, ніж очевидним фактам. Психологи дійшли висновку, що зміст телепередач з негативним забарвленням підвищує рівень злочинності та суїциду у суспільстві, особливо підліткової. При-

кладом є Росія, де в лютому 2012 року самогубство підлітків, по суті, було розрекламовано у теленовинах. Після репортажів про перші самогубства, з поясненням того, що вони заздалегідь планувалися підлітками через Інтернет-сторінки своєрідного «клубу самогубців», відбулась ціла хвиля суїцидів. Невідомо наразі, чи ця хвиля вже припинилася [7, с. 92].

Людина, споживаючи сучасні, вільні від контролю етики, телепрограми, не може раціонально оцінити характер їхнього впливу на поведінку і психіку. Держава, захищаючи споживача і країну в цілому, повинна накладати на такий вид продукції обмеження. С.Г. Кара-Мурза у книзі «Манипуляция сознанием» стверджує: «…якщо держава з якоїсь причини цього не робить, то стає співучасником телекорпорацій, що є корупцією. Суть корупції в тому, що телебачення платить державі підтримкою за допомогою доступної йому маніпуляції суспільною свідомістю» [8, с. 177]. Дослідження серед дорослих засуджених показало, що 63% з них здійснили злочин, наслідуючи телевізійних героїв, а 22% перейняли «техніку злочину». Подібні дослідження серед неповнолітніх в'язнів, на жаль, не проводились, але, враховуючи їхню вразливість, дані були б набагато більші.

Збільшилась і кількість злочинів, які здійснюються для того щоб потрапити в новини. Наприклад, в одному з містечок Північного Йоркширу в 2010 році шибеник підпалив будинок, у якому спали два пенсіонери. Після арешту чоловік зрадів: «Я потраплю в новини!». Третього березня 2012 року в США був арештований студент-відмінник, що мав намір влаштувати бійню, щоб потрапити в новини [9].

Неодноразово випуски новин повідомляли про те, що діти і дорослі після перегляду фільмів жахів, таких як «Двінок», «Пила», «Бригада», «Матриця», «Крик», здійснювали злочини та вбивства, подібні до побачених. Поясненням злочину було те, що вони, начебто, намагались наслідувати героїв фільму. Так, Нео Джошуа Кук, який проживав у містечку Оактон, штат Вірджинія, США, обвішавши всі стіни своєї кімнати плакатами із зображеннями героїв «Матриці», заявив, що він «знаходиться в Матриці», і в лютому 2002 р. вбив своїх батьків. Російський фільм С. Говорухіна «Ворошиловський стрілець», ймовірно, спонукав Андрія Кочетова до захисту честі своєї 15-річної сестри, зґвалтованої двома молодими людьми.

Вчені Стенфордського університету досліджували вплив сцен насилля на дітей дошкільного віку. Діти спостерігали сцени агресивної поведінки (биття ляльок, каліцтво штучних тварин). Через деякий час нормальні, соціально адаптовані дошкільники почали вести себе більш агресивно. Висновок вчених – сцени насилля, жорстокості і смерті викликають сильні агресивні імпульси [8, с. 186].

У журналі «Шпігель» було опубліковано дані дослідження, яке проводило Бі-Бі-Сі. Два повідомлення, одне з них правдиве, інше – брехня, було передано трьома видами повідомлень: надруковані в газеті, передані по радіо і показані по телебаченню. Розрізнили неправду лише 3,6% респондентів. Отже, за своєю природою телебачення таке, що правду і брехню розрізнити майже неможливо [8, с. 189].

Як підсумок, треба зауважити, що більшість телеглядачів довіряє телебаченню та інформаційним випускам новин, вважаючи їх відображенням реального життя. На сьогоднішній день сучасні ЗМІ повністю контролюють поширення інформації, що визначає наші уявлення, установки, маніпулюючи масовою свідомістю, змінюють нашу поведінку і реальну соціальну дійсність. Очевидно – чим менше розвинене суспільство, тим більшу шкоду наносить йому телебачення з невиваженою інформаційною політикою. Тому ми пропонуємо проводити дослідження щодо зв’язків між насильством на екрані та насильницькою поведінкою, оприлюднювати дані цих досліджень та порушувати це питання для його вирішення на найвищому рівні, а саме – держави та законодавства.

Література

1. Конвенція про захист прав людини і основоположних свобод. – [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/995_004/

2. Декларація про свободу вираження поглядів та інформації. – [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/994_885

3. Рада Європи «Про силу візуальних образів». – [Електронний ресурс]. – Режим доступу: http://medialaw.org.ua/library/rekomendatsiya-1276-1995-pro-sylu-vizualnyh-obraziv/

4. Череповська Н. «Візуальна медіа культура учнів ЗОШ» Київ: Інститут соціальної та політичної психології НАПН України, 2010, – 155 с.

5. Медіа-культура населення України: Інформаційний бюлетень. Червень 2008 / За. Ред.. Л.А. Найдьонової, О.Т. Баришпольця; Упоряд. Л.П. Черниш. – Київ., 2008. – 52 с.

6. Федоров О.В. «Насильство на екрані». – [Електронний ресурс]. – Режим доступу: http://www.mediakrytyka.info/drukovani/06/nasylstvo-na-ekrani.html

7. Куляс І., О. Макаренко. Ефективне виробництво теленовин: стандарти інформаційного мовлення; професійна етика журналіста-інформаційника. Практичний посібник для журналістів. – Київ, видавництво ХББ, 2006. – 120 с.

8. Кара-Мурза С.Г."Манипуляция сознанием". – Москва, 2000 – 485 с.

9. Trayvon Martin was suspended three times from school ». – [Електронний ресурс]. – Режим доступу: http://usnews.nbcnews.com/_news/2012/03/26/10872124-trayvon-martin-was-suspended-three-times-from-school

УДК 327

Ожеван М. А.
доктор філософських наук, професор
Національний інститут стратегічних досліджень при Президентові України

ЕСКПЕРТНО-МЕДІЙНІ МЕРЕЖІ ТА ЇХ РОЛЬ В РОСІЙСЬКИХ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ СПЕЦОПЕРАЦІЯХ АНТИУКРАЇНСЬКОГО СПРЯМУВАННЯ

Особливістю медіа-експертів (в англомовній традиції - «пандитів» («Pundit»), яких також іронічно називають «розмовляючими головами» («a talking heads»), є їх активне залучення до реалізації таких провладних функцій як медіація; зведення складного до простого шляхом творення «правди»; легітимація влади; окреслення ситуацій; встановлення пріоритетів («порядку денного») тощо. Розвиток онлайнових мереж породив феномени експертів-блогерів та «мережевої експертизи» (networked expertise).

Привертає увагу пул західних аналітиків й журналістів, які беруть участь в організованих російськими спецслужбами «активних заходах» (рос. «активных мероприятиях»; англ. «Active Measures»). Переважно таких «пандитів» РФ залучає з числа нон-

конформістів, які перебувають на лівих й правих маргінесах політичної думки, маючи обмежені засоби донесення антимейнстрімних поглядів до масової аудиторії. Отже, тут відбувся своєрідний функціональний обмін: російське політичне керівництво надало західним мислителям-маргіналам потужні канали зовнішнього мовлення та інформування, а вони своїм авторитетом в певних академічних та політичних колах підкріпили московську пропаганду на Заході враженнями самобутності й автентичності.

У продемонстрованому 26 квітня 2015 р. на каналі «Россия 1» з нагоди 15-річчя перебування В.Путіна при владі фільмі Володимира Соловйова «Президент» В.Путін робить безпрецедентну антиамериканську заяву про те, що він, мовляв, більше 20-ти років терпів спроби американських спецслужб розхитати внутрішньополітичну ситуацію в РФ, але тепер вирішив, що вже настав час «вставати з колін».

Квазірелігійні й квазінаціоналістичні ескапади російського президента в рольовій функції виразника й захисника традиційних цінностей свідомо розраховані на попит не тільки в країнах Третього світу, але також в певних колах інтелектуалів та політиків в в цитаделі глобалізаційних процесів, - США, країнах ЄС тощо. До них слід віднести, зокрема, Австрійську партію свободи (нім. Freiheitliche Partei Österreichs, FPÖ) й французький Національний Фронт (Нацфронт).

Головною зовнішньополітичною метою Нацфронту є припинення існування ЄС і НАТО, заміна цих утворень «партнерством незалежних країн», яке має включати також Росію і управлятися потрійним союзом «Берлін – Париж – Москва». Не дивно, що Нацфронт у числі інших ультраправих партій Євросоюзу є одним з основних прихильників політики В.Путіна на Заході.

Зокрема, різні неонацисти і неофашисти включно з представниками Нацфронту, склали ядро європейських «спостерігачів» за перебігом нелегітимного референдуму в Криму 16 березня 2014 р., підтримавши таким чином анексію Криму Росією. А в квітні 2014 р. Марін Ле Пен публічно заявила про підтримку терористів на Сході України й осуд тодішнього київського політичного керівництва. Згодом, всередині травня того ж року, вона заявила, що поділяє з Путіним єдині цінності й підтримує політику федералізації в Україні.

На базі французького Нацфронту діє медійний офшор у Франції «Голосу Росії» (Voix de la Russie) й телестанція ProRussia

TV (діє з 2012 р.), якою керує колишній політичний радник Нацфронту Жіль Арно (Gilles Arnaud). Аудиторія телеканалу у Франції складала, станом на кінець 2013 р., 700 тис. глядачів [1].

Подібні проросійські медіа існують і в інших західних країнах, спираючись на підтримку міжнародного телеканалу «Росія сьогодні» (RT) й однойменної міжнародної інформагенції (колишня «РИА Новости») та її підрозділу Sputnik, РС «Голос Росії» тощо. У заснованої наприкінці 2005 р. RT нині шість каналів мовлення, - три англомовних новинних (RT International, RT America, RT UK), новинні канали на іспанській й арабській мовах й пізнавальний канал RTД.

Західних аналітиків й журналістів певного ґатунку «проросійською мережею за лаштунками кампанії антиукраїнського наклепу» [2]. Проте «проросійськість» цієї аналітично-медійної мережі не слід перебільшувати, бо вона є радше ситуативною. Головний редактор телеканалу RT й MIA «Росія сьогодні» Маргарита Симонян, зокрема, високо оцінюючи кадровий склад своїх західних співробітників, заявляє: «В масі своїй у нас працюють ідейні люди, які хочуть працювати саме у нас, бо вони вірять в те, що ми робимо. Наприклад, колишні активісти» [3]. При цьому М.Симонян, посилаючись на дані західних медіа-соціологічних агенцій оцінює аудиторію каналів російського іномовлення як досить поважну, хоча й не вирішальну для формування громадської думки. За даними агенції Nielsen, щоденна аудиторія RT у США — 1,3 млн. (і це тільки тільки в семи найбільших містах); в країнах Близького Сходу й Магребу — більше 6,5 млн. Щоденна аудиторія RT в Великобританії — більше 0,5 млн. (дані Ipsos EMS). Дослідження іспаномовної аудиторії RT заплановане на кінець 2015 р. [3]. RT вельми популярна у відеохостингу YouTube (в 2015 р. загальне число переглядів на всіх акаунтах перевищило 2,5 млрд.). Більш скромною була відвідуваність сайту RT.com (за даними SimilarWeb, у липні 2015 р. - 52,8 млн. відвідувань), хоча вона й перевищила відвідуваність сайтів Al Jazeera (12 млн.), Deutsche Welle (15,4 млн.), Voice of America (9,1 млн.) [3].

У основного міжнародного проекту MIA RT, - Sputnik, заснованого наприкінці 2014 року, наразі вже є радіомовлення і сайти більш ніж 30-ма мовами. У планах MIA Sputnik - мовлення 39-ма мовами як в радіоефірі, так і в Інтернеті. Сукупна місячна аудиторія онлайн-ресурсів RT, за даними агентства лише впродовж 2015 досягла майже 47 млн. [3].

Російське ідеологічно-медійне керівництво доклало неабияких зусиль з метою репрезентації подій в Україні 2014-2015 рр. й тих, що їм передували, не як закономірного руху до здобуття незалежності від колишньої імперії-поневолювача, а як змову «фашистів» з олігархами, які не зупинилися в прагненні самоутвердження перед спонуканням західної експансії. Така репрезентація подій була підхоплена лівими й правими екстремістами на Заході, простимульованими з Кремля. Зокрема, незалежний геополітичний аналітик» Ерік Дрейцер (Eric Draitcer) у тексті, оприлюдненому на Заході в розпал української Революції гідності спочатку у власному електронному виданні Stop Imperialism (StopImperialism.com), а згодом на сайті Центру досліджень глобалізації (The Centre for Research on Globalization), виданням «Контрудар» (CounterPunch) та ін. доходив до крайніх оцінок революційних подій в Україні 2013-2014 рр. як «останнього прикладу зростання найбільш підступної форми фашизму в Європі з часів падіння Третього Рейху» [4].

Колишній американський розвідник Ф.Енгдал (F. William Engdahl) приписував вбивства на Майдані УНА-УНСО, яку вважає частиною пронатовської глобальної таємної організації «ГЛАДІО» [5].

Приблизну таку ж конспірологічну версію трагічного розвитку подій на Майдані розвивали Мішель Чоссудовский й Бонні Фоллкнер (Michel Chossudovsky; Bonnie Faulkner) у матеріалі «Український «демократичний» державний заколот: керований з Вашингтону «неонацистсько-неоліберальний» проксі-уряд». За логікою цього матеріалу, вбивства цивільних осіб на Майдані були приводом для «зміни режиму», тобто розстріл снайперами своїх же прихильників замовили лідери Євромайдану і опозиції, використавши цю трагедію як привід для зміщення «законно обраної влади» [6].

Російській пропаганді та її впливам на західну громадську думку сприяє факт володіння російськими олігархами деякими західними ЗМІ та їх «доброчинність» стосовно потужних університетів та аналітичних центрів [7].

Особливо активно використовується в інформаційно-психологічних операціях, дирігованих з московського центру, Інтернет-видання Global Research, яке належить канадському The Centre for Research on Globalization (CRG), очолюваному Міше-

лем Чосудовським, професором економіки в університеті Оттави. Критики М.Чосудовського та його колег небезпідставно звинувачують їх в надмірному захопленні конспірологією. Адже список інвектив канадського дослідника та чільних співпрацівників його Центру на адресу США надто довжелезний. Америка, виявляється, винайшли особливий тип зброї, яка спричинила глобальне потепління; вони наперед знали про терористичні напади 11 вересня 2001 року та цунамі 2004 року, але не попередили ці катастрофи й т.п. Центр М.Чосудовського тісно співпрацює з розміщеним в Москві й очолюваний Борисом Кагарлицьким Institute for Globalization and Social Movements.

Чимало співпрацівників Centre for Research on Globalization є водночас членами наукового комітету італійського журналу Geopolitica (Eurasia, Rivista di Studi Geopolitici»; редактор Тіберіо Граціані), палкими захисниками євразійської співпраці та членами Вищої ради Міжнародного євразійського руху, очолюваного російським неофашистом Олександром Дугіним.

Більшість західних експертів старшої генерації належать до табору «совєтологів» або «кремленологів» (Sovietology&Kremlinology), які після краху СРСР розкололись на два великих табори: традиціоналістів та ревізіоністів. Типовим прикладом проросійськи налаштованого транзитолога-ревізіоніста є Стівен Коен (Stephen Frand Cohen), який наразі консультує американську телестанцію CBS News й водночас російський міжнародний пропагандистський телеканал Russia Today (RT). Окрім того, Стівен Коен є професором Нью-Йоркського й Прінстонського університетів та чільним співробітником наближеного до правлячої Демократичної партії, найстарішого в США, створеного ще в 1911 році, аналітичного центру (think tank) The Council on Foreign Relations (CFR), практично-аналітичним органом якого є часопис The Foreign Affairs. Стівен Коен набув репутації «апологета Путіна №1» й неодноразово піддавався гострій критиці у західному науково-академічних та медійно-аналітичних колах [8; 9; 10].

Саме таких політологів та політиків як Стівен Коен серед симпатиків України прийнято порівнювати з горезвісними західними учасниками «мюнхенської змови» 1938 р., які під приводом відвернення загрози нової війни пішли на далекосяжні поступки агресорові, – Адольфу Гітлеру, санкціонувавши аншлюс Австрії та розчленування Чехословаччини.

Проте, було б грубою помилкою вважати політологів, до групи яких належить Стівен Коен, «путінськими найманцями».

Вони, як і «мюнхенці» зразка 1938 р., передусім керуються міркуваннями національної безпеки США й країн західного блоку й саме тому посідають угодовську (опортуністичну) позицію стовно дій нинішнього політичного керівництва РФ. Псевдопацифістське формулювання «Чи варто підтримувати Україну в її збройному конфлікті з Росією?» теж має історичну аналогію в вигляді довоєнного запитання «Чи варто вмирати за Данциг?» (фр. Pourquoi mourir pour Dantzig?). Коли в травні 1939 р. Адольф Гітлер вперше випробував на міцність сусідню Польщу, пред'явивши їй ультиматум щодо передачі до складу Німеччини Вільного міста Данціг (нинішнього Гданська), французький політик-соціаліст Марсель Деа опублікував антивоєнну статтю «Вмирати за Данціг», спрямовану проти втручання Франції у Другу Світову війну й надання Польщі військової допомоги. Нинішні західні прибічники продовження політики залучення Росії до західного блоку держав попри усю ворожість до цього блоку й міжнародного миру, яку демонструє путінська Росія, є вочевидь уподібнюються до деяких французьких інтелектуалів зразка 1939 р.

Проте, в Україні є в середовищі західних інтелектуалів є й чимало симпатиків. Зокрема, ще в 1993 р. на сторінках Foreign Affairs, професор Чиказького університету Джон Міршаймер (John H. Mearsheimer) попереджав що адміністрація Білла Клінтона робить історичну помилку, стимулюючи ядерне роззброєння України, яка за іншої політики могла би перетворитися на надійний фактор стримування агресивних зазіхань Москви («Ukrainian nuclear weapons are the only reliable deterrent to Russian aggression»). При цьому Міршаймер попереджав також про неуникність українсько-російського воєнного зіткнення, прогнозуючи, що війна між Росією й Україною буде нещастям...Ймовірним наслідком цієї війни стане підкорення Росію України (Russia's reconquest of Ukraine), що обернеться сумними перспективами для миру в Європі (injure prospects of peace throughout Europe) [11].

Література

1. ProRussia // Wikipedia. [Електронний ресурс]. – Режим доступу: https://fr.wikipedia.org/wiki/ProRussia

2. Шеховцов, Антон. Проросійська мережа за лаштунками кампанії антиукраїнського наклепу // Українська правда. 04 лютого 2014. [Електронний ресурс]. – Режим доступу: http:// www. pravda.com.ua/articles/2014/02/4/7012704/

3. Симоньян, Маргарита. Интервью РБК: «Либеральное СМИ как раз мое» // РБК: [Електронний ресурс]. – Режим доступу: http://mediaprofi.org/community/interview/item/2810-siminyan_intrview

4. Draitcer, Eric. Ukraine and the Rebirth of Fascism // CounterPunch. January 24. 2014. [Електронний ресурс]. – Режим доступу: http://www.counterpunch.org/2014/01/29/ukraine-and-the-rebirth-of-fascism/

5. Engdahl, F. William. Ukraine: Secretive Neo-Nazi Military Organization Involved in Euromaidan Sniper Shootings // Global Research, November 22, 2014. [Електронний ресурс]. – Режим доступу: http://www.globalresearch.ca/ukraine-secretive-neo-nazi-military-organization-involved-in-euromaidan-snyper-shootings/5371611

6. Chossudovsky, Michel. Faulkner, Bonnie. Ukraine's «Democratic» Coup D'état: Washington's «Neo-Nazi Neoliberal» Proxy Government // Global Research, March 12, 2014. [Електронний ресурс]. – Режим доступу: http://www.globalresearch.ca/ukraines-democratic-coup-detat-washingtons-neo-nazi-neoliberal-proxy-government/5373073

7. Оксфорд критикуют за то, что он принял от олигарха благотворительный взнос в 75 млн фунтов // Инопресса. Ру. 04 ноября 2015. - [Електронний ресурс]. Режим доступу: http://www. inopressa.ru/ article/04nov2015/guardian/blav.html

8. Kirchick, James. Meet the Anti-Semites, Truthers, and Alaska Pol at D.C.'s Pro-Putin Soiree // The Daily Beast. June 17, 2014.

9. Chait, Jonathan The Pathetic Lives of Putin's American Dupes // New Yorker. March 14, 2014.

10. Chotiner, Isaac. Meet Vladimir Putin's American Apologist // New Republic. March 2, 2014.

11. Mearsheimer, John J. The Case for a Ukrainian Nuclear Deterrent // Foreign Affairs, Vol. 72, No. 3 (Summer 1993), pp. 50-66.

УДК 343.337.4

Олєйніков Д. О.
кандидат юридичних наук
Інститут підготовки юридичних кадрів для
Служби безпеки України Національного університету
«Юридична академія України імені Ярослава Мудрого»

ПРОТИДІЯ ОКРЕМИМ ПРОЯВАМ ІНФОРМАЦІЙНОЇ АГРЕСІЇ В КОНТЕКСТІ СТ.СТ. 111 ТА 436 КК УКРАЇНИ

Криміналізація злочину, передбаченого ч. 1 ст. 111 КК України, заснована на вимогах ст. 65 Конституції України, згідно з якою захист Вітчизни, незалежності та територіальної цілісності України є обов'язком громадян України. Захист Вітчизни – це не лише її оборона. Це і стан захищеності державного суверенітету,

конституційного ладу, територіальної цілісності, економічного, науково-технічного і оборонного потенціалу. Прагнення громадянина України свідомо надавати допомогу в розвідувально-підривній діяльності проти України, є зрадою інтересів держави і суспільства.

Зрада державі – це, по-суті, своєрідний різновид співучасті, у ході якої громадянин держави сприяє зовнішньому супротивникові, діючи у контакті, зв'язку та взаємодії із ним. У будь-якій формі державної зради громадянин здійснює ворожу діяльність на користь іноземної держави спільно з представниками цієї держави. Важливість цього положення полягає у тому, що у кожному конкретному випадку розслідування державної зради повинні бути встановлені психічні моменти, які стосуються усвідомлення особою того, що вона діє: а) на шкоду своїй державі; б) на користь іншої держави; г) у співучасті з представниками іноземної держави.

Державна зрада у формі надання іноземній державі, іноземній організації або їх представникам допомоги в проведенні підривної діяльності проти України охоплює найрізноманітніші способи надання допомоги іноземній державі, іноземній організації або їх представникам в проведенні підривної діяльності проти України, за винятком тих, які утворюють склади державної зради в формі шпигунства або переходу на бік ворога в умовах воєнного стану або в період збройного конфлікту. По суті, вона є загальною формою державної зради, а перехід на бік ворога і шпигунство, названі окремо в статті, є її більш поширеними різновидами, а тому державна зрада у формі надання іноземній державі, іноземній організації або їх представникам допомоги в проведенні підривної діяльності проти України має місце лише тоді, коли відсутні ознаки її конкретних різновидів. Так, законодавець обмежився вказівкою на ті моменти, які є конструктивними її ознаками: а) діяння полягає в наданні допомоги іноземній державі, іноземній організації або їхнім представникам; б) допомога перерахованим вище адресатам надається в їх підривній діяльності проти України; в) така підривна діяльність, як і будь-яка інша форма державної зради, спрямована на заподіяння шкоди суверенітетові, територіальній цілісності та недоторканості, обороноздатності, державній, економічній чи інформаційній безпеці України, що прямо закріплено в тексті ч. 1 ст. 111 КК України.

Державна зрада в формі надання іноземному представнику допомоги в проведенні підривної діяльності проти України в більшості випадків полягає у здійсненні активних дій, які можуть полягати як у вчиненні злочинів проти основ національної безпеки України, які, як відомо, є найбільш небезпечними злочинними актами проти нашої держави, у вчиненні інших злочинів, відповідальність за які передбачена відповідними розділами Особливої частини КК України. Можливі ситуації, коли суб'єкт, розуміючи, що його дії є складовою загальної системи протиправної підривної чи розвідувальної діяльності іноземного представника, діючи, не вчиняє жодного із злочинів, передбаченого КК України, тобто вчиняє дії, які, хоча й є підривною діяльністю проти України, проте не підпадають під ознаки жодного із злочинів, передбаченого Особливою частиною КК України.

В умовах фактичної збройної агресії проти України спеціальні служби країни-агресора деякий час проводили широкомасштабну підривну діяльність, спрямовану на те, щоб схилити частину населення певної території чи місцевості до підтримки свої збройних сил чи розвідувально-диверсійних підрозділів. Роздмухуючи ненависть до існуючого суспільно-політичного устрою України, чинного уряду, була сформована атмосфера, в якій громадяни України, що піддались ворожій пропаганді, навіюванню та маніпулюванню, вчиняли публічні заклики до агресивної війни або до розв'язування воєнного конфлікту, а також виготовляли матеріали із закликами до вчинення таких дій з метою їх розповсюдження або розповсюджували такі матеріали. Вказані вище дії, окрім ч. 1 ст. 111 КК України, містять також ознаки складу злочину, передбаченого ст. 436 КК України (пропаганда війни).

Разом з тим, як видно, практика досудового розслідування зазначеної сукупності злочинів відсутня, оскільки з часом увага та зусилля правоохоронних органів були спрямовані на протидію більш гострим та небезпечним проявам підривної діяльності. Така ситуація є недопустимою, оскільки саме «завдяки» створенню підґрунтя для формування терористичних організацій сепаратистські утворення, діяльність яких скеровується та інспірується спецслужбами РФ, отримали можливість безперешкодно діяти на території України.

Наразі в соціальних мережах накопичено достатньо інформації щодо конкретних персоналій осіб, які на початку антитеро-

ристичної операції на Сході України закликали до введення іноземних військ на територію України та проведення бойових дій з метою відторгнення окремих областей та утворення на їх місці квазідержав по типу терористичних угруповань «ЛНР» та «ДНР». Зазначені факти підривної діяльності повинні отримати належну кримінально-правову кваліфікацію, а особи, причетні до злочинної діяльності, за умови наявності в їх діях складів відповідних злочинів, повинні бути притягнуті до кримінальної відповідальності.

УДК 32.019.5 (477)

Панченко В. М.
кандидат технічних наук, старший науковий співробітник
Національна академія СБ України

ІНФОРМАЦІЙНЕ ПРОТИБОРСТВО В УМОВАХ РОСІЙСЬКОЇ АГРЕСІЇ ПРОТИ УКРАЇНИ: ОЦІНКИ ЗАХІДНИХ ЕКСПЕРТІВ

Завданням даного дослідження є аналіз публікацій західних фахівців, присвячених інформаційному протиборству під час російської агресії проти України [1], з метою використання висновків, отриманих ними з російсько-українського конфлікту, для визначення стратегічних напрямків протидії зовнішньому інформаційному впливу.

Насамперед слід зазначити, що на сьогодні західні науковці та експерти переважно розрізняють поняття кібернетичної та інформаційної війни, на відміну від науковців пострадянських країн, зокрема російських, які вважають кібернетичну війну складовою інформаційної.

Так, на основі вивчення подій, пов’язаних із російською агресією проти України, західні фахівці дійшли висновку, що основними засобами інформаційної війни Росії є ЗМІ, соціальні медіа, дипломатичні канали, неурядові організації та академічні структури. Тобто, інформаційна війна полягає у поширенні спеціально підібраного контенту різними каналами та мовами у термінах, близьких для цільової аудиторії. На відміну від пропаганди ра-

дянських часів, яка переважно була однонаправленою (зверху вниз), сучасна інформаційна війна охоплює аудиторію по всьому світу, яка одночасно є і носієм, і джерелом створення наративу. Це стало можливим завдяки потужному розвитку онлайн-платформ таких, як соціальні медіа, що забезпечують інтерактивну взаємодію власного населення країни, діаспори та зарубіжної аудиторії з подіями у реальному часі. Основними цілями інформаційної війни є зменшення здатності і бажання опонента до спротиву (суспільно-політичний вектор впливу), а також деградація\демотивація збройних сил опонента (військовий вектор впливу). З метою досягнення цих цілей застосовують такі методи: створення незручних та незрозумілих ситуацій (згадаємо «зелених чоловічків»), формування громадської думки, нанесення шкоди даним та сервісам, руйнування інфраструктури тощо.

Зарубіжні експерти зазначають, що гібридна стратегія, яка передбачає у тому числі використання інформаційних засобів впливу на опонента, не нова для Росії (згадаємо події у Фінляндії 1939 року, в Естонії 1991 року, за якими можна прослідкувати основні етапи захоплення територій: залякування, легітимізація незаконних дій, інформаційне супроводження у вигляді загрози вторгнення). Незвичним і новим стало виявлене з боку РФ уміння управляти інтенсивністю конфлікту шляхом застосування інформаційних засобів, контролювати наслідки інформаційних атак. Саме широке застосування засобів інформаційної війни – змусити опонента думати і діяти у власних інтересах без застосування кінетичних сил (або з мінімальними жертвами та руйнуваннями) – нова і неочікувана для натівських країн стратегія. Адже раніше, до подій в Україні, інформаційна війна в розумінні союзників зводилась до війни кібернетичної – руйнування інфраструктури через автоматизовані системи управління, порушення системи управління через вплив на системи зв'язку тощо.

Аналізуючи події в Україні, західні фахівці відверто здивовані низькою інтенсивністю застосування кібернетичних засобів. Адже і Росія, й Україна мають значний потенціал в ІТ сфері, архітектура української інформаційної та телекомунікаційної інфраструктури добре відома росіянам, оскільки розбудовувалася у радянські часи та, за оцінками експертів, 90% телекомунікаційної інфраструктури України знаходиться у власності громадян РФ. Тому здійснення кібератак на неї надто легке завдання для росій-

ської сторони. З іншого боку, Україна знаходиться серед 10 країн світу із найбільшим рівнем кіберзлочинності, а також посідає п'ятнадцяте місце як країна, з доменів якої здійснюються DDoS-атаки. Зауважимо, що високий рівень кіберзлочинності в Україні обумовлений наявністю традиційної для пострадянських країн школи фізико-математичних наук, яка забезпечує підготовку висококваліфікованих ІТ-фахівців при відсутності розвиненої галузі інформаційних технологій та низьких зарплатах представників технічних професій у державних структурах у порівнянні з доходами від кіберкрадіжок.

Найбільш значимими кіберінцидентами за час російсько-українського конфлікту, на думку західних фахівців, були:

- листопад 2013 – російські хакери підмінили контент та здійснили DDoS-атаки на низку веб-сайтів українських телевізійних мовників, новинних ресурсів та політиків;
- лютий 2014 – російські війська здійснили фізичне від'єднання оптоволоконного кабелю між континентальною Україною і Кримом та отримали контроль над точкою доступу, що призвело до втрати мобільного, проводового зв'язку та інтернет-з'єднання з півостровом;
- березень 2014 – офіційні веб-сайти кількох міністерств та відомств України були недоступні протягом близько 72 годин, велика кількість урядових та новинних проукраїнських сайтів були піддані DDoS-атакам, велика кількість народних депутатів повідомили про злам їхніх мобільних телефонів;
- травень 2014 – проросійські активісти з «Кіберберкуту» взяли на себе відповідальність за порушення порядку роботи електронної системи Центральної виборчої комісії України, що полягало у підміні результатів голосування на виборах Президента;
- грудень 2015 – були здійсненні кібертатаки на Прикарпаттяобленерго, що призвели до припинення електропостачання на території Івано-Франківської області.

Таким чином, найбільш поширені форми кібератак - на критичну інфраструктуру та системи оборони - широко не застосовувалися під час конфлікту. На думку західних експертів, це обумовлено такими причинами:

- Україна не має достатньо висококваліфікованих хакерів;
- в Росії та Україні немає вагомих мішеней для кібератак;
- оскільки основними власниками української телекомунікаційної інфраструктури є російські бізнесмени, немає потреби її

руйнувати – російські спецслужби мають повний контроль над телекомунікаційною інфраструктурою України;

- ні Росія, ні Україна не хочуть ескалації конфлікту, а тому стримували застосування своїх можливостей у кіберпросторі;

- кіберзасоби не є «срібною кулею», яка вирішує всі проблеми, тобто при порівняній дешевизні та доступності кіберінструментарію його застосування було не завжди виправданим.

Так, прийом фізичного від'єднання інтернету в Криму від континентальної України шляхом отримання контролю над точкою доступу та пошкодження оптоволоконного кабелю став несподівано успішним для самих росіян, тому ймовірно вони будуть шукати можливість його застосування в інших конфліктах і слід передбачити захист від загрози такого типу, коли фізична втрата зв'язку ефективніше програмних засобів впливу. З іншого боку, перевагою інтернет-архітектури континентальної України є велика кількість точок доступу, отримати контроль над усіма неможливо, але їх переважна більшість знаходиться у російській власності. Отже, при плануванні кібератак велике значення має архітектура телекомунікаційної мережі об'єкта впливу.

Російська агресія проти України ще раз підтвердила гіпотезу про те, що тип атаки у кіберпросторі відповідає стратегічній культурі нападника, що у свою чергу корелює з іншим не менш відомим твердженням – тип політичного режиму держави визначається та визначає в ній панівний тип політичної комунікації, що в свою чергу впливає на формування телекомунікаційної системи цієї держави [2]. Зокрема, відомі кібератаки на іранську ядерну АЕС відповідають військово-політичній стратегії США – знищення інфраструктури з мінімальними жертвами. Для Китаю характерне приховане викрадення інформації під гаслом захисту власного населення від згубного американського впливу, для Росії – гібридна війна, що полягає в одночасному застосуванні тиску у кількох напрямках. Кібератаки ефективно використовувались російськими спецслужбами на тактичному та операційному (інструментальному) рівнях в Криму (кібершпіонаж, інформаційна ізоляція) та на Донбасі (розсилання листів з метою психологічного тиску, корегування вогню, засилання дронів за аналізом трафіку мобільних пристроїв українських військових, психологічний тиск на родичів мобілізованих українців, вербування бойовиків). На думку західних фахівців, у порівнянні з конфліктами в

Естонії (2007) та Грузії (2008), Росія не мала наміру розголошувати, демонструвати свої кіберпотужності, тому використовувала кіберзасоби не на стратегічному, а на тактичному рівні, як засіб підтримки основної операції. При цьому акцент був на маніпулюванні контентом у той час, як кіберзасоби широко використовувались з метою шпіонажу, але не з метою знищення інфраструктури чи військового потенціалу. Перші два прийоми (маніпулювання та шпіонаж) давали достатньо інформації для розуміння ситуації та управління нею у власних інтересах настільки, що фізична руйнація стала економічно та політично невиправданою.

Події, які характеризують інформаційне протиборство Росії та України засвідчили, що кіберзасоби створюють операційний простір, у якому держави можуть проводити наступальні дії з меншим політичним ризиком, оскільки: 1) відсутні нормативні акти, які регулюють міждержавні відносини у кіберпросторі; 2) завжди існує можливість заперечити свою причетність до кіберінцидентів за рахунок залучення у конфлікт недержавних суб'єктів, а також суб'єктів неявно контрольованих державою, що ускладнює/унеможливлює притягнення агресора до юридичної відповідальності. Таким чином, на сьогодні кібернетичні засоби стали невід'ємною складовою конфліктів та воєн, і як би вони не застосовувалися – як складова війни інформаційної або як бекграунд (підготовка та супроводження) військових операцій – вони розмивають кордон між миром та війною, що позбавляє можливості апелювати для вирішення конфлікту до міжнародного законодавства, навіть якщо ім'я агресора вже не можна приховати. Зокрема, правова оцінка дій РФ щодо України на підставі міжнародних нормативних актів, надана експертами НАТО, визнає анексію Криму міждержавним протистоянням (незаконне захоплення однією державою території іншої суверенної держави у порушення Будапештського меморандуму 1994 року та Угоди про дружбу, взаємодію та партнерство 1997 року, а також статті 2 (4) Статуту ООН про незастосування сили), у той час як агресію на сході України не можна кваліфікувати як міжнародний збройний конфлікт, оскільки діяльність сил РФ у цьому регіоні не відповідає критерію «повного контролю» (щоб відповідати критерію «повного контролю», держава «повинна не тільки фінансувати, тренувати, екіпірувати або надавати операційну підтримку місцевим силам, але й відігравати роль організатора, координатора та

планувати їх діяльність» [1, С.130]). Це відкриває можливості для маніпулювання громадською думкою, адже у дискурсі європейських ораторів стосовно подій на Донбасі замість «не міжнародний» (non-international) часто вживається термін «внутрішній (internal) конфлікт», що автоматично сприймається як «громадянська війна» в Україні. А це значно обмежує можливості України в отриманні іноземної підтримки та/або міжнародної допомоги.

Слід також звернути увагу на те, що дослідження російсько-українського конфлікту західними фахівцями спрямовані, насамперед, на визначення загроз і наслідків російської агресії для країн Заходу, а не на вирішення проблем України. Серед таких загроз - атака на європейські цінності, спроба скомпрометувати стратегію НАТО щодо стримування війни, загроза розпочати збройний конфлікт у Європі. Усвідомлюючи провокативний характер дій російського уряду та високу ймовірність їх негативних наслідків, країни Альянсу не поспішають із різкими заявами та радикальними кроками, навіть незважаючи на незаконність анексії Криму. Крім того, затримка у наданні допомоги Україні, на нашу думку, може бути обумовлена й тим, що особи, які приймають рішення, так само на певний час стали жертвами російської інформаційної війни. Отже, необхідно усвідомлювати, що для Заходу сценарій локальної нестабільності в Україні є найменш агресивним, а отже і найбільш сприятливим у порівнянні із такими сценаріями, як «залякування кіберінцидентами» країн-членів НАТО (на кшталт появи підводних човнів в акваторії Норвегії або порушення кордонів повітряного простору країн НАТО), «заморожений кіберконфлікт» (через порушення функціонування інтернету), «примушення до миру» (через кібератаки на фінансові та оборонні телекомунікаційні системи країн НАТО) [1, С. 155].

Насамкінець, висвітлимо ще декілька проблемних для України питань, на яких акцентували увагу у своїх публікаціях західні фахівці:

1) у 2015 році РФ має дійсно продуману військову доктрину з питань кібернетичного та інформаційного протиборства, у той час як Україна у цьому напрямку перебуває лише на етапі становлення;

2) на рівні стратегічних комунікацій під час конфлікту Росія створила собі імідж «незамінного переговорника». Натомість, Україна орієнтується на Захід та НАТО, тобто не має власної по-

зиції. Росія сконцентрувала увагу на національних інтересах, у той час як Україна апелює до міжнародної спільноти для розуміння і підтримки;

3) незважаючи на те, що українські експерти з кібербезпеки налагодили обмін інформацією із західними колегами, зокрема в межах роботи CERT та кримінальних справ, ця співпраця не є настільки ефективною, якою б вона могла бути, у зв'язку із тим, що Захід поки що недостатньо поважає та довіряє українським фахівцям та не надає повну інформацію;

4) незважаючи на порівняно велику кількість патріотично налаштованих кіберборців в Україні, українські урядові структури не змогли інтегрувати, об'єднати, скоординувати, підпорядкувати єдиній меті ці сили для реалізації спільних потужних акцій, не змогли забезпечити управління ними – можемо констатувати факт відсутності інтегрованих національних потужностей/можливостей (на відміну від Росії, яка має можливість фінансово мотивувати «недержавних» суб'єктів протиборства у кіберпросторі). Найбільш кваліфіковані ІТ-фахівці в Україні – кіберзлочинці – не залучені до акцій протидії зовнішньому агресору на користь національним інтересам України, їх не вдалося зацікавити діяльністю, що не приносить прибуток.

Разом з тим, західні експерти відзначають, що Україна має потенціал для того, щоб стати рівноправним суб'єктом інформаційного протиборства в кібернетичному просторі. Адже, як свідчить досвід Естонії (невеликої за територією та кількістю населення країни), фінансові та військові потужності держави, навіть такої як Росія, не є визначальними для забезпечення інформаційного суверенітету.

З огляду на викладене, можемо зробити такі висновки. Західна експертна думка розрізняє поняття кібернетичної та інформаційної війни, не встановлюючи відношення підпорядкованості між ними. Натомість вважається, що ці поняття мають різну природу: інформаційна війна - поширення спеціально підібраного контенту різними каналами (ЗМІ, соціальні медіа, дипломатичні канали, неурядові організації, академічні структури); кібернетична війна – руйнація або порушення порядку функціонування інформаційних та телекомунікаційних систем.

Засоби інформаційної та кібернетичної війни можуть застосовуватися як складові одного задуму, так і в окремих операціях

військово-політичного характеру. Так, кіберзасоби використовувалися для підготовки до кінетичних чи інформаційних операцій, формування власного наративу для загалу, у тому числі міжнародного. У свою чергу, заходи інформаційного впливу не вимагають обов'язкового застосування кіберзасобів.

Водночас, під час російсько-українського конфлікту найбільшу ефективність виявили саме засоби інформаційного війни, не в останню чергу через недостатню розвиненість ІТ-галузі в Україні та порівняно низький рівень інформатизації об'єктів критичної інфраструктури й оборонної сфери. При цьому росіяни стали несподівано успішними в управлінні інтенсивністю конфлікту за допомогою інформаційних засобів. Це ще раз свідчить про хибність орієнтації на західний підхід при формуванні переліку галузей знань та спеціальностей вищої освіти в Україні, який не передбачає підготовку фахівців за спеціальністю «Інформаційна безпека». Нагадаємо, що новий перелік галузей знань та спеціальностей, затверджений Постановою Кабінету Міністрів України від 29.04.2015 № 266, не містить галузі знань «Інформаційна безпека». Натомість пропонується підготовку фахівців для цієї галузі здійснювати в межах спеціальності «Кібербезпека» галузі знань «Інформаційні технології».

Як кібернетичні засоби «розмивають кордон між миром та війною», що позбавляє можливості апелювати при вирішенні конфлікту до міжнародного законодавства, так інформаційні операції розмивають кордон між правдою та неправдою, реальністю та видуманими фактами, що ускладнює прийняття рішення та змушує об'єкта інформаційного впливу діяти не на користь власним інтересам.

Навіть невеликі країни можуть отримати переваги у кіберпросторі над країнами, які мають значні ресурси та потужний військовий потенціал. На сьогодні в Україні є всі передумови для того, щоб вона стала рівноправним суб'єктом інформаційного протиборства в кібернетичному просторі. Але для цього необхідно нарешті позбавитись залежності від думки інших, і почати діяти у власних інтересах. Адже проведене дослідження красномовно свідчить, що увага західних фахівців до російсько-українського конфлікту обумовлена, насамперед, необхідністю захисту країн НАТО від наслідків російської агресії, а не вирішення проблем України.

Література

1. Cyber War in Perspective: Russian Aggression against Ukraine / Kenneth Geers (Ed.) - Tallinn: NATO CCD COE Publications, 2015. – 175 p.
2. Литвиненко О. Інформаційні впливи та інформаційні операції: механізми самоорганізації / О.В.Литвиненко // Людина і політика. — 1999. — № 6. — С. 32-36.

УДК 159.9.075

Пилипенко В. М.
Львівський державний університет безпеки життєдіяльності
Гриник Р. О.
Львівський державний університет безпеки життєдіяльності

ОСОБЛИВОСТІ СПЕЦПРОПАГАНДИ ЯПОНІЇ У ДРУГІЙ СВІТОВІЙ ВІЙНІ

Ґрунтовного дослідження й узагальнення потребує організація та здійснення інформаційно-психологічного впливу Японією на власних громадян та державу в цілому. До засобів ведення Японії інформаційно-пропагандистської війни потрібно віднести комплекс заходів щодо зародження серед військовослужбовців і усього японського народу культу так званих “камікадзе”. Не маючи військової переваги над американцями, відтягуючи неминучий програш, японці намагалися залякати противника атаками смертників [1]. Найбільшу увагу японці приділяли питанням консолідуючої пропаганди, називаючи її “політичною війною”, яку, за їхньою оцінкою, не можна доводити до того, щоб уряд захопленої країни не погодився зі своєю плачевною участю, а промисловість давала незадовільні результати. Японія повністю контролювала економіку окупованих країн, оборот і друк грошей без найменшого покриття, здійснювали конфіскацію будь-якого виду підприємств, доводячи їх до краху, а згодом викуповували засоби виробництва за безцінь. Японські загарбники обмежували засоби контактування, тероризували, підвищували ціни на продукти першої необхідності, зачиняли лікарні та шкільні установи. Окупанти мали певний банк підтримки у місцевого населення, яке через своє лояльне ставлення не чинило спротиву їхнім діям [2].

Всі захоплені японцями радіостанції працювали в режимі «гострої пропаганди», газети друкувались максимальними тира-

жами, видавалося велике число книг, що пропагують військові ідеї, показуючи агресію Японії проти сусіднього Китаю [1]. У 1937-1939 рр. в Японії особливо активно пропагувалася вірність імператору, возвеличення його культу особи. Як і внутрішня так і зовнішня пропаганда Японії носила відверто антирадянський характер. Спостерігаючи за політикою і військовими формуванням фашистської Німеччини в 1938 р., уряд Коное і командування збройних сил Японії все більше схилялась до думки, що вирішальний бій за «перерозподіл» буде бій між Німеччиною і СРСР, і тому вважали, що військовий союз з Німеччиною повинен спрямовуватись тільки проти Радянської держави. Для пропаганди глобальних державних цілей в 1941 р. була створена масова націоналістична організація "Східноазіатська ліга великої Японії". Своєрідною "біблією" тенноїзму стала в цей час брошура видана в 1937 р. Міністерством освіти, "Основні принципи імператорського шляху", яка складається з ідей, що полягають "підданим великої Японської імперії", заснована на визнанні "божественного" походження імператорської династії, вона використовувалася в якості основного "морального виховання" молодого населення Японії в шкільних закладах та в університетах [3].

Коли були знищені зародки пропаганди гуманізму і міжнародного соціалізму, розпочалось активне виховання молоді через наукові і художні видання, театр і кіно, що повинно було викликати у них поняття шовінізму, проповіді культу війни і ненависті, для насаджування божевільних ідей завоювання всієї Азії та створення могутньої азіатської імперії під головуванням Японії. Мілітаризація всіх галузей життя японського суспільства напередодні другої світової війни прийняла глобальний характер [2]. Таким чином, восени 1939 року Японія швидкими темпами готувалася до війни з метою створення азіатської імперії. При цьому загарбницькі задуми японського імперіалізму аж ніяк не обмежувалися Азією і басейном Тихого океану.

Провал в пропагандистській війні японці зазнали тільки завдяки військовій перемозі суперника. У такому розумінні ядерне бомбардування Хіросіми та Нагасакі 6 і 8 серпня 1945 року було психологічною атакою американців на стратегічному рівні – боротьбою за місце у світовій політиці після військового періоду, початком ери демонстрації сили в «холодній війні».

Отже, аналіз ведення пропаганди Японією в роки Другої світової війни свідчить про те, що вона формувала менталітет

громадян згідно культу камікадзе. Основний удар пропаганди відносився до військовослужбовців збройних сил, вербування їх у так званих смертників-камікадзе. Провідними формами інформаційно-пропагандистської війни були друкована продукція та радіопропаганда. Також велася широкомасштабна націоналістична пропаганда. Перший значимим пунктом якої була расистська теорія переваги японського народу над іншими націями. Проголошувалася непримиренна боротьба з комуністичним і прогресивним рухом не тільки в Японії, але і по всій території Азії. Особлива жорстокість виявлялася щодо Радянського Союзу, чиї далекосхідні землі давно не давали спокою правлячій владі Японії.

Література

1. Волковский Н.Л. История информационных войн : в 2 ч. Ч. 2 / Н. Л. Волковский. – СПб. : Полигон, 2003.– 736 с.

2. История Второй мировой войны. 1939–1945 : в 12 т. – М. : Воениздат, 1973–1982.

3. Крысько В. Г. Секреты психологической войны (цели, задачи, методы, формы, опыт) / В. Г. Крысько ; под общ. ред. А. Е. Тараса. – Минск : Харвест, 1999. – 448 с.

УДК 323:007(477)

Присяжнюк М. М.
кандидат технічних наук, старший науковий співробітник
Національна академія СБ України

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ МЕХАНІЗМИ ФОРМУВАННЯ ІМІДЖУ УКРАЇНИ

В умовах глобалізації, політичної модернізації та формування інформаційного суспільства Україна прагне бути конкурентоспроможною на міжнародній арені. Такі поняття як імідж, репутація розглядаються як необхідні складові стратегічного надбання держави.

Формування позитивного іміджу держави можливе за двох умов: ефективної внутрішньої і зовнішньої політики та інформаційно-комунікаційного забезпечення цієї політики. За умови незначних успіхів у внутрішній і зовнішній політиці імідж держави формується за допомогою інформаційно-комунікаційних механі-

змів і технологій піару. Формування позитивного іміджу, як правило, включає висвітлення найбільш успішних результатів діяльності держави, значення яких може перебільшуватися. Наприклад: «руїни подолані», «зарплата повільно, але зростає, а раніше й цього не було», «країна впевнено дивиться в майбутнє» тощо.

Як відомо, іміджу властивий значний елемент міфологічного. Люди сприймають навколишній світ головним чином через існуючі й постійно відтворювані політичні міфи та стереотипи. Проте, будь-який міф рано чи пізно втрачає свою привабливість, якщо він постійно не підкріплюється певними фактами. Ці завдання покладаються на інформаційні служби та засоби масової комунікації, які висвітлюють події в необхідному ракурсі.

Політичний імідж часто вибудовується не на реальних фактах, а на штучно створеному образі чи міфі, який для переконливості повинен базуватися на реальній інформації. Створений міф часто спрацьовує, бо громадська думка сприймає за правду те, у що їй хочеться вірити.

Важливим фактором формування позитивного іміджу держави є інформаційно-комунікаційні механізми і технології. Так в Окінавській Хартії глобального інформаційного суспільства інформаційно-комунікаційні технології зафіксовано як один із найбільш важливих факторів, що впливає на формування суспільства XXI століття.

Враховуючи, що з розвитком інформаційної революції особливе значення при формуванні зовнішньополітичного іміджу держави мають засоби масової комунікації, важливу роль при цьому має відігравати державна інформаційна політика, розвиток міжнародних зв'язків з громадськістю та публічна дипломатія.

Усе більшої популярності набувають інноваційні інформаційні технології, а саме Інтернет, що змінює комунікаційні процеси. Завдяки сучасним інформаційно-комунікаційним технологіям кожен бажаючий користувач Інтернету може створити особистий блог, який здатен виконувати функції засобу масової інформації та комунікації.

Основними напрямками здійснення зовнішньополітичних іміджевих комунікацій у мережі Інтернет є створення та підтримка веб-порталів, використання веб-сайтів зовнішньополітичного відомства та дипломатичних представництв за кордоном із відповідним інформаційним наповненням та мовною доступністю;

створення на цих веб-порталах та веб-сайтах служб тематичних інформаційних розсилок; публікація іміджевих матеріалів як на власних веб-ресурсах, так і у світових Інтернет-виданнях та стрічках новин; використання доменних імен; контроль за іміджем держави в мережі тощо.

З метою створення позитивного іміджу України необхідно активно застосовувати рекламно-інформаційні технології. Для того, щоб наша держава сприймалася в міжнародному просторі як надійний і передбачуваний партнер, що розділяє європейські демократичні цінності, необхідно задіяти такі інформаційно-комунікаційні механізми, як:

- налагодження комунікації з міжнародними громадськими організаціями, що симпатизують Україні й готові співпрацювати з метою формування позитивного іміджу країни за кордоном;
- створення власних та співпраця із закордонними ЗМІ з метою ознайомлення міжнародної громадськості з принципами своєї зовнішньої і внутрішньої політики;
- заснування інформаційних центрів, органів зовнішньополітичної пропаганди, агентств, завданням яких повинна бути роз'яснювальна робота з цільовими аудиторіями і формування певної думки про Україну;
- організація супутникового мовлення в міжнародному інформаційному просторі українською та англійською мовами;
- включення кращих іміджевих вітчизняних телевізійних програм у пакети кабельного телебачення іноземних держав;
- організація науково-практичних конференцій, прес-конференцій, зустрічей з представниками міжнародної громадськості;
- активне залучення Інтернет ресурсів та їх наповнення іміджевим матеріалом;
- широке використання прийомів і методів PR.

Варто зазначити, що всі ці механізми стануть корисними лише за умови усунення існуючих внутрішньополітичних проблем, що негативно впливають на імідж держави й досягнення реальних успіхів у соціально-економічному розвитку країни та зміцненні авторитету державної влади.

Література

1. В.М. Петрик, М.М. Присяжнюк, Д.С. Мельник та ін. Забезпечення інформаційної безпеки держави: підручник. – К.: ПАТ «Віпол», 2015. – 672 с.

2. Семченко О.А. Іміджева політика України // О.А. Семченко. – Монографія. – К.: ВЦ «Академія», 2014. – 272 с.

3. Качинська Н.О. Комунікативні тактики формування привабливого міжнародного іміджу держави / Н.О. Качинська // Гілея: науковий вісник. Збірник наукових праць. – К.: ВІР УАН, 2010. – Випуск 36. – С. 318 – 329.

УДК 55.244.1:356.255.2

Рогов П. Д.
кандидат технічних наук
Національний університет оборони України
імені Івана Черняховського;
Ткаченко В.А.
кандидат військових наук,
Національний університет оборони України
імені Івана Черняховського

СТРАТЕГІЧНІ КОМУНІКАЦІЇ ЯК ОСНОВА ПІДГОТОВКИ ТА ПРОВЕДЕННЯ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ

Інформаційна безпека держави є невід'ємною складовою кожної зі сфер національної безпеки. Це повною мірою стосується інформаційної безпеки держави у воєнній сфері, яка є важливою самостійною складовою забезпечення національної та воєнної безпеки. Саме тому розвиток України як суверенної, демократичної, правової й економічно стабільної держави, з високим рівнем воєнного потенціалу та захищеною інформаційною інфраструктурою її Сектору безпеки й оборони можливий тільки за умови забезпечення належного рівня інформаційної безпеки у воєнній сфері, зокрема, своєчасного виявлення інформаційних загроз та прийняття відповідних превентивних заходів захисту.

Протидія небажаному інформаційному впливу передбачає проведення широкого спектра інформаційних (інформаційно-психологічних) операцій, пасивних і активних дій та заходів (пасивних - підвищення захищеності інформаційної інфраструктури; активних - попередження, стримування та ефективне безпосереднє реагування на інформаційний вплив).

Воєнна доктрина України визначає "стратегічні комунікації" як скоординоване й належне використання комунікативних

можливостей держави — публічної дипломатії, зв'язків із громадськістю, військових зв'язків, інформаційних та психологічних операцій, заходів, спрямованих на просування цілей держави [1]. Головна та ключова засада комунікацій: гарантування реалізації національних інтересів [2]. Для повного розуміння змісту стратегічних комунікацій потрібно з'ясувати складові інформаційної сфери, в яких реалізується державна інформаційна політика [2-4]: інформаційної безпеки; електронного урядування; розвитку інформаційного суспільства; інформатизації; захисту (інформаційних) прав і свобод людини та громадянина; інформаційних та психологічних операцій, Збройними Силами України; функціонування та розвитку медіапростору тощо.

Відповідно до [2 - 4], можна виділити компоненти системи забезпечення стратегічних комунікацій, взявши за зразок стандарти НАТО при підготовці та проведенні інформаційних операцій (далі – ІО) збройними силами тощо, де питанням стратегічної комунікації приділена надзвичайна питома вага: зв'язки з громадськістю та ЗМІ; публічна дипломатія та військові заходи на підтримку публічної дипломатії; інформаційні заходи міжнародного військового співробітництва; цивільно-військове співробітництво; дії в кіберпросторі, включаючи соціальні мережі; залучення ключових лідерів до проведення інформаційних заходів; внутрішня комунікація (робота з особовим складом/внутрішній PR); самі інформаційні та психологічні операції; інформування про ситуацію та документування подій на полі бою; розвідувальне забезпечення проведення інформаційних заходів; показ дій військ; введення в оману; безпека операцій; фізичний вплив; протиборство в електромагнітному просторі. Таким чином, стратегічні комунікації - це процес, від ефективності якого безпосередньо залежить реалізація державної інформаційної політики і забезпечення національної безпеки України в цілому, інформаційної безпеки у воєнній сфері, ефективність проведення ІО тощо, до здійснення якого залучені не лише суб'єкти стратегічних комунікацій, а й суб'єкти з інших сфер діяльності.

З метою упорядкування термінів та визначення їх понять доцільно сформувати такі групи основних термінів системи забезпечення стратегічних комунікацій з точки зору підготовки та проведення ІО, а саме: терміни, що визначають наукову основу стратегічної комунікації; терміни, що визначають предметну основу стра-

тегічної комунікації; терміни, що визначають характер діяльності (дій) щодо системи забезпечення стратегічних комунікацій.

До термінів, що визначають наукову основу стратегічної комунікації, слід віднести терміни, які використовуються в багатьох галузях знань, що мають відношення до інформаційній сфери та сфери інформаційної безпеки, ІО тощо, вони є однозначними, семантично уніфікованими і стилістично нейтральними. Терміни цієї групи мають відповідають вимогам однозначності та стійкості, тобто ці терміни однозначно вживаються в одній галузі знань і зберігають свій особливий сенс в кожній іншій галузі знань, а також є загальновизнаними.

До термінів, що визначають предметну основу стратегічних комунікацій щодо ІО слід віднести терміни, що означають поняття та їх співвідношення з іншими поняттями в межах інформаційної безпеки держави (як спеціальної сфери або галузі знань).

До термінів, що визначають характер діяльності (дій) щодо системи забезпечення стратегічних комунікацій стосовно забезпечення ІО слід віднести терміни, що служать позначеннями характерних для інформаційної сфери предметів, явищ, процесів, їх властивостей і стосунків (у тому числі сил, засобів та методів їх використання при рішенні завдань забезпечення інформаційної безпеки держави) щодо скоординованого і належного використання комунікативних можливостей держави. Терміни цієї групи означають широкий круг понять різного рівня: від технічного каналу інформаційного впливу до інформаційного протиборства (війни).

Інформаційну роботу під час інформаційної операції потрібно проводити так, щоб противник сперечався сам з собою; управління конфліктною ситуацією – створити таку атмосферу в стані та суспільстві противника, коли люди цієї держави самі починали домовлятися з нами; не вирішувати, що є правильним або неправильним.

Водночас, при підготовці до процесу реалізації системи стратегічних комунікацій в системі забезпечення ІО слід виокремити окремі блоки завдань, до яких можна віднести: аналіз ситуації; дослідження проблеми; комунікаційні ризики та потенційні можливості; стратегічно-операційні завдання; стратегічно-комунікаційні задачі; суб’єкти стратегічної комунікації; стратегічно-комунікаційна стратегія; стратегічно-комунікаційна тактика; оцінка ефективності; період часу і бюджет.

Література

1. Указ Президента України № 555/2015 «Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року «Про нову редакцію Воєнної доктрини України». Електронний ресурс : http://www.president.gov.ua/documents/5552015-19443.

2. В. А. Ліпкан. Роль стратегічних комунікацій в протидії гібридній війні проти України http://goal-int.org/rol-strategichnix-komunikacij-v-protidii-gibridnij-vijni-proti-ukraini/

3. В. А. Ліпкан. Експертний висновок на проект Стратегії розвитку ефективних комунікацій у ЗСУ http://goal-int.org/ekspertnij-visnovok-na-proekt-strategii-rozvitku-efektivnix-komunikacij-u-zsu/

4. Daniel Gage. The continuing evolution of Strategic Communication within NATO // The Three Swords Magazine 27/ 2014 p. 53—55.

УДК 005.3

Романов М. С.

кандидат юридичних наук, старший науковий співробітник,
доцент Національна академія СБ України

РАДІОЕЛЕКТРОННІ ЗАСОБИ ЗВ'ЯЗКУ ТА ЇХ ВПЛИВ НА КОНТРРОЗВІДУВАЛЬНИЙ РЕЖИМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

До контррозвідувального режиму, зазвичай, відносять окремі норми адміністративно-правових режимів охорони державних таємниць, державного кордону України, прикордонного, виїзду з України і в'їзду до неї, митного, внутрішньооб'єктового, надзвичайного стану, паспортного, перебування іноземців в Україні, користування повітряним транспортом, пропускного, судноплавства та деяких інших . У тім, цей перелік уявляється неповним. Так, в сучасних умовах важливим інструментом розвідувально-підривної діяльності спецслужб іноземних держав є радіоелектронні засоби (далі – РЕЗ) зв'язку, як важливий інструмент впливу на контррозвідувальний режим в Україні.

Контррозвідувальний режим у сфері використання РЕЗ в Україні охоплює елементи адміністративно - правових режимів: 1) телекомунікацій; 2) користування радіочастотним ресурсом; 3) радіомовлення і телебачення; 4) протидії використанню РЕЗ

технічної розвідки. Вони формуються нормативно-правовими актами міжнародного і національного рівней, останній – тільки актами національного законодавства.

Міжнародно-правову основу адміністративно-правових режимів користування радіочастотним ресурсом і телекомунікацій, у тому числі радіомовлення і телебачення, закладено Статутом Міжнародного союзу електрозв'язку (далі – Статут), Конвенцією міжнародного електрозв'язку (далі – Конвенція), Регламентом радіозв'язку і Регламентом міжнародного електрозв'язку. Так, зі статей 34, 37 Статуту випливає, що будь-яка держава (у т.ч. Україна) має право: 1) без інформування передавальної станції організаційними заходами або створенням перешкод перервати зв′язок будь-якої юридичної або фізичної особи, яка не репрезентує офіційно іншої держави у разі, якщо такий зв′язок загрожуватиме безпеці країни; 2) вправі здійснювати пошук і перехоплення принаймні міжнародних повідомлень електрозв′язку, котрі містять дані про загрози державній безпеці . Положення згаданих міжнародних нормативно-правових актів утворюють фундамент національного законодавства в галузі телекомунікацій, користування радіочастотним ресурсом, телебачення та радіомовлення. В Україні загальний порядок використання РЕЗ у вказаних областях регламентовано законами України „Про телекомунікації", „Про радіочастотний ресурс", „Про радіомовлення і телебачення".

На забезпечення контррозвідувального режиму безпосередньо впливає припис п. 2 ст. 33 Закону України „Про телекомунікації", яким споживача телекомунікаційних послуг зобов'язано не допускати використання свого кінцевого обладнання для вчинення дій, що суперечать інтересам національної безпеки. Очевидно, що порушення цього зобов'язання спричиняє внутрішні загрози національній безпеці України (залежно від характеру дій порушника - у сферах державної, інформаційної безпеки тощо), отже, контролювати його дотримання негласними (оперативними) методами контррозвідувальної діяльності повинна СБ України. Приписом п. 3 ст. 9 Закону «Про телекомунікації», операторів та провайдерів телекомунікацій зобов'язано вживати відповідно до законодавства технічних та організаційних заходів із захисту телекомунікаційних мереж, засобів телекомунікацій, інформації з обмеженим доступом про організацію телекомунікаційних мереж

та інформації, що передається цими мережами, - тобто, забезпечувати технічний і криптографічний захист інформації (далі – ТЗІ і КЗІ). Згідно зі ст. 1 Закону України „Про державну таємницю", ТЗІ і КЗІ є складовими заходів з охорони державної таємниці. Із положень ст. 36 цього Закону та п.2 ст. 6 Закону України „Про контррозвідувальну діяльність" випливає, що стан захисту державної таємниці негласно контролюється СБ України у ході оперативно-розшукової та контррозвідувальної діяльності. Отже, приписом п. 3 ст. 9 Закону України „Про телекомунікації" фактично визначається потреба у здійсненні СБ України негласного контррозвідувального контролю за станом технічного і криптографічного захисту державної таємниці, що обертається в телекомунікаційних мережах загального користування. Під час реалізації цієї функції підрозділами радіоконтррозвідки виявляється робота РЕЗ, функціонування яких створює загрози витоку інформації з обмеженим доступом (з одного боку, незахищених у встановленому порядку РЕЗ телекомунікацій, з іншого – РЕЗ технічної розвідки).

Згідно зі ст. 6 Закону України „Про телебачення та радіомовлення", не допускається використання телерадіоорганізацій, зокрема, для поширення відомостей, що становлять державну таємницю, або іншої інформації, яка охороняється законом, закликів до насильницької зміни конституційного ладу України. Відповідно до ст. 6 Закону України „Про основи національної безпеки", однією із загроз національній безпеці в інформаційній сфері визначено намагання маніпулювати суспільною свідомістю шляхом поширення недостовірної, неповної або упередженої інформації. Ці загрози можуть реалізовуватись у відкритому (зовнішня інформаційна агресія) або прихованому (спеціальна інформаційна операція) вигляді через засоби телебачення і радіомовлення. Отже, запобігання їм потребує негласного контролю за роботою РЕЗ телебачення та радіомовлення, як вітчизняних, так і тих, що здійснюють цілеспрямовані теле- і радіотрансляції на населення України з позицій закордону. В цьому контексті статті 6 Закону України „Про телебачення та радіомовлення", ст. 7 Закону України „Про основи національної безпеки України" слід розглядати як такі, що містять критерії віднесення роботи РЕЗ телебачення та радіомовлення до загрозливої для державної безпеки. Відтак,

контррозвідувальний режим у сфері використання РЕЗ – сукупність обов'язкових вимог, принципів та правил, що визначені діючим законодавством у сфері використання РЕЗ та сприяють захисту національних інтересів України від зовнішніх та внутрішніх загроз.

Отже, робимо такі висновки: виконання підрозділами СБ України завдань радіоконтррозвідувальної діяльності потребує формування дієвого контррозвідувального режиму у сфері використання РЕЗ. Контррозвідувальний режим у сфері використання РЕЗ охоплює адміністративно-правові режими здійснення телекомунікацій, телебачення і радіомовлення, користування радіочастотним ресурсом, протидії технічним розвідкам. Перелічені елементи контррозвідувального режиму створюються обов'язковими вимогами, принципами, нормами та правилами, що сприяють забезпеченню державної безпеки та визначені: 1) нормативно-правовими актами Міжнародного союзу електрозв'язку; 2) законами України „Про телекомунікації", „Про радіочастотний ресурс України", „Про телебачення та радіомовлення", „Про інформацію", „Про державну таємницю", „Про захист інформації в інформаційно-телекомунікаційних системах"; 3) підзаконними нормативно-правовими актами, що регламентують використання РЕЗ та його контроль. Дотримання деяких норм, встановлених чинним національним законодавством за переліченими напрямами правового регулювання, сприяє здійсненню контррозвідувальної діяльності з виявлення, попередження та припинення використання РЕЗ на шкоду безпеці держави.

Література

1. Закон України «Про основи національної безпеки України» // Відомості Верховної Ради України (ВВР). – 2003. – № 48.

2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» // Відомості Верховної Ради (ВВР), 1994, № 31.

3. Закон України «Про державну таємницю» // Відомості Верховної Ради (ВВР), 1994, № 16/

4. Закон України «Про інформацію» // Відомості Верховної Ради України. – 1992. – № 48.

УДК 005.3

Савінова Н. А.
доктор юридичних наук, старший науковий співробітник
Науково-дослідний інститут інформатики і права
Національної академії правових наук України

СТРАТЕГІЇ СОЦІАЛЬНИХ КОМУНІКАЦІЙ ЯК СПОСІБ ЗНИЖЕННЯ СОЦІАЛЬНОЇ НАПРУГИ НА МАКРО-, МЕЗО- ТА МІКРОРІВНЯХ

Протягом останніх вже більш як двох років перед практиками у сфері забезпечення національно безпеки постає питання формування у свідомості населення розуміння феномену інформаційного суверенітету та автономії національної свідомості. Утім, незважаючи на неодноразові акценти вчених на необхідності побудови належної системи комунікацій у контексті забезпечення безпеки спілкування, автономії волі людини (2014, 2015), необхідності криміналізації умисного поширення хибних новин та умисних деструктивних медіавпливів на свідомість населення (2007, 2009, 2010, 2011, 2014, 2015), до цього часу на рівні законодавства та дій Міністерства інформаційної політики України не зроблено жодних вагомих кроків у цих напрямках.

Усвідомюючи необхідність негайного втручання РНБО та органів національної безпеки захисту державності, інформаційного суверенітету (як єдності і неподільності влади народу України в межах її території) та свідомості людини в умовах гібридної агресії, вважаємо за необхідне запропонувати систему рівневих комунікативних заходів убезпечення свідомості населення від залякування, спотворення офіційної інформації, яка б забезпечувала прямий і зворотній зв’язок населення з владою на всі рівнях.

Якщо умовно поділити систему комунікацій від влади до населення на макро-, мезо- та мікро- рівні, то кожний з них має забезпечувати певне коло інформаційних потреб решти, надаючи виключно корисну та легітимну інформацію, утворюючи, таким чином систему спілкування «центральна влада» - «регіональна влада» - «населення» у послідовності та компетенції, чітко визначених на законодавчому рівні.

Якщо макрорівень – це рівень вихідних та вхідних комунікацій вищого порядку в державі, то мезорівень – рівень держав-

них адміністрацій (у перспективі – префектур), а мікрорівень – рівень певних груп населення, окремих громадян та юридичних осіб.

Оскільки формування первинної легітимної комунікації відбувається на вищому рівні, така інформація первинно витікає від центральних органів влади і, з використанням, насамперед, офіційних джерел, а у другу чергу – ЗМІ, потрапляє на мезо- та мікрорфівень. У той же час, якщо на мезорівні отримання інформації, незалежно від режимів доступу, така комунікація забезпечується документообігом, на рівні населення (мікрорівні), вона потрапляє, нерідко неповна, перекручена, забарвлена ставленням преси, неналежно прокоментована. Внаслідок такого подавання інформації у суспільстві утворюються відчуття нерозуміння, непочутості, обманутості, покинутості, незадоволення.

Задля подолання подібного ефекту, який, на жаль, утворюється внаслідок непрофесійності, або політичної заангажованості ЗМІ, основний тягар тлумачення для населення інформації від центрально влади має покладатися на органи державної влади мезорівня. Отже, на регіональному рівні основним доповідачем, поширювачем і тлумачником рішень та ді органів влади має ставати обласна влада (префектура), яка і в межах своєї компетенції і за рівнем можливостей, делегованих законом має забезпечувати належне пояснення населенню відповідного регіону що саме, чому і заради чого прийняте те чи інше рішення вищими органами влади держави.

Мікрорівень – рівень населення та інститутів громадянського суспільства, може, у такому випадку, споживати не повідомлення преси з приводу дій влади, а отримувати офіційне тлумачення, розуміти реальну реакцію регіональної влади та відчувати ефективну взаємодію регіонального керівництва з центром. Відповідно, в регіонах не відчуватиметься покинутість, непомітність населення центральною владою, бачення єдності регіону з державою, і, головне, у населення виникатиме ефективний комунікатор, який готовий до діалогу, розпочавши його первинно.

Діалог має бути зворотним. Інакше він так і не вийде за формат монологу влади, що ми спостерігаємо вже понад 20 років…

Мезорівень накопичуватиме і відфільтровуватиме величезну низку проблем, але такі проблеми через їх чисельність, і, здавалось би, неоднаковість, є фактично неможливим для переробки

апаратом влади через обсяг і неоднаковість. У той же час, система типових, системних скарг, телекомунікаційних повідомлень та опитування завжди має значно кращий результат усвідомлення проблем, ніж очікування скарг, обсяг яких нереально переробити на регіональному, а тим більше – на центральному (мега-) рівні.

Утім, проблеми можуть бути сформовані у певні блоки, які легше вирішувати. Одна і та сама проблема, яка, наприклад, на рівні всієї України звучить як «пагані дороги», може значно швидше бути вирішення, якщо постановлена як «Необхідно частково відремонтувати 20 км дороги Р06 від 112 до 132 км. Вартість ремонту становить …. грн. Обрахунок додається».

І подібна процедура може утворитися на стадії створення ефективної комунікації мезо- - мікрорівень: між обласними адміністраціями та населенням регіонів.

Комунікація між кожним окремим громадянином, або групою людей, юридичною особою процес, який за часів спроби розбудувати громадянське суспільство в державі до очікуваних результатів так і не призвів: громадянське суспільство утворилося «всупереч» діям держави, і далеко не під її патронатом. Утім воно є, яскраві і розумні люди себе проявляють, і лідери виробництва також повною мірою відомі.

Але ж до цього часу такі люди і групи не поєднані заради вирішення власних потреб, і лишаються в «радянському» очікуванні, що хто вартий за них дізнатися, за них довести, і за них зробити. За таких очікувань суспільство можна ототожнити з жебраком, який стоїть і просить подаяння, а не очікуючи його бере зброю і йде щось «міняти», знову ж таки не розуміючи чого він хоче.

У той же час, забезпечення вертикальної комунікації населення, насамперед з обласною адміністрацією (префектурою) давало б змогу акумулювати скарги, побажання, очікування населення, сортувати їх, вкладати в системні блоки і… обговорювати можливість власного, регіонального вирішення таких проблем. І, насамперед, з населенням, яке сьогодні необхідно якактивніше залучати до реформування системи комунікацій з владою, впроваджувати громадянські інститути та неформальних лідерів громад до державницьких справ, важливих для міста, району, села.

Діалог між мезо- і мікрорівнями, у разі продуктивної комунікації має призводити до інтеракції – взаємодії, спочатку інтелектуальної на рівні стратегій дії, розподілу ролей і, фактично, до-

лей у вирішенні певних регіональних проблем, залучення інвесторів, правоохоронців, ЗМІ, тощо. Так, ремонт дороги або побудова дитячого садка може здійснюватися у дольовому фінансуванні громади, мерій і обласної адміністрації, у межах наявного бюджету.

Така комунікація має бути також відкритою, легітимною, не допускати маніпулювань, адже останні, у разі виявлення, призводитимуть до соціальних вибухів, спалахів гніву людей.

Цікавим вдається за таких умов рівень комунікації між мезо- та мегарівнями. Така комунікація повною мірою має супроводжуватиме первинну вертикальну комунікацію з населенням. Повноваженням обласних адміністрацій є інформування центру про стан справ на рівні комунікацій мікро- - мезорівнів, сутність скарг та проблем, порядок їх вирішення, зміст домовленостей і т. д. Так само, вертикальна комунікація від обладміністрацій до центру повною мірою охоплюється запитами на необхідні та додаткові витрати на область, додаткові потреби нефінансового характеру, включаючи внесення певних змін до законодавства та підзаконних актів, якщо це вмотивовано необхідно.

Зворотна вертикальна комунікація іде має йти по тому ж циклу, який описувався вище.

Такий зв'язок забезпечуватиме офіційне відкрите і систематизоване спілкування всіх рівнів комунікаторів в державі, створюватиме в суспільстві і у окремої людини важливості її потреб і ініціатив, нівелюватиме сепаратистські настрої на регіональному рівні, а також надавати державі на всіх рівнях адміністрування реальну картину взаємодії населенням та швидко демонструватиме реальну картину реакції населення на ті, чи інші політичні та інші перетворення в державі.

Соціальна напруга у разі побудови такої системи комунікацій знижуватиметься за рахунок активного залучення населення до вирішення регіональних проблем та можливості впливу на рішення на макрорівні. Люди значно активніші, ніж вважає влада, і, у разі надання їм реальної можливості впливати на власний добробут та долю своїх населених пунктів, ставатимуть, фактично, волонтерами держави і славне себе. Звичайно, що під спрямуванням дій префектур, які, фактично, одночасно являться представниками влади на місцях і представниками населення в центрі.

Вважаю, що сьогодні, це єдиний виправданий, ефективний шлях побудови комунікацій між населенням і владою, який, дійс-

но, може привести до мінімізації соціально напруги, утвореної маніпуляціями окремих зацікавлених осіб через ЗМІ, розпалювання хибних міжрегіональних непорозумінь та зневірливого ставлення до рішень центрально влади.

Запропонована система фактично не вимагає будь-яких законодавчих модернізацій: вона повною мірою описана на рівні повноважень органів влади стосовно прозорості влади та розподілу повноважень між центральним та регіональними органами.

Проект побудови системних комунікацій макро-, мезо- та мікрорівнях може бути впроваджений на рівні пілотного проекту на рівні однієї з областей країни, і, в подальшому, бути поширений на територію всієї країни.

УДК 005.3

Стецишин Р. В.
кандидат юридичних наук
Національна академія СБ України

ПРОВЕДЕННЯ ЛЕКЦІЙ-БЕСІД З МОЛОДДЮ, ГРОМАДСЬКІСТЮ ТА ОРГАНАМИ ДЕРЖАВНОЇ ВЛАДИ ЯК ЕФЕКТИВНИЙ ЗАСІБ ПІДВИЩЕННЯ РІВНЯ ПРАВОСВІДОМОСТІ ТА СОЦІАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ НАСЕЛЕННЯ

Відповідно до ч. 2 ст. 2 Закону України “Про Службу безпеки України” до завдань Служби безпеки України, з-поміж виявлення, припинення та розкриття злочинів, віднесених до підслідності СБ України, також входить попередження злочинної діяльності.

Служба безпеки України, активізувавши програму лояльності “На тебе чекають вдома”, фактично демонструє щире бажання керівництва держави у межах чинного законодавства зробити все можливе для відмови від заходів державного примусу на користь возз’єднання спантеличених та цинічно ошуканих кремлівською пропагандою сімей Донбасу.

У продовження толерантного ставлення української держави та її спецслужби до формування здорового морально-психологічного клімату серед громадян, що проживають у районі

проведення АТО, вважаємо вкрай важливим напрямком роботи заходи не лише спеціальної, але й загальної превенції.

Службі безпеки України, іншим правоохоронним органам України слід спільно з військово-цивільними адміністраціями й органами місцевого самоврядування Донецької і Луганської областей спланувати та вжити додаткових заходів інформаційно-роз'яснювального характеру, спрямованих на підвищення патріотичного виховання та самосвідомості населення східних і південних регіонів України, демонстрацію загроз, які несе російська агресія тощо.

Зважаючи на напруженість ситуації в регіоні та довгоплинність протікання соціальних процесів, проведення роз'яснювальної роботи із тутешніми представниками органів місцевої влади, громадських організацій, учнями старших класів та студентами має закласти підвалини ефективної протидії російсько-терористичним окупаційним ініціативам та формування толерантного світогляду представників місцевого населення до державної влади України.

На сьогодні вкрай важливо не лише усувати існуючу загрозу незрілості певних груп населення східних регіонів, проте чи не ретельніше зосередити зусилля на недопущенні подібних злочинних проявів у майбутньому. Іншими словами, після двох років бойових дій на території окремих районів вказаних областей, занепаду тамтешньої економіки та поглиблення зневіри місцевого населення щодо швидкого відновлення мирного укладу життя неодмінно потрібно думати про ментальність та правосвідомість населення краю через декілька років (програма з умовною назвою "Донбас-2020").

Звичайно, до розробки повноцінної структури роз'яснювальних зустрічей необхідно підійти виважено та відповідально. Основою для такої дискусії має стати неупереджена, місцями самокритична дискусія щодо сучасної України, в якій широко вживаються не одна, а дві мови, існують метальні відмінності між вихідцями різних регіонів, панує, на жаль, шалена корупція. Поряд з тим, важливо відзначити, що ми завжди були єдині і поважали ідентичність один одного, а от іноземна держава, якими би зовні благими не були її наміри, завжди мислитиме своїми інтересами, інколи відверто загарбницькими, що є дикістю для європейського цивілізаційного простору у XXI столітті.

Окремі зусилля при цьому слід докласти до поступового вплетення у свідомість невластивих на тамтешніх територіях понять прав людини, гідності особи та поваги до них. У цьому напрямку уже є певні, хоча й несистемні, поступи вперед. Прикладом є облаштування восени 2015 року в окремих населених пунктах Донецької області (м. Артеміськ, Краматорськ) низки білбордів з текстом про необхідність шанувати історію, право і закон - "Поважай себе! Донбас – це Україна!".

Переходячи ближче до конкретики, однією із запропонованих тем зутрічей може бути така: "Корупція та сепаратизм як способи знищення держави".

У ході зустрічі тривалістю 60-80 хв. пропонується розглядати такі змістові блоки:

1. Корупція в Україні – найзручніший інструмент розгойдування настроїв населення та ідеальне підґрунтя сепаратизму.

2. Народ як об'єкт тотальної маніпуляції: причини та наслідки сепаратизму в Україні.

3. Програма Служби безпеки України з повернення колишніх учасників незаконних збройних формувань до мирного життя.

Додатковий превентивний ефект вказаного проекту буде досягнуто завдяки висвітленню цих бесід через місцеві та загальнонаціональні засоби масової інформації, а також через мережу Інтернет.

Очікувані результати програми:

1. Розрив шаблону у сепаратистських колах в плані інформаційної війни. Поки Російська Федерація намагається повністю дискредитувати українську владу через заангажовані засоби масової інформації, з нашого боку буде впроваджено діалог не "через ящик", а очі в очі.

2. Формування принаймні у "думаючої" частини представників органів державної влади та молоді більш цілісного уявлення про неприпустимість допущення у регіоні порушень територіальної цілісності.

3. Поетапне об'єднання населення довкола ідеї утвердження в Україні єдиного народу на всій її території не за принципом "роби, як я", а за принципом "єдині в різноманітті". Останнє формується у тому числі через донесення правди про кремлівську агресію як прояв цинічного плюндрування сусіднього народу заради досягнення своїх меркантильних імперських цілей.

4. Встановлення у ході таких бесід особистого контакту з представниками органів місцевої влади сприятиме налаштуванню більш ефективної роботи в інтересах національної безпеки.

5. Створення іміджу державної влади України та правоохоронних органів як структур, що безпосередньо дбають про виховання правової культури населення, зокрема молоді.

6. Вдосконалення вкрай важливого для побудови в Україні інститутів громадянського суспільства соціального діалогу між державою та суспільством; створення атмосфери довіри між владними інституціями та громадянами, формування ідеї соціальної відповідальності всіх без винятку органів державної влади, органів місцевого самоврядування та громадськості.

УДК 355.404.5(1-87):(477)

Титаренко Я. А.
Національна академія СБ України

ОСОБЛИВОСТІ ВИКОРИСТАННЯ СПЕЦІАЛЬНИМИ СЛУЖБАМИ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ СИЛ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ ДЛЯ ПРОВЕДЕННЯ РОЗВІДУВАЛЬНОЇ ДІЯЛЬНОСТІ НА ТЕРИТОРІЇ УКРАЇНИ

Інформаційний простір України постійно перебуває під зовнішнім та внутрішнім впливом, що проявляється у спробах встановити контроль над засобами масової комунікації з метою маніпулювання громадською думкою в інтересах, які нерідко суперечать національним. Досвід сучасних воєнних конфліктів переконує, що на сьогодні жодна держава не в змозі захистити себе, використовуючи лише військово-технічні засоби. Забезпечення безпеки стає комплексним завданням, до якого входять політичні, економічні, військові, науково-технічні, інформаційні та інші заходи.

Сучасна боротьба держави за власну незалежність – це свого роду й інформаційна боротьба, яка здійснюється в таких формах:

1) інформаційної розвідки - пошук, збирання, обробка та аналіз інформації про інформаційні ризики і загрози;

2) планування інформаційних заходів тактичного (внутрішньодержавного), оперативного (поширюються на суміжні держа-

ви) і стратегічного (спільно з державами, які впливають на розвиток геополітики) рівнів;

3) проведення заходів інформаційного характеру (інформаційних операцій, дій, акцій) в цілях реалізації завдань внутрішньої і зовнішньої політики держави;

4) оцінки ефективності інформаційних заходів – визначення рівня досягнення успіху.

Інформаційні заходи стали невід'ємною частиною політики держави. У цьому сенсі РФ не тільки випередила розвинені європейські країни, а й стала конкурувати в питаннях інформаційного впливу з США і Китаєм. Про те, що російська пропаганда глибоко проникла в західне середовище і створила у себе контрпропагандистський щит фахівці зазначали вже в кінці 2013 року. Інформаційна експансія російського іномовлення («RT», «Голос Росії», ВГТРК) і система внутрішньої пропаганди («Газпром Медіа Холдинг», «Національна Медіа Група») створили потужну інформаційну платформу російської системи інформаційної безпеки, що дозволяє проводити інформаційні атаки на інші держави.

Об'єктами інформаційного впливу були визначені:

1) аудиторія конфліктуючої сторони – в даному випадку України (для формування точки зору про справедливість рішень РФ і планів російського керівництва);

2) внутрішня аудиторія РФ та аудиторії підтримуючих її держав (для демонстрації впевненості дій російського керівництва і формування у населення думки щодо підтримки рішень Кремля);

3) зовнішня аудиторія (для створення інформаційних умов позитивного сприйняття політики РФ).

Сьогоднішні реалії в Україні – бойові дії на Донбасі, їх колосальна інформаційна та військова підтримка з боку Кремля наочно демонструють зацікавленість Москви в розпалюванні конфлікту. На передній план у цій війні вийшли російські спеціальні інформаційні операції для завоювання інформаційної переваги в Україні, які ведуться одночасно з воєнними діями, терористичними актами, захопленням полонених тощо.

Для проведення спеціальних інформаційних операцій на полі бою залучені спеціальні підрозділи ЗС РФ. До складу російських підрозділів інформаційно-психологічного впливу на сході України увійшли:

1) групи спеціальних журналістів (8-10 окремих груп), які працюють безпосередньо на російські інформаційні канали. До їх

складу входять 3-4 осіб (журналіст, оператор, водій, може бути охоронець). Групи готувалися до умов війни напередодні і мають чіткі інструкції про те, як висвітлювати події. Вони добре оснащені, мають перепустки по всій території Донбасу, які контролюються бойовиками;

2) оперативні групи психологічних операцій (4 групи ПСО) – являють собою мобільні підрозділи від загону ПСО, який дислокується неподалік Ростова-на-Дону. Їх склад 2-4 осіб. На території окупованого Донбасу вони виконують завдання по:

- усній пропаганді, в тому числі і роботі з місцевим населенням;
- поширенню пропагандистської літератури та іншої необхідної інформації;
- створенню пропагандистських груп в населених пунктах, що складаються з місцевих активістів, їх організації та координації дій;
- надання сприяння роботі російських журналістів;
- збір інформації і визначення найбільш гострих проблем у населення для використання цього надалі, як інформаційного приводу;
- моніторинг поточного морально-психологічного стану місцевого населення;

3) загін психологічних операцій дислокується на території Російської Федерації, недалеко від Ростова-на-Дону, спільно з пунктом управління розвідцентру ГРУ ГШ ЗС РФ. Загін ПСО здійснює основну керівну роль в інформаційно-психологічних заходах на території України. Його завдання:

- збір, обробка і аналіз інформації про поточний морально-психологічний стан населення України та підрозділів російських терористів (зона інтересів загону ПСО поширюється на всю територію України);
- керівництво підрозділами ПСО, які виконують спеціальні завдання по інформаційному впливу;
- розробка і здійснення інформаційно-психологічних операцій на території України;

4) агенти диверсійної психологічної роботи в інших областях України – фахівці від ГРУ ГШ або ФСБ, які виконують завдання з:

- створення диверсійно-пропагандистських груп в інших областях України серед місцевого авторитетного населення;

- навчання місцевих груп проведенню підривних пропагандистських акцій;

- забезпечення груп необхідним матеріально-технічним майном;

- безпосереднього проведення мітингів, акцій протесту і поширення пропагандистських матеріалів.

На загін психологічних операцій, який підпорядкований начальнику розвідки, покладена роль командного центру інформаційно-психологічних операцій, основне завдання цього центру є підтримка незаконних збройних формувань т.з. «ДНР» та «ЛНР». Сам же загін психологічних операцій постійної структури не має. В загоні ПСО, як правило, працюють такі штатні елементи:

1) штаб – організація виконання завдань з ефективного застосування підрозділів загону;

2) редакція і друкарня – складання макетів (ескізів) друкованих продуктів пропаганди і їх виробництво;

3) відділ розповсюдження друкованої та іншої пропагандистської продукції – поширення пропагандистських матеріалів серед призначеної аудиторії;

4) відділ усної пропаганди – використання звукопідсилювальної апаратури, проведення індивідуальних бесід з місцевим населенням, робота з полоненими і т.д.;

5) відділ пропаганди по радіо і телевізійним каналам – забезпечення радіо і телевізійного мовлення з використанням апаратних ресурсів на захопленій території або пересувних станцій;

6) відділ по роботі в інтернет-просторі – підрозділ, який виконує завдання з розвідки, блокування або зміни інформації в мережах, несанкціонованому входженню в пристрої, пов’язані з інтернетом і т.д.

Слід зазначити, що на початку 2014 року в російській армії були створені так звані кібер-війська, завданням яких є захист національних комп’ютерних мереж, обслуговуючих оборонні потреби, а також проведення атак на мережі потенційного противника. Ця нова категорія оборонного відомства стосується сфери інформаційної війни в інтернет-просторі в оперативних і стратегічних масштабах. За наявною інформацією військові кібер-фахівці РФ залучаються до виконання завдань інформаційно-психологічних операцій не тільки по окупованому Донбасу, але і по всій Україні.

Крім цього, фахівці інших загонів ПСО РФ, що дислокуються за тисячі кілометрів від Донбасу, віддалено працюють в мережі інтернет по контентному наповненню сайтів терористів («Новоросія», «Сварог», «Штаб російської армії» і ін.), а також по троллінгу в соціальних мережах і блогах. До такої роботи стали залучатися курсанти російських військових ВНЗ.

Отже, ефективність та результативність вирішення контррозвідувальними підрозділами СБ України покладених на них завдань, залежить від наявності своєчасної інформації про форми та методи діяльності спеціальних служб РФ, які використовують агентурну розвідку для проведення на території України (зокрема в зоні проведення антитерористичної операції) інформаційно-психологічних операцій, які здійснюються за допомогою сил інформаційних операцій, тим самим збільшуючи ефективність розвідувально-підривної діяльності проти Україні.

УДК 355 / 359-5 / -9, 355 / 359.7

Тімков В. Ф.
кандидат технічних наук, доцент
Рада національної безпеки і оборони України

МЕТОДОЛОГІЧНІ АСПЕКТИ ПОНЯТТЯ ГІБРИДНОЇ ВІЙНИ

До кінця 20-го століття склалася така система міжнародних відносин, що для зміни статус -кво в світі, наприклад, перерозподілу сфер впливу лише окремих військових, політичних, ідеологічних, економічних ... силових методів стало не достатньо. Для досягнення необхідного результату потрібно їх спільне використання, причому замасковане під внутрішні процеси держави (або групи держав), на яке направлені такі силові дії. Організаційно - технічною платформою нового виду війни стало поняття гібридна війна (далі - ГВ).

ГВ - це системні, комплексні, узгоджені в часі і просторі, як правило потайливі і закамуфльовані, силові дії однієї держави або групи держав на всі сфери життєдіяльності суспільства і структуру іншої держави або групи держав із стратегічною метою їх повної або часткової десуверенізації.

Структурна схема гібридної війни

1. Розробка концепції ведення ГВ. Вона, як правило, ґрунтується на понятті «failed state» - держава яка не відбулась, або не спроможна повноцінно функціонувати. Можливо також використання ідеї захисту співвітчизників.

2. Розробка, оперативне впровадження і підтримка інформаційних, ідеологічних та пропагандистських операцій супроводу ГВ.

3. Створення і задіяння інфраструктури 5-ї колони у противника. Дестабілізація його державної влади, політичного та соціально-економічного життя громадянського суспільства.

4. Історико-філософське, ідеологічне, політичне, світоглядне, економічне обґрунтування ГВ як всередині держав, що беруть участь у війні, так і в середовищі світової спільноти.

5. Оцінка ресурсу і можливої реакції супротивника.

6. Поетапний план - задум ГВ. Визначення і дедлайн проміжних завдань і цілей ГВ. Розробка комплексу відволікаючих і маскуючих заходів ГВ.

7. Синхронізовані в часі і взаємопов'язані між собою гібридні (асиметричні) поетапні силові операції, суміщені з відволікаючими і маскуючими діями в політиці, економіці, пропаганді, ідеології, релігії, екології, спрямовані на досягнення проміжних цілей і, як підсумок, - стратегічної мети.

8. Комплекс політичних, ідеологічних, пропагандистських, економічних, військових, дипломатичних, міжнародно-правових заходів і дій щодо закріплення і легалізації в системі міжнародних відносин досягнутих проміжних цілей і завдань в ГВ (як приклад – Мінські домовленості).

9. Комплекс політичних, ідеологічних, пропагандистських, економічних, військових, дипломатичних заходів і дій щодо маскування, камуфлювання і відволікання від справжніх цілей і завдань ГВ.

10. Створення інфраструктури, призначення відповідальних осіб, визначення ресурсу кожної з силових компонент ГВ: політичної, економічної, військової, дипломатичної, розвідувальної, пропагандистської, ідеологічної, релігійної, підтримка інфраструктури та ресурсу на достатньому рівні для ведення ГВ.

11. Створення єдиного центру координації та управління (далі - ЄЦКУ) - штабу ведення ГВ. Призначення відповідальних в ЄЦКУ за силові компоненти.

12. Створення синхронізованого у часі поетапного мережевого графіка ведення ГВ.

13. Створення осередків нестабільності в світі, а в разі потреби і нестабільного міжнародного середовища для відволікання уваги від регіону ведення ГВ.

14. Створення, обґрунтування і підтримка дружнього середовища щодо ведення ГВ як всередині держави, так і в міжнародному співтоваристві.

Методика ведення ГВ

На початку ГВ проводиться комплекс пропагандистсько-ідеологічних (а іноді і історико-філософських, як у випадку ГВ, що проводиться Росією в Україні) заходів щодо обґрунтування агресії, метою яких є створення іміджу жертви агресії як держави що не відбулася, або не спроможна виконувати свої функції. Одночасно в усі державні та громадські структури впроваджуються агенти впливу - 5-та колона. Далі дестабілізується державна влада і внутрішньополітичне життя суспільства, що обов'язково супроводжується інформаційно-пропагандистської компанією, заходами по перехопленню та перешкоджанню нормальної роботи органів управління на всіх рівнях і інформаційно-комунікаційних мереж. З цією метою розгортаються:

- кібернетичні атаки на органи управління державою і об'єкти критичної інфраструктури; - психологічні операції в засобах масової інформації, які покликані створити в суспільстві атмосферу страху і недовіри;

- деструктивні дії опозиційних і сепаратистських рухів, спрямовані на розчленування держави;

- диверсійні дії і збройні напади сепаратистських сил і озброєних формувань агресора без розпізнавальних знаків їх державної приналежності;

- економічні санкції, обмеження та ембарго, переривання господарських зв'язків і поставок енергоносіїв, блокування товарообігу.

З початком внутрішньої дестабілізації запускаються операції по зовнішньому силовому тиску - агресор перманентно проводить масштабні військові навчання, які в будь-який момент можуть перерости у війну. Проводиться дипломатичне і міжнародно-правове прикриття можливого силового військового втручання в розгортаючийся конфлікт. Перший проміжний етап ГВ за-

кінчується захопленням агресором частини території під виглядом підконтрольних йому сепаратистських сил. Далі проводяться заходи щодо міжнародно-правового закріплення її нового статусу, зміни політичного устрою, розміщення тут на постійній основі частин і підрозділів регулярних збройних сил агресора, як правило, закамуфльованих під місцеве ополчення. Мета другого і наступних проміжних етапів ГВ - агресор, використовуючи захоплену територію як плацдарм і інструмент проводить заходи щодо подальшої десуверенизації ще не захопленої території.

Заходи щодо мінімізації збитку ГВ

Оскільки ГВ ведеться у всіх сферах життєдіяльності держави і суспільства за мережевоцентричним принципом, то захист від агресора повинен бути побудований у вигляді багатошарової мережі, керованої і координованої з ЄЦКУ, вузлами якої є силові структури держави і волонтерські організації суспільства. ГВ - це нова сучасна форма ведення війни. Отже, необхідно адаптувати і оптимізувати під ГВ все законодавство України, а також ставити питання перед міжнародним співтовариством про зміну міжнародного законодавства щодо правового забезпечення ведення ГВ.

ГВ, яка розв'язана агресором, вимагає таких же гібридних методів протиборства з боку жертви агресії. Основою для планування відбиття агресії в ГВ може бути [1] "Керівництво по системі кризового реагування НАТО", яке включає 4 плани: план превентивних дій, план реагування на кризову ситуацію, план попередження загрози і план відбиття агресії. Особливе місце в цьому керівництві займає план превентивних дій. Заходи цього плану задіяні на всіх етапах ГВ і спрямовані як на саму державу-агресор, так і на окремі елементи його інфраструктури. Ці заходи включають весь спектр політико-дипломатичних, фінансово-економічних та інформаційно-пропагандистських ресурсів, необхідних для запобігання ескалації ГВ, мінімізації її збитку.

Література

1. Crisis management NATO
http://www.nato.int/cps/en/natolive/topics_49192.htm

УДК 342/354

Хаба Р. С.
Служба безпеки України

НАЯВНІ ПРОБЛЕМИ ЕКСПЕРТНОГО ОЦІНЮВАННЯ МАТЕРІАЛІВ, ЯКІ ПОШИРЮЮТЬСЯ В ЕЛЕКТРОННИХ, ДРУКОВАНИХ ЗМІ ТА ІНТЕРНЕТІ

В умовах військової агресії Російської Федерації проти України та інформаційного протиборства одну з найбільших загроз національній безпеці нашої держави становить систематичне проведення антиукраїнських інформаційних акцій, які здійснюється за наступними напрямками: розпалювання протестних настроїв у суспільстві з метою дестабілізації суспільно-політичної ситуації в Україні, підрив обороноздатності нашої держави, протидія євроінтеграційному курсу України та мінімізація міжнародної підтримки, легалізація самопроголошених утворень «ДНР/ЛНР» та анексії АР Крим.

У вітчизняному інформаційному просторі продовжується поширення матеріалів антиукраїнського характеру, зумовлене діяльністю ресурсів, які прямо або опосередковано використовуються російською пропагандою. Інформаційно-психологічний вплив на населення України здійснюється не лише через агресивну інформаційну політику російських ЗМІ, але й через пов’язані з російськими медіа-структурами вітчизняні суб’єкти інформаційного простору.

Аналіз стану інформаційної безпеки свідчить про недосконалість системи формування та реалізації державної інформаційної політики у частині забезпечення інформаційного суверенітету України та вжиття комплексних заходів щодо захисту національного інформаційного простору.

Зокрема, однією з нагальних проблем, що потребує термінового вирішення, є відсутність механізму експертного оцінювання інформаційних повідомлень та матеріалів, які поширюються в електронних, друкованих ЗМІ та Інтернеті і можуть містити ознаки злочинів проти основ національної безпеки України: заклики до терористичних дій, сепаратизму, повалення конституційного ладу, масових заворушень тощо.

Варто зазначити, що на даний час в Україні відсутні відповідні експертні установи, які б здійснювали належний первинний

аналіз таких матеріалів та надавали експертні висновки, які мали б перспективу розгляду у судових інстанціях.

Окремі функції, що були покладені на Національну експертну комісію з питань захисту суспільної моралі (діяльність НЕК припинена Постановою КМ України №333 від 27.05.2015 р.), потребують додаткового доопрацювання, ретельного розгляду та подальшої реалізації діючими державними органами.

Так, суспільно важливе питання щодо аналізу продукції друкованих засобів масової інформації фактично не проводиться, а державна реєстрація друкованих засобів масової інформації здійснюється Міністерством юстиції України або його регіональними підрозділами. Водночас, подальший нагляд за законністю їх діяльності фактично не проводиться.

Актуальним і таким, що потребує додаткового опрацювання усіма учасниками реалізації державної політики у сфері захисту вітчизняного інформаційного простору, є питання фактично неконтрольованого поширення антиукраїнських матеріалів в українському сегменті Інтернету.

Отже, є доцільним розглянути питання щодо впровадження експертного оцінювання інформації, поширюваної українськими мас-медіа та в Інтернеті, на предмет відповідності чинному законодавству України.

Вказані експертні оцінювання комплексно можуть бути реалізовані через можливості Міністерства інформаційної політики України, для чого необхідно доопрацювати і законодавчо врегулювати зміни до Положення «Про міністерство інформаційної політики України» (затверджено постановою Кабінету Міністрів України № 2 від 14 січня 2015 р.).

Експертні оцінювання можуть здійснюватись як на вимогу зацікавлених державних органів, так і незалежних громадських організацій, фізичних і юридичних осіб тощо.

Література

1. Конституція України // Офіційний вісник України. – 01.10.2010. – № 72/1. – Ст. 2598. – С. 15. – (Спеціальний випуск).

2. Закон України «Про контррозвідувальну діяльність» [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/374-15.

3. Закон України «Про основи національної безпеки України» [Електронний ресурс]. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/964-15.

4. Указ Президента України №555/2015 «Про рішення Ради національної безпеки і оборони України "Про нову редакцію Воєнної доктрини України"». – 02.09.2015 [Електронний ресурс]. – Режим доступу : http://www.president.gov.ua/documents/5552015-19443.

5. Закон України «Про інформацію» // Голос України. – 13.11.1992.

6. Закон України «Про друковані засоби масової інформації (пресу) в Україні» // Голос України. – 08.12.1992.

7. Закон України «Про телебачення і радіомовлення» // Голос України. –22.02.1994.

УДК 65.012.8:355.012 (470+571)

Черненко Т. В.
кандидат філософських наук
Національний інститут стратегічних досліджень

МОЖЛИВОСТІ ПРОТИДІЇ РОСІЙСЬКІЙ АГРЕСІЇ В ІНФОРМАЦІЙНОМУ ПОЛІ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ

Безпрецедентну пропагандистську інформаційну кампанію, що супроводжує військову агресію Росії в Україні, було розгорнуто в інформаційному просторі РФ задовго до початку агресії безпосередньо військовими силами.

Мета пропагандистської кампанії для внутрішнього інформаційного простору РФ полягає у наступному:

Забезпечення високого рівня підтримки влади РФ, зокрема її зовнішньополітичних рішень за рахунок руйнування історично-культурного символічного простору «братських російсько-українських відносин», використовуючи міфологеми радянського минулого (США – головний ворог).

Утримання високого рівня лояльності власних громадян до рішень та дій керівництва Кремля, легітимація економічних втрат через непрофесійні дії у економічній сфері та запровадження санкцій. Економічні труднощі мали б розмивати лояльність громадян до дій діючої влади, натомість соцопитування Левада-центру фіксують постійне зниження протестних настроїв громадян РФ протягом останніх трьох років [1] та постійне зростання схвалення рішень та дій керівництва Кремля. Дослідження свідчать про те, що громадяни уникають знання про об’єктивний стан економіки, освіти, охорони здоров’я у своїй країні, воліючи вірити «телевізійній реальності».

Забезпечення внутрішньополітичної стабільності шляхом спрямування активованого вектору дії найбільш радикально налаштованих представників пасіонарної частини російського суспільства («нацболи», «казаки», особи з кримінальним минулим, тощо) у напрямку «зовнішнього ворога» - «українських фашистів», на допомогу «братському народу Сирії».

Дія російської пропаганди на масову свідомість власного населення відзначається високим рівнем ефективності з наступних причин:

Чітко відібрано та створено систему емоційно насичених символів, що дозволяє охопити якнайбільший відсоток споживачів такого інформаційного продукту (об'єднавчим центром символічної системи стала війна 1941-45 рр. - її сприйняття у масовій свідомості не викликає розбіжностей у відношенні до тих чи інших фактів);

Символьну систему було активовано у масовій свідомості російського населення (а також навіть у значної частини вихідців з країн пострадянського простору по всьому світу) задовго до реальних потреб (з початку приходу Путіна до влади);

Символами насичується увесь спектр повідомлень, які отримує споживач інформаційного продукту (особлива увага приділяється кіно та телепродукції, бо поєднуються вербальний та візуальний ряд). Символьний ряд укріплюється дезінформацією дії [3].

Влада РФ веде із власним суспільством дуже грубий, проте ефективний діалог (чітко враховуються всі соціально-психологічні зміни та результати системних досліджень змін індексів соціального самопочуття, рівнів підтримки рішень влади) [2]. Враховуючи запит, що існує в сучасному російському суспільстві, це діалог з приземленими базовими потребами середньостатистичної людини, яка чутиме лише те, що вона хоче чути.

Свідченням таких вдалих маніпуляцій масовою свідомістю громадян РФ є і 90 % рейтинг Путіна, 70% підтримка діяльності нинішнього керівництва РПЦ, різке підвищення почуття гордості за власну країну (соціологічні дослідження продовжують фіксувати значний ріст патріотичних настроїв, активований завдяки «відновленню історичної справедливості» - повернення Криму).

З моменту першого терміну перебування у владі В.Путіна структура ідентифікації росіян зазнала радикальних змін (вже у 2008 р. проєвропейськи налаштованих було лише 21%).

Слід наголосити, що настрої у російському суспільстві чітко корелюються з кількістю та тоном повідомлень про ті чи інші події у російських ЗМІ [2].

Основним джерелом інформації у переважної більшості населення лишається телебачення (від 71 до 90 % за різними дослідженнями отримують інформацію про події саме шляхом перегляду ТБ. Із величезним відривом лідерами рейтингів незмінно залишаються федеральні телеканали - 1-й (раніше ОРТ), Росія-1 та НТВ).

Наглядним прикладом ефективності залякування населення на території РФ, активної антиукраїнської пропаганди та насильницької асиміляції є те, що за період від перепису 2002 р. до 2010 р. кількість громадян РФ, що ідентифікували себе як українці, зменшилась на третину (з 3 млн.чол. у 2002 р. до 2 млн. чол. У 2010 р.) [2].

Нова парадигма відносин між Україною та Росією, яка вибудовується сьогодні в умовах «гібридної війни», існуватиме довгий проміжок часу, полягатиме у відмові від симетричних відносин та визначатиметься взаємною психотравмою масової суспільної свідомості, як українського, так і російського населення. Інформаційно-поведінкова складова російської агресії буде продовжена з метою уможливлення посилення режиму власної безпеки Кремлем, застосовуючи подальше обмеження прав людини шляхом продовження процесу змін законодавства РФ у частині подальшого обмеження прав громадян. Завдяки потужному інформаційному супроводу такі заходи будуть і надалі сприйматися переважною більшістю населення із розумінням.

Детальне системне дослідження російського інформаційного простору дає підстави стверджувати, що запобігання загрозам національній безпеці в інформаційній сфері шляхом прямого реагування на інформаційні «вкиди» та спростуванням дезінформації не досягає мети. Створення можливостей для ослаблення негативного інформаційного впливу на внутрішню російську аудиторію, включно з представниками численної української діаспори, як одного з варіантів асиметричної дії у «гібридній війні», на жаль, залишається вкрай неефективним через велику особисту небезпеку для можливих «агентів» таких впливів.

Враховуючи високу заангажованість російської аудиторії, контрольованість (з тенденцією до посилення) інформаційного простору РФ, застосування відкритих можливостей об’єктивного

інформування російської аудиторії залишається вкрай мало (опозиційні ЗМІ, налагодження журналістської співпраці з діловими виданнями РФ, дипломатичні канали).

Література

1. Левада-центр. Оценка текущего положения дел в стране [Електронний ресурс]. – Режим доступу: http://www.levada.ru/indikatory/polozhenie-del-v-strane

2. Рынок труда: страхи и прогнозы россиян. Пресс-выпуск №2957 ВЦИОМ [Електронний ресурс]. – Режим доступу: http://wciom.ru/index.php?id=236&uid=115437

3. Darczewska J. The information war on Ukraine. New challenges // [Електронний ресурс]. – Режим доступу: www.cicerofoundation.org/lectures/Jolanta_Darczewska_Info_War_Ukraine.pdf

УДК 347.132.15 : 35.078.3

Чеховська М. М.
доктор економічних наук, доцент
Національна академія СБ України
Лісовська О. Л.
кандидат економічних наук, доцент
Національна академія СБ України
Крапівіна Н. В.
Національна академія СБ України

ІНФОРМУВАННЯ ГРОМАДЯН ПРО ВИНИКНЕННЯ НАДЗВИЧАЙНИХ СИТУАЦІЙ ЯК ФАКТОР ПРОТИДІЇ НЕГАТИВНИМ ІНФОРМАЦІЙНИМ ВПЛИВАМ

Однією із складових деструктивного психологічного впливу на суспільну думку та громадян країни у цілому, є створення панічних настроїв. Зважаючи на зазначене, у випадку виникнення надзвичайної ситуації важливе значення для населення має бути своєчасне отримання детальної інформації про наявні загрози від її впливу. Для цього державними органами влади створюється система оповіщення та інформування органів управління, суб'єктів господарювання та населення про загрозу або виникнення надзвичайних ситуацій.

Зазначимо, що інформацію з питань цивільного захисту становлять відомості про надзвичайні ситуації, що прогнозуються або виникли, з визначенням їх класифікації, меж поширення і наслідків, а також про способи та методи захисту від них [1]. Органи управління цивільного захисту зобов'язані надавати населенню через засоби масової інформації оперативну та достовірну інформацію про загрозу або виникнення надзвичайних ситуацій, а також про свою діяльність з питань цивільного захисту, у тому числі в доступній для осіб з вадами зору та слуху формі.

Вказане повідомлення має включати інформацію про надзвичайну ситуацію, місце і час виникнення надзвичайної ситуації, територію (райони, масиви, вулиці, будинки тощо), яка потрапляє в осередки (зони) ураження, порядок дій при надзвичайних ситуаціях, іншу інформацію [2]. Крім того, інформаційні повідомлення мають залежати від екстремальних умов, розмірів, тривалості та масштабів можливих наслідків надзвичайних ситуацій, ступеню небезпеки факторів ураження для населення міста та стану рятувальних і невідкладних аварійних і відновлювальних робіт.

Важливим є факт, що оприлюднення інформації про наслідки надзвичайної ситуації здійснюється відповідно до законодавства про інформацію.

Зазначимо, що оперативна та узагальнююча інформація про надзвичайні ситуації розміщується на сайті Міністерства надзвичайних ситуацій України, де, зокрема, зазначено, що у 2015 році в Україні зареєстровано 148 надзвичайних ситуацій, які розподілилися на: техногенного характеру - 63; природного характеру - 77; соціального характеру - 8, внаслідок чого загинуло 242 особи (з них 40 дітей) та 962 – постраждало (з них 422 дитини) [3].

За масштабами надзвичайні ситуації, що виникли у 2015 році, розподілилися на: державного рівня - 2; регіонального рівня - 9; місцевого рівня - 62; об'єктового рівня - 75. Збільшення на 41,5% кількості постраждалих в надзвичайних ситуацій у 2015 році сталося за рахунок зростання їх частки в НС, пов'язаних із інфекційною захворюваністю та отруєнням людей, а також НС соціального характеру (спричиненої противоправними діями терористичного спрямування, що здійснюються незаконними воєнізованими формуваннями на території Донецької та Луганської областей). Найбільшу кількість загиблих в надзвичайних ситуа-

цій (42 особи) зареєстровано у Донецькій області (переважна більшість з яких загинули унаслідок надзвичайних ситуацій державного рівня у м. Маріуполі, пов'язану із противоправними діями терористичного спрямування).

Широкого розголосу набувають надзвичайні ситуації державного рівня, інформація про які вчасно та оперативно оприлюднюється у засобах масової інформації для унеможливлення поширення неправдивих чуток. Йдеться про ті факти, що на території Донецької та Луганської областей, де внаслідок противоправних дій терористичного спрямування, які здійснюються незаконними воєнізованими формуваннями, зруйновано та пошкоджено житлові будинки, об'єкти інфраструктури, життєзабезпечення та соціальної сфери, що призвело до порушення нормальних умов життєдіяльності населення на тривалий час. Зокрема, зафіксовано випадки загибелі та травмування населення (найбільш критична ситуація виникла у м. Маріуполі Донецької області, де 24 січня 2015 року внаслідок обстрілу незаконними воєнізованими формуваннями житлового масиву «Східний» загинуло 30 осіб та поранено понад 120 осіб, а на території Луганської області внаслідок обстрілів населених пунктів Щастя, Станиця Луганська, Попасна, Кряківка загинуло 11 мешканців) [3].

Стосовно надзвичайних ситуацій регіонального рівня активно висвітлювалася ситуація щодо принаймні двох випадків: у Донецькій області, де внаслідок знеструмлення Донецької фільтрувальної станції та пошкодження хлоропроводу припинено водопостачання споживачів міста Авдіївка (без питного водопостачання залишаються 36,4 тис. мешканців міста, 7 шкіл, 7 дитячих садків, 3 лікарні, 216 багатоповерхових житлових будинків, 5200 приватних будинків, на межі зупинки виробництва знаходився Авдіївський коксохімічний завод. Припинено постачання технічної води до споживачів міста; та у м. Сватове Луганської області, де внаслідок пожежі з подальшою детонацією та розльотом уламків боєприпасів на території польового складу ракетно-артилерійського озброєння Міністерства оборони України (зберігалося близько 3 тис. 132 тонн боєприпасів), загинуло 4 особи та 20 осіб постраждало. За результатами обстеження будинків та інфраструктури міста Сватове, прилеглих населених пунктів, пошкодження різного характеру виявлено у 581 житловому будинку та 59 багатоповерхових, 1 приватний будинок повністю зруйновано, отримали пошкодження 21 об'єкт соціальної сфери, об'єкти

комунального господарства та промисловості. Орієнтовна сума завданих НС збитків становить понад 145 млн. гривень [3].

Таким чином, невідкладне та повне інформування громадськості щодо фактів настання надзвичайної ситуації, заходів, що здійснювалися уповноваженими органами щодо її ліквідації, унеможливить або значною мірою зменшить ефект від надання неправдивої або викривленої інформації, що у кінцевому рахунку вливає на стан забезпечення інформаційної безпеки країни.

Література

1. Шишкін Ю.І. Порядок отримання інформації про загрозу і виникнення надзвичайних ситуацій / Ю.І. Шишкін [Електронний ресурс]. – Режим доступу : https://kremen.gov.ua/.../17059276112935932

2. Про порядок оповіщення у разі виникнення надзвичайних ситуацій техногенного, природного та воєнного характеру, а також порядок укриття в захисних спорудах [Електронний ресурс]. – Режим доступу : http://pivdenka.berdyansk.net/pro-poryadok-opovishhennya-u-razi-viniknennya-nadzvichajnix-situaczij.html

3. Інформаційно-аналітична довідка про надзвичайні ситуації в Україні, що сталися впродовж 2015 року [Електронний ресурс]. – Режим доступу : http://www.mns.gov.ua/opinfo/8638.html

УДК 342.922

Шевченко М. О.
Національна академія СБ України

СПЕЦІАЛЬНИЙ ТЕХНІЧНИЙ ЗАСІБ ЯК ПРЕДМЕТ АДМІНІСТРАТИВНОГО ПРАВОПОРУШЕННЯ, ПЕРЕДБАЧЕНОГО СТ. 195-5 КУПАП

На сьогодні склалася критична ситуація у галузі розроблення, виготовлення спеціальних технічних засобів отримання інформації (далі - СТЗ) та торгівлі ними. Основною проблемою є те, що існуюча правозастосовча практика відносить до категорії СТЗ товари побутового призначення (диктофони, радіоняні, брелоки, ручки, GPS - трекери, тощо). Це пов'язано з відсутністю чіткого законодавчого врегулювання питань щодо сфери обігу СТЗ, зокрема, в частині, що стосується дефініції СТЗ [1].

Власне, зміст поняття «спеціальні технічні засоби» визначається на підзаконному рівні, а саме – Ліцензійними умовами провадження господарської діяльності з розроблення, виготовлення спеціальних технічних засобів для зняття інформації з каналів зв'язку, інших засобів негласного отримання інформації, торгівлі спеціальними технічними засобами для зняття інформації з каналів зв'язку, іншими засобами негласного отримання інформації, затвердженими наказом Центрального управління СБУ від 30.01.2011 р. № 35, зареєстрованими в Мін'юсті 23 лютого 2011 року за № 225/18963, згідно з якими – спеціальними технічними засобами вважаються технічні, програмні засоби, устаткування, апаратура, прилади, пристрої, препарати та інші вироби, призначені (спеціально розроблені, виготовлені, запрограмовані або пристосовані) для негласного отримання інформації" [2].

Аналогічне визначення дається у наказі Служби безпеки України від 12.08.2005 р. за № 440 «Про затвердження Зводу відомостей, що становлять державну таємницю» [3].

Окремі ознаки та технічні критерії належності технічних засобів до СТЗ визначені у розділі 5 частини 3 Списку товарів подвійного використання, що можуть бути використані у створенні звичайних видів озброєнь, військової чи спеціальної техніки, який додається до Порядку здійснення державного контролю за міжнародними передачами товарів подвійного використання, затвердженого постановою Кабінету Міністрів України від 28.01.2004 р. № 86 [4].

Такими ознаками належності виробів до СТЗ, спільними для усіх груп товарів є:

- малогабаритне (мініатюрне) виконання виробу в цілому або відокремленого модулю;
- конструктивне виконання виробів у вигляді безкорпусних мініатюрних модулів;
- використання при проектуванні радіоелектронних виробів схемотехнічних або конструкторських рішень.

Безумовною ознакою належності виробів до СТЗ є їх конструктивне виконання у закамуфльованому вигляді або у вигляді, яке передбачає їх камуфлювання.

Технологічні ознаки СТЗ визначені також у Методиці віднесення об'єктів до спеціальних технічних засобів негласного отримання інформації.

Отже, вищезазначені поняття та ознаки СТЗ, які даються у вказаних нормативно-правових актах, можна охарактеризувати як такі, що:

- по - перше, є надто загальними та некоректними, оскільки не надають однозначної відповіді на запитання, що саме слід розуміти під СТЗ;

- по - друге, відповідно до встановленого Списку товарів подвійного призначення до групи спеціальних технічних засобів може бути віднесено необмежене коло електронних (і не лише електронних) побутових приладів і товарів;

- по - третє, висновок щодо належності (неналежності) предмета до СТЗ надається на основі експертизи, яка проводиться на основі базового нормативно - технічного документа: «Загальна методика віднесення об'єктів до спеціальних технічних засобів негласного отримання інфформації», що зареєстрована в Міністерстві юстиції України 02.03.2011 р. за №17.0.01.

Вказана методика є підзаконним нормативно - правовим актом, який з точки зору теорії права, має базуватися на положеннях закону, зокрема в частині, що стосується понятійно-категоріального апарату. Як зазначалося науковцями, єдиного законодавчого визначення поняття СТЗ не існує. У зв'язку з цим виникають питання однозначності експертних висновків щодо віднесення певного предмету до категорії СТЗ.

В. О. Гацелюк зазначає, що чинне законодавство не дає підстав для однозначних висновків щодо приналежності тих чи інших пристроїв до спеціальних технічних засобів негласного отримання інформації [4].

Відсутність у законодавстві чіткого поняття СТЗ, їх ознак і закритість методики віднесення об’єктів до спеціальних технічних засобів негласного отримання інформації дає підстави констатувати факт, що сьогодні в Україні громадяни не лише не знають, але й не можуть знати, чи нестимуть вони адміністративну або кримінальну відповідальність за свої діяння, а відповідно, і передбачити наслідки своїх діянь, відмежувати правомірну поведінку від протиправної.

Таким чином, стаття 195-5 КУпАП потребує вдосконалення. Сьогодні на розгляді Верховної Ради України знаходиться проект Закону України «Про внесення змін до Кримінального кодексу України та Кодексу України про адміністративні правопорушен-

ня щодо відповідальності за незаконне поводження із спеціальними технічними засобами негласного отримання інформації», реєстр. № 1196, поданий народним депутатом України Швецем В.Д.

Законопроектом пропонується викласти статті 359 КК України та 195-5 КУпАП у новій редакції, у яких, окрім іншого, передбачити конкретне визначення та вказати вичерпний перелік СТЗ. Однак, з огляду на долю попередніх ініціатив, не можна бути впевненим щодо його прийняття. Так, на думку деяких представників правоохоронних органів, однією з підстав, які роблять неможливим формування відкритого для суспільства виключного переліку СТЗ, є те, що технічні засоби, у тому числі СТЗ, завдяки швидким темпам науково - технічного прогресу постійно модернізуються й удосконалюються, тому формування та підтримання їх переліку в актуальному стані буде проблематичним. Іншою підставою є те, що відомості щодо окремих СТЗ містять державну таємницю або службову інформацію та не можуть бути включені до відкритого списку [1].

Підсумовуючи все вищевикладене, з метою приведення положень статті 195-5 КУпАП у відповідність до принципу правової визначеності, а також недопущення обмеження прав і свобод громадян вважається доцільним на законодавчому рівні чітко визначити поняття «спеціальних технічних засобів негласного отримання інформації», а саме:

«Спеціальний технічний засіб» – це технічні, програмні засоби, устаткування, апаратура, прилади, пристрої, препарати та інші вироби, призначені (спеціально розроблені, виготовлені, запрограмовані, пристосовані) для негласного отримання інформації, конструктивна побудова яких забезпечує конспіративність їх використання, зокрема захист від виявлення фактів їх встановлення та застосування.

Література

1. Проект Закону про внесення змін до Кримінального кодексу України та Кодексу України про адміністративні правопорушення щодо відповідальності за незаконне поводження із спеціальними технічними засобами негласного отримання інформації (реєстр. № 1196), народного депутата України / Швеця В.Д. // [Електронний ресурс]. – Режим доступу: http://w1.c1.rada.gov.ua/pls/ zweb2/webproc4_1?pf3511=45300.

2. Наказ ЦУ СБУ "Про затвердження Ліцензійних умов провадження господарської діяльності з розроблення, виготовлення спеціальних техніч-

них засобів для зняття інформації з каналів зв’язку, інших засобів негласного отримання інформації, торгівлі спеціальними технічними засобами для зняття інформації з каналів зв’язку, іншими засобами негласного отримання інформації та Порядку контролю за додержанням Ліцензійних умов" від 30.01.2011 р. № 35, зареєстрований в Міністерстві юстиції України 23.02.2011 р. № 225/18963 [Електронний ресурс]. – Режим доступу: http:// zakon.rada.gov.ua/laws/show/z0225-11.

3. Наказ Служби безпеки України "Про затвердження Зводу відомостей, що становлять державну таємницю" від 12.08.2005 р. № 440, зареєстрований в Міністерстві юстиції України 17.08.2005 року № 902/11182 [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/rada/show/z0902-05.

4. Гацелюк В. О. Криміналізація «на вимогу» та проблеми оціночних ознак складу злочину в контексті відповідальності за незаконні дії із спеціальними технічними засобами негласного отримання інформації/ В. О. Гацелюк // Наше право – 2011 – №1.Ч.2. – С.160-168.

РЕФОРМУВАННЯ СИСТЕМИ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ ТА СЛУЖБОВОЇ ІНФОРМАЦІЇ В КОНТЕКСТІ ЄВРОАТЛАНТИЧНОЇ ІНТЕГРАЦІЇ

УДК 005.52:005.334:004.056

Архипов О. Є.
доктор технічних наук, професор
Науково-технічний університет України
«Київський політехнічний інститут»

ЕКОНОМІКО-ВАРТІСНІ АСПЕКТИ ЗАХИСТУ ІНФОРМАЦІЇ

В низці статей [1-5] наведено матеріали дослідження економічних та вартісно-мотиваційних відносин, характерних для ситуації «атака-захист» в інформаційній сфері, зокрема при реалізації атакуючою стороною А (зловмисник) загрози Т відносно деякого інформаційного ресурсу І, який належить стороні В. Вважатимемо, що D – загальна вартість витрат атакуючої сторони А на реалізацію загрози Т, g – отриманий при цьому «виграш», величина якого обумовлюється цінністю ресурсу І для зловмисника. Збитки, яких зазнає в цій ситуації сторона В (власник ресурсу І), точніше вартість ресурсу з точки зору його власника, оцінюється ним як q (причому вважатимемо, що ця оцінка вище за g: $q > g$), а загальна вартість реалізованої системи захисту інформації (СЗІ), тобто інвестиції в СЗІ, - с. Крім того, За цих умов пропонується оцінювати ризик, що виникає у випадку можливої реалізації загрози Т, співвідношенням [2; 4; 5]:

$$R = P_t P_v q = P_t \frac{q}{q + s\frac{c^2}{D}} q = (1 - \frac{D}{g}) \frac{q^2 D}{qD + sc^2}, \quad (1)$$

де P_t – ймовірність активації (виникнення) загрози, P_v – ймовірність вдалого використання нападом вразливостей СЗІ, s - коефіцієнт, який визначає рівень ефективності інвестувань с в сис-

тему захисту інформації: чим більше значення s, тим нижче, за умови одного і того ж обсягу інвестицій с.

Припустимо [2; 3], що при нульових інвестуваннях у СЗІ ймовірність P_v=1 й вихідний інформаційний ризик становить $R_1 = P_t q$. Інвестування у СЗІ призводить до зменшення ймовірності успішного використання вразливості: P_v<1. Залишковий ризик в цьому випадку дорівнюватиме $R_t = P_t P_v q$, величина втрат, які вдалося попередити – $R_1 - R_t = P_t q - P_t P_v q = (1 - P_v) P_t q$, тобто отримуємо «прибуток» –

$$\Delta_R = R_1 - R_t - c = (1 - P_v) P_t q - c \,. \quad (2)$$

З аналізу виразу (2) випливає, що якщо рівень інвестицій с перевищує деяке граничне значення c_{max} = q(P_t s–1)/s, «прибуток» від введення захисту стає негативним, тобто в загальному випадку діапазон можливих значень с раціонально обмежити так званим діапазоном «розумних» інвестицій [2; 3]:

$$\frac{qP_t}{2}\left(1 - \sqrt{1 - \frac{4D}{sqP_t^2}}\right) \le c \le \frac{qP_t}{2}\left(1 + \sqrt{1 - \frac{4D}{sqP_t^2}}\right). \quad (3)$$

При цьому можна виділити три базових сценарія ризикових ситуацій [4].

Сценарій 1. Фінансово-економічні можливості атакуючої сторони вкрай обмежені, зловмисник не має достатнього досвіду і знань, необхідних для реалізації ефективних атакуючих дій, тому ймовірність вразливості P_v визначається практично тільки рівнем інвестицій с. Вважаючи, що для цього варіанту характерні припущення $D \to 0, P_t \to 1$, можна застосувати спрощену модель ризику [2; 3; 5]:

$$R = P_v q = \frac{q}{q + sc_t} q, \quad (19)$$

за якою оцінимо граничні значення діапазону допустимих інвестицій: $0 \le c \le q - 1/s$, причому найбільш ефективними інвестиції будуть в околі значення $c_{eff\,\max} = 0{,}25q$.

Сценарій 2. Атакуюча сторона - одна особа або група осіб, що володіють достатнім досвідом і необхідними професійними знаннями, але мають обмежені фінансово-економічні можливості й у своїх діях керуються суто комерційними інтересами. Аналізуючи цей сценарій, з (3) отримуємо умову: $D \le 0{,}25sqP_t^2$. З іншого

боку, збільшуючи (починаючи з 0) значення інвестицій атакуючої сторони, визначаємо, що при $D \to 0{,}25sqP_t^2$ права і ліва межі діапазону (3) зближуються, стягуючись в точку $c = \frac{qP_t}{2}$ при $D = 0{,}25sqP_t^2$. У цьому граничному випадку найбільша величина інвестицій в СЗІ складає $c_{eff\max} = 0{,}5qP_t$.

Сценарій 3 - «Зловмисник-виконавець». В ситуації «атака-захист» обидві сторони в своїх діях зазвичай керуються принципом економічної доцільності (розумної достатності). Зокрема, в двох представлених вище варіантах ризикових ситуацій цей принцип враховувався наявністю пари обмежень: $D \le 0{,}25sgP_t^2$ і $g \ge$ D. Однак, як показано в [2; 4; 5], при певних обставинах наведені обмеження можуть виявитися не актуальними. Наприклад, це стосується ситуації, в якій атакуюча сторона для досягнення своїх цілей користується послугами найманого виконавця (звідси назва моделі - «Зловмисник-виконавець»), який за будь-яких обставин зобов'язаний виконувати поставлені перед ним завдання, тобто для нього ймовірність активації погрози $P_t \equiv 1$. Модель ризику для цього варіанта має вигляд:

$$R = \frac{q}{q + s\frac{c^2}{D}}q. \qquad (3)$$

Порівняно з моделлю (1) застосування формули (3) не потребує у описі ситуації «атака-захист» зіставленні чистого прибутку зловмисника D із цінністю g ресурсу I. Якщо ця цінність ресурсу I для атакуючої сторони A значна, зокрема, якщо g >>D, можна припустити, що зловмисник спробує використати будь-які шанси для реалізації своєї загрози T. Очевидно, що в цій ситуації знов приходимо до вже сформульованої вище тотожності $P_t \equiv 1$. Однак найбільш суттєва особливість **Сценарія 3** полягає в тому, що в разі особливої важливості поставленої перед «зловмисником-виконавцем» цілі, він може розраховувати на залучення для підтримки своїх дій певних додаткових ресурсів: фінансових, технічних, інформаційно-аналітичних, оперативних. На практиці це означає можливість реалізації в рамках **Сценарія 3** дуже високозатратних атак. При цьому очевидно, що якщо $D \to \infty$, то $P_v \to 1$, тобто у цій ситуації успішна реалізація загрози атакуючої сторо-

ною А виявляється практично гарантованою. Типовим прикладом подібної ситуації є виконання особливо важливого завдання співробітником спецслужби, який є професіоналом, підготовленим до здійснення атакуючих дій в кіберпросторі.

Крім того, якщо сторона В, створюючи свою СЗІ, виходить із принципу розумної достатності, грунтуючись виключно на власних «внутрішніх» уявленнях про цінність ресурсу I, а атакуюча сторона А оцінює його вище (тобто $q < g$), остання може домогтися успіху і при порівняно низьких (як на свій погляд) витратах. Фактично маємо ситуацію з асиметричними уявленнями сторін А і В про цінність одного й того ж інформаційного ресурсу, через що отримані вище інвестиційні показники будуть занижені і їх слід скорегувати. Зокрема, для **Сценарія 1**: $0 \le c \le q - g/s$, $c_{eff\,\max} = 0{,}25q^2/g$.

Література

1. Архипов А.Е. Применения мотивационно-стоимостных моделей для описания вероятностных соотношений в системе «атака-защита» // А.Е.Архипов, С.А. Архипова Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні – 2008. – вип. 1(16). – С. 57-61.

2. Архипов О.Є. Ризиковий підхід до визначення граничного обсягу інвестицій у захист інформації // О.Є. Архипов, Є.О. Архипова. Інформаційна безпека людини, суспільства, держави, - 2015. - №2 (18) - 60-71.

3. Архипов А.Е. Применение экономико-стоимостных моделей информационных рисков для оценивания предельных объемов инвестиций в безопасность информации // А.Е.Архипов. Захист інформації. – 2015. - Том 17, №3. – С.211-218.

4. Архипов О.Є. Информационные риски: модели рисков, исследование и использование // О.Є.Архипов, А.В.Скиба. Інвестиції: практика та досвід. – 2016. – №1. – С. стор. 51 - 60.

5. Архипов О.Є. Вступ до теорії ризиків: інформаційні ризики: моногр. / О.Є.Архипов. – К.: Нац. Акад. СБУ, - 2015. – 248с.

УДК 35.078:342.738

Ботвінкін О. В.
Національна академія СБ України

ПРАВОВЕ ТА ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНУВАННЯ РЕЖИМУ ВИЇЗДУ ГРОМАДЯН ЗА КОРДОН, ЯК СКЛАДОВОЇ ЗАГАЛЬНОДЕРЖАВНОЇ СИСТЕМИ ЗАХИСТУ ДЕРЖАВНОЇ ТАЄМНИЦІ (ДРУГА ПОЛОВИНА XX СТОЛІТТЯ)

Формування системи охорони державної таємниці передбачає запровадження системи взаємодіючих адміністративно-правових режимів, функції яких, в тій чи іншій мірі, направленні на охорону державної таємниці. В цій системі, зокрема, важливе місце відводиться режиму виїзду громадян за кордон, оскільки використання каналів туризму, науково-технічного, культурного обміну та ін. створює іноземним розвідкам сприятливі умови для здобування необхідної їм інформації, в т.ч. з обмеженим доступом.

В рамках дослідження проблем захисту секретної інформації в Україні цікаво вивчити питання забезпечення функціонування згаданого адміністративно-правового режиму в попередні роки. Оскільки проблема запобігання витоку секретної інформації в результаті порушень, які могли мати місце при відправленні за кордон спеціалістів, особливо обізнаних у інформації, що становила державну таємницю, починає набувати особливої актуальності починаючи з 1950-х рр. (по мірі розвитку міжнародних контактів радянських міністерств і відомств з іноземними партнерами) і в подальшому постійно зростає хронологічні рамки дослідження пропонується обмежити другою половиною XX століття.

Отже, одним з наслідків деякої лібералізації внутрішнього життя в СРСР, що мала місце після смерті Й.Сталіна у 1953 р., стало, зокрема, і збільшення кількості радянських громадян, в першу чергу спеціалістів, що відряджалися за кордон для вивчення технічних досягнень і новітніх зразків зарубіжної техніки. Відповідно до розпорядження РМ СРСР від 25 лютого 1956 р. № 984рс, урядом УРСР було затверджено кількість радянських спеціалістів, яких планувалось відрядити за кордон, та перелік країн, куди направлялися спеціалісти. Відповідні міністерствами й відомствами республіки повинні були подати до РМ УРСР і ЦК КПУ

списки спеціалістів для відрядження їх за кордон. В подальшому подібні постанови щодо відрядження спеціалістів за кордон з'являтимуться щороку.

3 лютого 1958 р. РМ СРСР прийняла постанову № 140-61 "Про впорядкування відрядження радянських спеціалістів у капіталістичні країни для вивчення досягнень зарубіжної науки й техніки та про впровадження матеріалів, одержаних в результаті цих відряджень, в народне господарство" (постанова РМ УРСР від 18 квітня 1958 року № 454-19), яка визначила державні органи, відповідальні за організацію закордонних відряджень радянських спеціалістів (крім делегацій АН СРСР на наукові конгреси й конференції та для спеціалістів оборонних галузей). Такими органами стали Державний науково-технічний комітет РМ СРСР та Держбуд СРСР (в частині будівництва і промисловості будівельних матеріалів). Постановою РМ УРСР від 23 вересня 1958 р. № 1337-55 республіканським відповідникам цих органів доручено визначати порядок відрядження у капіталістичні країни радянських спеціалістів з установ і підприємств УРСР.

Особи, відібрані для закордонного відрядження повинні були пройти спеціальну перевірку органами КДБ. Така перевірка здійснювалась за дорученням комісії з виїздів за кордон при ЦК компартій союзних республік, крайкомах і обкомах партії та являла собою певний комплекс і порядок здійснення перевірочних заходів, в результаті яких передбачалось отримання інформації, достатньої для прийняття рішення щодо відповідності особи вимогам, які висувались діючою на той час інструкцією з режиму секретності. При наявності серйозних компрометуючих матеріалів стосовно відряджених за кордон радянських громадян і туристів, а також у випадках, коли органи КДБ мали дані, які перешкоджали виїзду за кордон особи, обізнаної з державною таємницею, повідомлялось про небажаність їх виїзду з СРСР.

За виїзд за кордон без встановленого паспорта чи дозволу відповідних органів громадянин СРСР підлягав кримінальній відповідальності (стаття 80 КК УРСР 1927 р., пізніше - стаття 75 КК УРСР 1961 р.).

23 серпня 1972 р. РМ СРСР постановою № 637-207 затвердила "Положення про порядок здійснення зв'язків міністерств, відомств, підприємств, установ, організацій СРСР та їх представників з іноземними установами, фірмами та їх представниками в

галузі науково-технічного і економічного співробітництва". Відповідно до цього Положення координація зв'язків у галузі науково-технічного і економічного співробітництва міністерств, відомств, підприємств, установ та організацій та їх представників з іноземними установами і їх представниками а також контроль за вказаними зв'язками була покладена відповідно на Державний комітет РМ СРСР з науки і техніки, Державний комітет СРСР з зовнішньоекономічних зв'язків та Міністерство зовнішньої торгівлі.

Міністерства й відомства повинні були заздалегідь організовувати підготовку осіб, що відряджалися за кордон, обмежуючи при цьому виїзд осіб, широко обізнаних у відомостях, які становили державну таємницю, та які мали безпосереднє відношення до особливо важливих об'єктів МО СРСР та інших міністерств і відомств, і утримуючись від надання цим особам рекомендацій для роботи в міжнародних організаціях.

Загалом же до кінця 1980-х рр. виїзд за кордон у приватних, службових справах, в якості туриста регулювався партійними органами і перебував під їхнім контролем. Відповідно до "Положення про комісію з виїздів за кордон при обкомі, крайкомі партії, ЦК компартій союзних республік", затвердженого Секретаріатом ЦК КПРС у липні 1975 р., до основних обов'язків таких комісій, зокрема, належали розгляд подань міністерств, відомств та організацій стосовно виїзду за кордон радянських громадян; спостереження за роботою місцевих органів внутрішніх справ щодо розгляду заяв та оформлення виїздів за кордон радянських громадян у приватних справах тощо.

11 січня 1983 р. ЦК КПРС затверджено "Положення про порядок виїзду за кордон осіб, обізнаних у державних секретах". З урахуванням вимог цього Положення у прийнятій в 1987 р. "Інструкції з забезпечення режиму секретності в міністерствах, відомствах, на підприємствах, в установах і організаціях СРСР" виділено окремий розділ, присвячений питанням забезпечення режиму секретності при направленні за кордон осіб, обізнаних у державних секретах.

Демократичні зміни в суспільстві у другій половині 1980-х рр. призвели до спрощення виїзду радянських громадян за кордон. У 1989 р. РМ СРСР приймає постанову "Про вдосконалення порядку виїзду за кордон в службових справах", яка спрощувала процедуру направлення за кордон делегацій і спеціалістів, роз-

ширювала права і посилювала відповідальність організацій у міжнародних відносинах. Союзні республіки одержали більше прав у вирішенні питань виїзду за кордон і оформленні для цього документів.

Наступного року постановою РМ СРСР "Про порядок направлення радянських спеціалістів в зарубіжні країни для практичного стажування" підприємства дістали право самостійно укладати контракти з іноземними фірмами про стажування спеціалістів.

Таким чином, в СРСР та Україні як його складовій було створено комплексну систему норм які регулювали питання виїзду за кордон радянських громадян. Державою було встановлено правовий порядок, який регламентував питання виїзду радянських громадян за кордон, визначені відповідні державні органи, уповноважені проводити діяльність, в тій чи іншій мірі направлену на забезпечення функціонування в країні режиму виїзду радянських громадян за кордон.

УДК 004.7(045)

Гордієнко С. Б.
Кандидат технічних наук, доцент
Національна академія СБ України

СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ: ОБҐРУНТУВАННЯ ОСНОВНИХ ФУНКЦІЙ

Національний банк України запровадив два галузеві стандарти управління інформаційною безпекою [1]. Документи [2, 3] визначають вимоги і правила впровадження системи управління інформаційною безпекою та дублюють міжнародні стандарти управління інформаційною безпекою ISO/IEC 27001 та ISO/IEC 27002. На додачу, тенденція приваблення іноземних інвестицій змушує комерційні організації впроваджувати міжнародні стандарти управління, в тому числі і стандарти управління інформаційною безпекою. Ці факти пояснюють підвищення попиту на впровадження систем управління інформаційною безпекою на українських підприємствах.

Система управління інформаційною безпекою (СУІБ) – частина загальної системи управління, яка ґрунтується на підході, що враховує бізнес-ризики, призначена для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення інформаційної безпеки (ІБ) [2].

Галузеві стандарти України “ГСТУ СУІБ 1.0/ISO/IEC 27001:2010” [2] та “ГСТУ СУІБ 2.0/ISO/IEC 27002:2010” [3] містять певні вимоги до СУІБ. Документ [4] підсумовує ці вимоги.

Головним чином, СУІБ має працювати, спираючись на існуючі політики. В іншому випадку, політики можуть бути розроблені в процесі впровадження або функціонування СУІБ. Під політикою інформаційної безпеки слід розуміти набір законів, правил, обмежень, рекомендацій і т. ін., які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз. Термін "політика безпеки" може бути застосовано до підприємства, інформаційної системи, окремого ПК і т. ін.

Документ [5] пропонує наступні обов'язкові документи СУІБ:

1. Записи ключових управлінських рішень стосовно СУІБ;
2. Набір політик інформаційної безпеки, у тому числі політика СУІБ і політика ІБ;
3. Опис сфери впливу СУІБ;
4. Опис заходів ІБ;
5. Документація контролів (засобів захисту, які охоплюють політику, заходи, настанови, втілення або організаційні структури [3]);
6. Методи оцінки ризиків;
7. Звіти оцінки ризиків;
8. Інструкції щодо дій відносно ризиків;
9. Оперативні заходи СУІБ;
10. Оцінки ІБ;
11. Звіт відповідності;
12. Заходи з контролю документів;
13. Заходи з контролю записів;
14. Записи ознайомлення з умовами безпеки, навчальні матеріали, а також матеріали ознайомлення з інформаційною безпекою, звіти з оцінками навчання та відгуками;
15. Плани та заходи внутрішнього аудиту СУІБ, а також звіти з аудиту СУІБ, погоджені плани дій і звіти з планових заходів, перевірок, припинення;

16. Заходи з виправлення невідповідностей;

17. Заходи із запобігання невідповідностям.

СУІБ може використовувати систему управління вмістом для забезпечення обміну інформацією, наприклад, висновками аудиту, політиками і т.п. Система управління вмістом має бути обрана з врахуванням особливостей підприємства. Рекомендовано застосовувати метод структурованої специфікації та оцінки (як для вибору методів управління та аналізу ризиків).

Існують безкоштовні (з відкритим вихідним кодом) і комерційні продукти, розроблені для підтримки СУІБ. Їх можна поділити на наступні типи:

1. Системи управління вмістом (Content Management Systems, CMS);

2. Системи управління документами (Document Management Systems, DMS);

3. Системи управління навчанням (Learning Management Systems, LMS);

4. Системи управління політиками (Policy Management System, PMS).

Система управління вмістом є необов'язковою для СУІБ, і обмін інформацією може підтримуватись безпосередньо СУІБ, або виконуватись вручну для відносно малих підприємств чи на рівні вищого керівництва.

Якість ІБ може бути оцінена по різноманітних параметрах – від кількості заблокованих повідомлень спаму до ступеня досягнення стратегічних цілей. Відносно СУІБ, автор наполягає на вимірі ефективності управлінськими оцінками, такими як кількість завершених завдань нижчого рівня, умовного значення ризику, який відвернутий заходом безпеки і т.п. Така оцінка забезпечує краще розуміння на рівні вищого керівництва.

Друга найважливіша мета впровадження СУІБ окрім забезпечення прозорого управління підприємством – отримання сертифікату відповідності одному або декільком стандартам ІБ (наприклад, сімейства ISO27k, CobiT, PCI DSS).

Процес сертифікації включає зовнішній аудит корпоративної системи інформаційної безпеки для визначення відповідності стандарту(ам). Щоб гарантувати успіх зовнішнього аудиту, підприємство може влаштувати внутрішній аудит безпеки до початку процесу сертифікації.

Оскільки СУІБ зберігає та обробляє найважливіші дані оцінки безпеки, впровадження відповідних функцій може значно полегшити перебіг внутрішнього аудиту.

Враховуючи зазначені вимоги до СУІБ, сформульовані наступні необхідні функції програмного продукту для управління інформаційною безпекою.

1. Представлення для керівників високого рівня завдяки простим інтерфейсам та звітам, орієнтованим на вище керівництво;

2. Відстеження і управління ризиками ІБ на підприємстві з негайною переоцінкою в разі будь-яких змін в наборах активів чи загроз;

3. Планування зовнішнього або внутрішнього аудиту, контроль процесу аудиту за допомогою зведених звітів;

4. Реєстрація порушень, відхилень та зауважень в процесі аудиту шляхом подання потрібної інформації в спеціальному звіті;

5. Використання шаблонів для політик, описів та інших робочих документів. Ці шаблони повинні відповідати державним стандартам України;

6. Створення і зберігання всіх необхідних настановних та регулюючих документів ІБ (функціональні обов'язки, інструкції, політики безпеки і т.п.) шляхом зберігання, оновлення та включення інформації щодо ІБ в установі безпосередньо до документів;

7. Підтримання спільних баз знань та методичних матеріалів, архівація для забезпечення управлінських рішень фактичними даними;

8. Проведення аналізу стану ІБ і створення звітів для правління у вигляді зрозумілих таблиць і діаграм, оскільки представити інформацію щодо ІБ неспеціалістам зазвичай проблематично;

9. Раціональний розподіл ролей, повноважень і ресурсів між співробітниками та завданнями;

10. Інформативно-аналітична підтримка рішень правлінням організації відносно управління ІБ, тому що за наявності зрозумілої та об’єктивної інформації приймати раціональні рішення легше;

11. Забезпечення формування вимог до СУІБ та оцінок її ефективності, що важливо в контролі досягнення встановлених цілей;

12. Оцінка і управління бюджетом створення і експлуатації СУІБ, щоб контролювати витрати на СУІБ, чи на ІБ організації взагалі;

13. Відстеження виконання завдань і надання рекомендацій для підвищення загальної продуктивності проектів.

Література

1. Про набрання чинності стандартами з управління інформаційною безпекою в банківській системі України [Текст]: постанова правління Національного банку України від 28 жовтня 2010 р. № 474. – К.: Національний банк України, 2010.

2. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2005, MOD) [Текст]: ГСТУ СУІБ 1.0/ISO/IEC 27001:2010. – К.: Національний банк України, 2010. – 49 с. – Код УКНД 35.040.

3. Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою (ISO/IEC 27002:2005, MOD) [Текст]: ГСТУ СУІБ 2.0/ISO/IEC 27002:2010. – К.: Національний банк України, 2010. – 163 с. – Код УКНД 35.040.

4. ISO/IEC 27000 series FAQ – ISO27k Forum [Електронний ресурс]. – Режим доступу: http: // www.iso27001security.com/ html/ faq.html.

5. Salah, O. Mandatory Information Security Management System Documents Required for ISO/IEC 27001 Certification [Електронний ресурс] / O. Salah, G. Hinson. – Режим доступу: http: // www.iso27001security.com/ ISO27k_mandatory_ISMS_documents.rtf.

УДК [340.111.5=>347.2/3]:[001.8:[001.891.3:340.113]

Гордієнко С. Г.
доктор юридичних наук, доцент
Національний технічний університет України
«Київський політехнічний інститут»

ФУНДАМЕНТАЛЬНІСТЬ ПІДГОТОВКИ – НЕОБХІДНА УМОВА РОЗУМІННЯ ПРОБЛЕМ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕННЯМИ У ДОСТУПІ ТА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ В УКРАЇНІ

Автор вважає за доцільне ще раз відзначити, що запропонована до розгляду на конференції тематика досить складна і потребує прискіпливої уваги. Лише співвіднесення між собою теоретичних напрацювань та юридичної практики дасть можливість відпрацювати ефективні програми, концепції тощо удосконалення і розроблення нових теоретико-прикладних розробок вітчиз-

няної юридичної науки. Адже останні активно будуть формувати особистість молодих фахівців.

Основною проблемою різноманіття та суперечливості зазначеного питання, на наш погляд, є неадекватність наукових та законодавчого визначень понятійно-категоріального апарату інформаційної сфери (інформація, знання, система, інформаційний простір, безпека, інформаційна безпека, держава, право, власність, інтелект, право власності, право інтелектуальної власності, діяльність, забезпечення, охорона, захист, режим тощо). Необхідним вважається також визначення якісних критеріїв класифікації сфер людської творчості.

Тепер більш детально про основні проблеми та шляхи їх вирішення.

По-перше, понятійно-категоріальний апарат нормативно-правових актів стосовно інформаційного права та права інтелектуальної власності застосовується у нормах неоднаково, а його обґрунтованість викликає сумніви.

За законодавством України майже 20 документів декларують різного роду конфіденційну інформацію та «таємниці» і виділяють майже 40 різновидів інформаційних масивів, які мають різні критерії обмеження у доступі.

Задля визначення істинності наукового та практичного знання про понятійно-категоріальний апарат слід знати і розуміти різницю між існуючими методологічними платформами пізнання соціально-правових явищ, а також підстави їх адекватного застосування.

Найбільш відпрацьованими та ефективними вважаються: діалектика, науковий реалізм, науковий матеріалізм, марксизм, структурно-функціональний аналіз, СМД-методологія, синергетика, конвергенції теорія, що є лише часткою серед відомих автору 72 методологій,

Слід також відзначити, що центральною проблемою будь-якої методології є визначення і застосування понятійно-категоріального апарату.

По-друге, якість та рівень нормативно-правового регулювання діяльності різних органів та організацій залежить від правової кваліфікації їх юристів, які мають схильність роз’яснювати на практиці спосіб застосування норм у бік необхідний керівництву, що протирічить світовій практиці. Закон необхідно виконувати, а не тлумачити.

Третьою проблемою є велика кількість державних органів та недержавних організацій, які беруть участь у забезпеченні безпеки інформаційних масивів, та їх неоднозначна компетенція.

На наш погляд, окрім підкомітетів Верховної Ради України, ще 10 органів виконавчої гілки влади забезпечують діяльність у сфері інформаційного права та охорони інтелектуальної власності.

До структури організацій з регулювання охорони інтелектуальної власності відноситься також мережа недержавних організацій (творчі спілки та інші недержавні інституції).

На думку парламентарів, в сучасних умовах до інституційної бази набуття, здійснення й захисту інтелектуальної власності належать також 10 органів виконавчої гілки влади, 4 державні органи зі спеціальним статусом та органи судової влади.

Четвертою проблемою є явна неузгодженість об'єктів інтелектуальної власності (ОІВ) зазначених у законодавчих актах з переліком об'єктів, зазначених у Цивільному Кодексі України, яка породжує правову казуїстику.

Ця проблема породжена невідповідністю світових традиційних параметрів класифікації та розподілу ОІВ новітнім науковим доробкам.

П'ятою проблемою виступає якість та кількість т.зв. «закритих» норм з урегулювання трансферу таємних технологій та технологій подвійного використання, які є ОІВ, або їх структурними елементами та визначення їх компетенції виходячи з інтересів керівництва окремих гілок державної влади, а не у відповідності до реальних потреб суспільства.

Шостою проблемою являється – проблема власності різноманітних інформаційних ресурсів та відсутність переліку стратегічних інформаційних ресурсів і ОІВ держави, у тому числі таємних.

Сьомою проблемою є практично повна відсутність якісних, науково-обґрунтованих методик оцінки інформаційних масивів та ОІВ.

Останнє також стосується великої кількості документів на рівні ноу-хау, що знаходяться на нині не діючих підприємствах ОПК та народного господарства і які мають грифи таємності, тобто інформаційних масивів придатних до оформлення в ОІВ на перспективу.

Таким чином, визначена для розгляду проблема не являється штучною, а реально існує і потребує НЕГАЙНОГО вирішення на державному рівні.

В ході детального опрацювання зазначених завдань ми зможемо узагальнити емпіричні та теоретичні знання і запровадити ефективну методику їх викладання у ВНЗ.

При цьому, ми маємо завжди пам’ятати про головний принцип науково-педагогічної діяльності – принцип єдності теорії та практики. Наблизитися до нього ми можемо тільки при детальному розумінні загальної методології пізнання та системного методу.

Таким чином, глибоке знання та розуміння загально-наукових засад юридичної науки викладачами та студентами можливе лише за умови їх фундаментальної та практичної підготовки.

УДК 35.746.1

Драчук С. М.
кандидат юридичних наук
Український науково-дослідний інститут спеціальної техніки та судових експертиз СБ України

ОРГАНІЗАЦІЙНО-ПРАВОВА ТА НАУКОВО-ТЕХНІЧНА СКЛАДОВА РЕФОРМУВАННЯ СИСТЕМИ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ ТА СЛУЖБОВОЇ ІНФОРМАЦІЇ В КОНТЕКСТІ ЄВРОАТЛАНТИЧНОЇ ІНТЕГРАЦІЇ

Актуальність запропонованого напряму наукової дискусії чітко корелюється з відповідним рішенням Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України" щодо необхідності реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом, захисту державних інформаційних ресурсів, технічного і криптографічного захисту інформації з урахуванням практики держав - членів НАТО та ЄС.

Питання формування відповідної державної політики України у сфері охорони державної таємниці та службової інформації пов’язана з таким пріоритетним напрямом розвитку науки і техніки на період до 2020 року як інформаційні та комунікаційні технології.

Методи, засоби та заходи організаційно-правового захисту інформації з обмеженим доступом стали постійним напрямом на-

укових досліджень, результати яких періодично публікуються на шпальтах заснованого Національною академією СБУ науково-практичного журналу «Інформаційна безпека людини, суспільства, держави».

Сьогодні основними напрямами державної політики з питань національної безпеки України в інформаційній сфері, серед іншого, є вдосконалення державного регулювання розвитку інформаційної сфери шляхом: створення нормативно-правових передумов для розвитку національної інформаційної інфраструктури та ресурсів; заборони дискримінації в інформаційній сфері; впровадження новітніх технологій в інформаційній сфері.

Пропонуємо розглянути ці три складові в контексті запропонованого напряму наукового пошуку.

По-перше, створення та удосконалення нормативно-правових передумов як основи реформування системи захисту та охорони інформації з обмеженим доступом, що є загальноприйнятною практикою реалізації принципу законності в країнах ЄС.

В цьому контексті слід наголосити на тому, що порядок віднесення інформації до таємної або службової, а також порядок доступу до неї регулюються законами. Будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом. На відміну від Закону України «Про державну таємницю» в Україні до цього часу не прийнято відповідного закону, який би врегульовував питання віднесення інформації до службової, що негативно впливає на розвиток національної інформаційної інфраструктури і потребує свого вирішення. Також, з метою реформування системи охорони інформації з обмеженим доступом в контексті євроатлантичної інтеграції, сприяння міжнародній співпраці в інформаційній сфері та входження України до світового інформаційного простору, вбачається за доцільне доповнити Закон України «Про інформацію» новим розділом «Міжнародне співробітництво у сфері інформаційних відносин». Наочним прикладом необхідності внесення таких змін є наявність в Законі України «Про науково-технічну інформацію» відповідного розділу «Міжнародне співробітництво у сфері науково-технічної інформації», в якому, серед іншого, передбачені вимоги до забезпечення суверенітету України у сфері науково-технічної інформації, що є дотичним до компетенції СБ України.

По друге, європейське законодавство висуває жорсткі вимоги щодо недопущення дискримінації суб'єктів інформаційних відносин, що на нашу думку, обов'язково має враховуватися в ході реформування системи охорони державної таємниці та службової інформації в контексті євроатлантичної інтеграції.

Системний аналіз вітчизняного правового забезпечення інформаційних відносин свідчить про наявність в ньому дискримінаційних положень, зокрема в частині реалізації права на інформацію суб'єктами владних повноважень та державою. З метою усунення наявних дискримінаційних положень реалізації права на інформацію, зокрема суб'єктами владних повноважень а також державою, доцільно внести відповідні зміни до абзацу 2 статті 5 Закону України «Про інформацію» та викласти у наступній редакції: «Реалізація права на інформацію не повинна порушувати громадські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи і законні інтереси інших громадян, права та інтереси юридичних осіб, суб'єктів владних повноважень та держави».

По-третє, впровадження результатів науково-технічної діяльності у вигляді новітніх технологій в сфері охорони державної таємниці та службової інформації, що є розповсюдженою практикою в країнах ЄС.

Охорона державної таємниці передбачає комплекс організаційно-правових, інженерно-технічних та інших заходів, спрямованих на запобігання розголошенню секретної інформації та втратам її матеріальних носіїв. З метою охорони державної таємниці впроваджуються єдині вимоги до виготовлення, обліку, користування, зберігання, схоронності, передачі та транспортування матеріальних носіїв секретної інформації, а також технічний та криптографічний захисти секретної інформації. Забезпечення охорони державної таємниці, у межах визначеної законодавством компетенції, покладається на СБ України, яка, серед іншого, має право контролювати стан охорони державної таємниці в усіх державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях. З метою ефективної реалізації права СБ України контролювати стан охорони державної таємниці пропонується розробити та впровадити в серійне виробництво USB-флеш накопичувачі з апаратним шифруванням для їх

використання під час роботи з секретною інформацією в органах законодавчої, виконавчої та судової влади, органах прокуратури України, інших державних органах, органах місцевого самоврядування, підприємствах, установах та організаціях усіх форм власності, об'єднаннях громадян, що провадять діяльність, пов'язану з державною таємницею, громадян України, іноземців та осіб без громадянства, яким у встановленому порядку наданий доступ до державної таємниці.

На останок нагадаємо, що права і свободи Українського народу - громадян України всіх національностей та їх гарантії визначають зміст і спрямованість діяльності держави Україна. Утвердження і забезпечення прав і свобод громадян України, зокрема в інформаційній сфері, є головним обов'язком держави Україна. Водночас держава Україна має дбати і про свої інтереси як суб’єкта міжнародного інформаційного права, що кореспондується з відповідною державною політикою у сфері забезпечення державної безпеки.

Література

1. Конституція України: Конституція від 28.06.1996 №254к/96-ВР [Електронний ресурс]. - Режим доступу : http//zakon.rada.gov.ua;

2. Про інформацію: Закон України від 02.10.1992 № 2657-XII [Електронний ресурс]. - Режим доступу : http//zakon.rada.gov.ua;

3. Про науково-технічну інформацію: Закон України від 25.06.1993, № 3322-XII [Електронний ресурс]. - Режим доступу : http//zakon.rada.gov.ua;

4. Про державну таємницю: Закон України від 21.01.1994 № 3855-XII [Електронний ресурс]. - Режим доступу : http//zakon.rada.gov.ua;

5. Про основи національної безпеки України: Закон України від19.06.2003 № 964-IV [Електронний ресурс]. - Режим доступу : http//zakon.rada.gov.ua;

6. Про пріоритетні напрями розвитку науки і техніки: Закон України від 11.07.2001 № 2623-III [Електронний ресурс]. - Режим доступу : http//zakon.rada.gov.ua;

7. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України": Указ Президента України від 26.05.2015 № 287/2015 [Електронний ресурс]. - Режим доступу : http//zakon.rada.gov.ua.

УДК 35.746.

Князєв С. О.
кандидат юридичних наук, старший науковий співробітник
Національна академія СБ України
Шлапаченко В. М.
кандидат юридичних наук, старший науковий співробітник
Національна академія СБ України

ШЛЯХИ УДОСКОНАЛЕННЯ НОРМАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ПРОЦЕДУРИ ВІДНЕСЕННЯ ІНФОРМАЦІЇ ДО КАТЕГОРІЇ СЛУЖБОВОЇ

З 2011 року в законодавстві України запроваджено окремий вид інформації з обмеженим доступом – службову інформацію. У зв'язку з цим відповідні зміни було (хоч і не одразу) внесено до закону України «Про інформацію», Кримінального кодексу України, Кодексу України про адміністративні правопорушення тощо.

Таким чином законодавець продемонстрував зацікавленість у збереженні статусу службової інформації, як інформації з обмеженим доступом та необхідність її охорони. Разом з тим, є очевидним, що кваліфікація будь-яких посягань щодо службової інформації передбачає, передусім, чітке встановлення предмету злочину чи правопорушення, а отже безпосередньо пов'язана з питаннями віднесення інформації до зазначеної категорії. Відтак, важливим є визначення та нормативне закріплення процедури такого віднесення.

Пунктом 3 ст.21 Закону «Про інформацію» встановлено, що «порядок віднесення інформації до службової, а також порядок доступу до неї регулюються законом». Проте, дотепер єдиного порядку віднесення інформації до службової жодним законом України не встановлено. Даний факт безперечно ускладнює правові відносини щодо використання службової інформації та її законодавчу охорону.

Низка науковців неврегульованість питань віднесення пов'язують з тим, що законодавець, на відміну від державної таємниці, дотепер не дав чіткого

визначення службової інформації, та не зазначив необхідність її охорони.

Відсутність окремого закону, спрямованого на впорядкування суспільних відносин, пов'язаних з використанням службової інформації, про нагальну необхідність якого наголошувало чимало науковців, продовжує залишатись головною проблемою щодо використання даного виду інформації з обмеженим доступом у державі.

Не визначеність на рівні закону процедури віднесення інформації до категорії службової спонукала фахівців у галузі права шукати інші шляхи для вирішення даної проблеми. У цьому зв'язку головним завданням стає формування відомчих переліків відомостей, що становлять службову інформацію, які повинні створювати органи державної влади, органи місцевого самоврядування, інші суб'єкти владних повноважень, у тому числі на виконання делегованих повноважень.

Важливість створення зазначених переліків полягає у тому, що саме вони, у подальшому, дозволяють визначити чи містить матеріальний носій службову інформацію і, відповідно, надати йому гриф обмеження доступу «Для службового користування».

З 1998 року до 2011 року основними загальнодержавними вимогами щодо формування переліків службової інформації (на той час - конфіденційної інформації, що є власністю держави) були Орієнтовні критерії віднесення інформації до службової інформації, визначені у 13 додатку до Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію (затверджена Постановою Кабінету міністрів України від 27 листопада 1998 року № 1893).

Після прийняття законодавчого положення про те, що порядок віднесення інформації до службової регулюється законами (а не підзаконними актами) згадані Орієнтовні критерії втратили чинність. Хоча сама Інструкція про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію залишається чинною.

Ця Інструкція до сьогодні залишається єдиним нормативно-правовим актом, який регламентує питання пов'язані з використанням матеріальних носіїв, які містять службову інформацію.

Замість Орієнтовних критеріїв віднесення інформації до категорії службової, стаття 9 Закону України «Про доступ до публічної інформації» визначає, що до службової інформації може належати така:

- що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень;

- зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

Розмитість та неконкретність цих критеріїв різко контрастує з визначенням критеріїв віднесення відомостей до державної таємниці, зазначених у відповідному Законі та їх конкретизацією у ЗВДТ.

Зазначені положення ст. 9 Закону «Про доступ до публічної інформації» є юридичною основою для подальшого формування переліків службової інформації органами державної влади, органами місцевого самоврядування, іншими суб'єктами владних повноважень, та створюють передумови неоднозначних підходів до обмеження доступу до інформації.

Аналіз значної кількості публікацій стосовно використання службової інформації дозволяє стверджувати, що нормативно-правова неврегульованість використання службової інформації породжує у суспільстві негативну тенденцію щодо сприйняття обмеження доступу до інформації як способу приховати інформацію, що дискредитує владу.

Вирішення питання нормативного врегулювання процедури віднесення відомостей до службової інформації потребує нагального закріплення як концептуальних засад, так і механізмів їх реалізації спрямованих на:

- визначення основного категорійного апарату у сфері використання службової інформації (понять «службова інформація» («службова таємниця»), «охорона службової інформації»; «віднесення інформації до категорії службової», «суспільно-необхідна інформація», «інформація з обмеженим доступом» тощо);

- удосконалення процедури віднесення інформації до категорії службової (створення типового загальнодержавного переліку службової інформації, обрахування шкоди від розголошення

службової інформації; визначення суспільно-необхідної інформації тощо);

- визначення строків та порядку перегляду службової інформації;

- визначення уповноважених державних суб'єктів та ефективних механізмів контролю за її використанням тощо.

УДК 351.746

Козій О. М.
Національна академія СБ України

ФОРМАЛІЗАЦІЯ ПОДАННЯ ІНФОРМАЦІЙНИХ ПРОЦЕСІВ

Складна оперативна обстановка, що склалася у існуючих політичних та економічних умовах нашої держави, у тому числі з врахуванням антитерористичної операції, яка проводиться на сході країни, значно збільшилася кількість проведення негласних оперативних заходів оперативно-технічними підрозділами (далі - ОТП) СБ України, у порядку визначеному Законом України «Про оперативно-розшукову діяльність» [1]. Зазначене ускладнює інформаційну діяльність ОТП СБ України та призводить до збільшення об'ємів інформації, яку вони отримують за результатами їх проведення в умовах протидії виникаючим каналам витоку інформації.

Аналіз основних особливостей інформаційної діяльності ОТП СБ України в умовах протидії каналам витоку інформації, як об'єкта моделювання, проведений з метою вибору відповідних методів і обґрунтування принципів побудови моделі, показав, що до числа таких особливостей у першу чергу необхідно віднести [2]:

- стохастичність інформаційних процесів у діяльності ОТП СБ України, обумовлена випадковими проміжками часу виконання процедур збору, обробки інформації, прийняття рішень і керування;

- стохастичність впливу погроз безпеки інформаційної діяльності ОТП СБ України й наявність двох рівнів протидії погрозам:

- нижнього - обумовленого структурно-залежними механізмами забезпечення інформаційної безпеки;

- верхнього - обумовленого структурно-незалежними механізмами забезпечення інформаційної безпеки.

До теперішнього часу, для дослідження процесів з такими особливостями, розроблена велика кількість моделей, що відносяться до класу математичних.

Методи математичного моделювання в цей час широко застосовуються в дослідженні складних систем, завдяки своїй ефективності, оперативності й дешевині в порівнянні з натурними випробуваннями цих систем [3]. Серед методів математичного моделювання найбільше поширення одержали методи аналітичного та імітаційного моделювання.

Разом з тим, наведені вище особливості інформаційної діяльності ОТП СБ України, як об'єкта моделювання, а також незначна глибина опрацювання питань формалізації інформаційних процесів у цих системах обумовили вкрай обмежене число аналітичних і імітаційних моделей. Основним недоліком імітаційних моделей інформаційної діяльності ОТП СБ України є обмежені можливості застосування класичних методів математичного аналізу при проведенні досліджень, що призводить, у деяких випадках, до суперечливості отриманих результатів. Істотний недолік аналітичних моделей інформаційної діяльності - низька адекватність процесів моделювання.

Разом з тим відомо [4], що математичні моделі, засновані на комбінації аналітичного й імітаційного підходів, володіють, у порівнянні з моделями, заснованими тільки на методології імітаційного або аналітичного моделювання, низкою переваг, до числа яких відносять:

- простота опису й формального подання процесів моделювання;

- можливість аналізу параметрів класичними методами математичного аналізу;

- низька вартість і можливість одержання результатів з необхідною точністю й адекватністю процесом моделювання.

Незважаючи на те, що вдосконалення методології математичного моделювання стало надзвичайно актуальною проблемою, розробка моделей дослідження ефективності заходів щодо протидії каналам витоку інформації практично не проводилися.

Розробка математичної моделі інформаційної діяльності ОТП СБ України відповідно до визначених особливостей полягає у формалізації її інформаційних процесів і синтезі моделей цих процесів.

В основу формалізації інформаційних процесів у ОТП СБ України в умовах протидії каналам витоку інформації повинно бути покладене подання різнотипних процедурного й функціонального описів цих процесів у вигляді однотипного ієрархічного опису. Як засіб первинної формалізації інформаційної діяльності ОТП СБ України в умовах комплексного застосування різнорідних підходів до забезпечення інформаційної безпеки пропонується використовувати методологію структурного аналізу.

Література

1. Закон України "Про оперативно-розшукову діяльність" від 18.02.1992 № 2136-XII [Електронний ресурс]. – Режим доступу: http//rada.gov.ua;

2. Нечеткие множества в моделях управления и искусственного интеллекта. / Под ред. Д.А. Поспелова. – М.: Наука, 1986. – 312 с.;

3. Советов Б.Я., Яковлев С.А. Моделирование систем: Учебник для вузов по спец. «Автоматизированные системы управления». – М.: Высшая школа, 1985. – 271 с.;

4. Бусленко Н.П. Моделирование сложных систем. – М.: Наука, 1978. - 400 с.

УДК 005.3

Михайлов А. А.
Служба безпеки України

РЕФОРМУВАННЯ СИСТЕМИ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ ТА СЛУЖБОВОЇ ІНФОРМАЦІЇ В КОНТЕКСТІ ЄВРОАТЛАНТИЧНОЇ ІНТЕГРАЦІЇ

На сучасному етапі глибоких суспільно-політичних і соціально-економічних перетворень в Україні, спрямованих на розбудову демократичної держави, одним із пріоритетних завдань виступає захист життєво важливих інтересів людини і громадянина, суспільства й держави.

Стаття 17 Конституції України визначає, що забезпечення інформаційної безпеки є однією з найважливіших функцій держави, справою всього Українського народу. Тому, в умовах сьогодення, коли Російська Федерація окупувала частину території

України та розв'язала воєнну агресію на території Донецької і Луганської областей, керівництвом нашої країни значна увага приділяється питанням функціонування повноцінної та ефективної системи охорони інформаційних ресурсів, насамперед секретної та службової інформації.

Зокрема, Стратегією національної безпеки України, яку затверджено Указом Президента України від 26 травня 2015 року № 287/2015, передбачено реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом, захисту державних інформаційних ресурсів, систем електронного врядування, технічного і криптографічного захисту інформації з обмеженим доступом з урахуванням практики держав-членів НАТО та ЄС.

Необхідність формування нових підходів до забезпечення функціонування системи охорони інформації з обмеженим доступом зумовлена передусім взятим Україною курсом на інтеграцію у світове співтовариство та розширенням міжнародного співробітництва у політичній, оборонній, науково-технічній та інших сферах діяльності.

З метою реалізації визначених у Стратегії національної безпеки України завдань, Службою безпеки, як спеціально уповноваженим державним органом у сфері забезпечення охорони державної таємниці, у 2015 році розпочато роботу з адаптації та гармонізації національного законодавства до стандартів безпеки НАТО та ЄС.

Важливість зазначеного питання, яке безпосередньо стосується національної безпеки України, потребує виваженого підходу до впровадження певних новацій та ретельного вивчення практики їх застосування в інших державах. При цьому, врахуванню підлягає також вітчизняний досвід у цій сфері, а також досвід іноземних держав, які проводили реформування свого законодавства за схожих з Україною підстав та умов (Польщі, Румунії, Литви, Молдови).

У зв'язку з цим, спеціально створеною в СБУ робочою групою, за результатами проведеного аналізу вимог стандартів безпеки інформації країн євроатлантичної спільноти, визначено основні напрями, за якими у подальшому здійснюватиметься дослідження.

Серед таких напрямів дослідження, метою якого є визначення переліку, обсягу та змісту змін, які планується внести до

нормативно-правових актів України, та підготовка проекту Концепції реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом, слід виділити наступні:

- можливість впровадження встановлених політикою безпеки інформації НАТО та ЄС стандартів та процедур безпеки щодо визначення ступенів обмеження доступу (важливості) інформації, доступ до якої обмежується в інтересах цих міжнародних організацій («класифікованої інформації»);
- врегулювання функцій державних органів у сфері охорони секретної інформації;
- удосконалення порядку перевірки осіб у зв'язку з допуском їх до державної таємниці;
- удосконалення механізму засекречування та розсекречування інформації;
- перегляд процедури надання, зупинення та скасування спеціального дозволу на провадження діяльності, пов’язаної з державною таємницею;
- можливість застосування вимог НАТО та ЄС щодо фізичної безпеки (поділу на відповідні зони залежно від рівня секретності інформації);
- удосконалення державного контролю і координації діяльності державних органів з питань технічного захисту інформації.

Виходячи з практики, а також досліджень і публікацій ряду вчених, особлива увага приділяється питанням нормативно-правового врегулювання такого виду інформації з обмеженим доступом, як службова інформація.

Наразі, законодавче тлумачення службової інформації, яке наведено у статті 9 Закону України «Про доступ до публічної інформації», не містить чітких критеріїв віднесення інформації до службової.

Відповідно до положень цього Закону відомості, що становлять службову інформацію, визначаються у відповідних переліках, які складаються органами державної влади, органами місцевого самоврядування, іншими суб'єктами владних повноважень, у тому числі на виконання делегованих повноважень.

Враховуючи, що на законодавчому рівні єдині вимоги щодо таких переліків не встановлені, розпорядники інформації відносять її до службової на свій розсуд. При цьому, контроль за цим процесом не здійснюється жодним державним органом.

Вказане створює передумови до безпідставного оприлюднення інформації, у тому числі зібраної у процесі оперативно-розшукової, контррозвідувальної діяльності та у сфері оборони країни, витік якої може завдати шкоди національним інтересам України.

Таким чином, першочергово постає питання щодо запровадження поряд із державною таємницею поняття «службової таємниці» або іншого терміну для визначення категорії інформації, яка на даний час визначена як службова.

Зазначений порядок полягає у застосуванні встановлених НАТО та ЄС стандартів і процедур безпеки до всієї інформації, доступ до якої обмежується (загальноприйнятий термін – «класифікована інформація»). Ступені обмеження доступу (важливості) такої інформації розподіляються за рівнем шкоди, яку може бути заподіяно інтересам міжнародних організацій та держав-учасниць у разі розголошення класифікованих відомостей.

Закріплення на законодавчому рівні критеріїв для віднесення інформації до державної та службової таємниці з відповідними грифами обмеження доступу дозволить демократизувати цей процес (забезпечивши його прозорість) та сприятиме оптимізації роботи з визначення ступенів секретності матеріальних носіїв інформації.

З урахуванням міжнародного досвіду внесення змін потребує процедура засекречування та розсекречування інформації, зокрема в частині функціонування інституту державних експертів з питань таємниць.

Удосконалення вимагає порядок перевірки громадян у зв’язку з допуском до державної таємниці, оскільки встановлені на даний час для органів СБУ терміни її проведення не дають можливості всебічно та об’єктивно вивчати питання, що ставляться перед цими органами. Тому, необхідним вбачається збільшення терміну проведення такої перевірки залежно від форми допуску, її поглиблення, розширення переліку підстав, за яких допуск до державної таємниці на надається тощо. При цьому, слід враховувати вимоги НАТО щодо необхідності врахування при вирішенні питань допуску громадян до секретної інформації критеріїв благонадійності, ступеня довіри та надійності особи, а також її близьких родичів й оточення.

Змін також потребує дозвільна система провадження підприємствами, установами, організаціями діяльності, пов’язаної з

державною таємницею. Зокрема, слід врахувати, що суб'єктами режимно-секретної діяльності в більшості є державні органи, призупинення чи скасування яким відповідного спецдозволу призведе до припинення їх діяльності.

З метою зосередження основних зусиль на збереженні секретної інформації відповідно до її важливості, зони, де така інформація обробляється та зберігається, доцільно класифікувати, встановивши вимоги щодо її захисту залежно від класу зони (зональний принцип забезпечення фізичної безпеки інформації закріплено у стандартах безпеки НАТО та ЄС).

Очевидно, що система охорони державної таємниці функціонуватиме лише за умови відповідності правових норм законодавства, які регулюють відносини в цій сфері, сучасному розвитку суспільства, держави, міжнародного співробітництва та наявним загрозам безпеці інформації (як зовнішнім так і внутрішнім).

У зв'язку з цим, під час роботи з реформування законодавства у сфері безпеки інформації, поряд із міжнародним досвідом, враховуватимуться наявні напрацювання СБУ, інших державних органів та науковців.

Література

1. Закон України «Про державну таємницю» від 21.01.1994 № 3855-XII;
2. Закон України «Про доступ до публічної інформації» від 13.01.2011 № 2939-VI;
3. Закон Республіки Польща «Про охорону інформації з обмеженим доступом» від 05.08.2010;
4. Закон Республіки Молдова «Про державну таємницю» від 27.112008 № 245-XVI;
5. Закон Румунії «Про охорону інформації з обмеженим доступом» № 182/2002;
6. Політика безпеки НАТО С-М (2002)49 від 17.06.2002;
7. Правила безпеки для охорони інформації з обмеженим доступом ЄС від 23.09.2013 (2013/48/EU);
8. Домовленості про безпеку між Службою безпеки України (СБУ) та Управлінням безпеки Генерального секретаріату Ради ЄС (УБГСР ЄС) і Департаментом безпеки Європейської комісії (ДБЄК) стосовно захисту інформації з обмеженим доступом, якою обмінюються України та ЄС.

УДК 355.40:351.746.1

Попутніков В. Б.
Національна академія СБ України

ШЛЯХИ УДОСКОНАЛЕННЯ ПРАВОВОГО ТА ОРГАНІЗАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ ПРИ ЗДІЙСНЕННІ КОНФІДЕНЦІЙНОГО СПІВРОБІТНИЦТВА

Важливим питанням є забезпечення охорони державної таємниці при здійсненні конфіденційного співробітництва.

Так, після змін до Закону України "Про державну таємницю", що були внесені Законом України від 06.07.2010 № 2432-VI, у статті 27 визначено, що доступ до державної таємниці, крім інших категорій осіб, надається:

- особам, залученим до конфіденційного співробітництва з оперативними підрозділами правоохоронних та інших спеціально уповноважених органів, які проводять оперативно-розшукову, розвідувальну або контррозвідувальну діяльність, у порядку, визначеному керівниками зазначених органів за погодженням із Службою безпеки України;
- особам, залученим до конфіденційного співробітництва оперативними підрозділами Служби безпеки України - у порядку, визначеному Головою СБУ.

У зв'язку із цим, на відомчому нормативному рівні такий порядок наприкінці 2010 року було визначено відповідною Інструкцією.

Слід підкреслити, що запроваджений тоді механізм фактично діє і зараз, хоча згадану Інструкцію у серпні 2014 року визнано такою, що втратила чинність, а її приписи увійшли окремим розділом до наказу СБУ з питань конфіденційного співробітництва.

На моє переконання, запроваджений підхід є єдино можливим в межах чинного законодавства.

Так, виходячи з норми статті 22 Закону (у новій редакції), надання допуску до державної таємниці залученим до конфіденційного співробітництва особам не передбачено. З іншого боку слід враховувати, що вказані особи можуть ознайомлюватися лише з окремими секретними відомостями і з огляду на специфіку негласної діяльності не мають реальної потреби для оформ-

лення їм постійного допуску за тією чи іншою формою, оскільки вони не працюють з таємною документацією чи виробами. Більш того, окремі категорії осіб (зокрема, з кримінального середовища, а також з числа іноземців та осіб без громадянства) взагалі за встановленою процедурою й не могли б отримати допуск до державної таємниці.

Поряд із цим, якби нова редакція Закону навіть й дозволяла надавати допуск до державної таємниці особам, залученим до конфіденційного співробітництва з оперативними підрозділами правоохоронних та інших спеціально уповноважених органів, які проводять оперативно-розшукову, розвідувальну або контррозвідувальну діяльність, існуючий механізм його документального оформлення створює передумови для розшифрування джерел, є занадто складним, що однозначно ускладнило б ведення оперативної роботи.

На сьогодні концептуально визначено, що обсяг секретної інформації, що доводиться до особи, залученої до конфіденційного співробітництва, залежить від конкретної оперативної ситуації і повинен бути мінімально необхідним для виконання покладених на неї функцій. Розроблено також механізм надання відповідного дозволу, порядок заохочення конфідентів, яким надано доступ до державної таємниці, та система контролю за дотриманням у ході конфіденційного співробітництва положень законодавчих і відомчих нормативно-правових актів з питань їх охорони.

Зокрема, забороняється надавати особам, залученим до конфіденційного співробітництва, доступ до відомостей, що становлять державну таємницю, необхідність в яких не викликається характером оперативних завдань, що ними виконуються.

Таким чином, внесення вищеозначених змін до законодавства у сфері охорони державної таємниці та прийняття на цій основі відомчих нормативно-правових актів дозволило зробити Службі безпеки України впевнений крок до розв’язання правових колізій, що існували довгий час.

У той же час, для створення правових підстав притягнення осіб, з якими здійснюється конфіденційне співробітництво, до відповідальності у разі розголошення секретної інформації оперативного характеру, що стало їм відома під час такого співробітництва, законодавець має бути послідовним і внести необхідні зміни й доповнення до відповідних актів законодавства України.

Разом із цим, незважаючи на певну оптимізацію поряду надання доступу вказаним вище особам до секретної інформації оперативного характеру, на сьогодні ще не всі проблеми вдалося розв'язати.

Так, залишається невирішеним питання надання доступу до державної таємниці особам, які сприяють діяльності СБУ. Документальне оформлення рішень про надання доступу до секретної інформації оперативного характеру значною мірою забюрократизовано, що, у свою чергу, на практиці створює певні труднощі в роботі оперативного складу.

З огляду на зазначене, в рамках діяльності у складі робочої групи, створеної розпорядженням ЦУ СБУ у липні минулого року, мною розроблено конкретні пропозиції, реалізація яких дозволить суттєво покращити стан справ та вирішити основні нагальні проблеми.

Подальші кроки щодо кардинального удосконалення вказаного питання, на мою думку, полягають у звуженні змісту відомостей, які можуть бути віднесені до державної таємниці.

У цьому контексті, вбачається за доцільне провести ґрунтовну роботу в рамках затвердженої у вересні минулого року керівництвом СБУ Програми дій щодо адаптації та гармонізації національного законодавства до стандартів НАТО та ЄС, яку розроблено відповідно до Стратегії національної безпеки України, затвердженої Указом Президента України від 26.05.2015 № 287/2015.

Зокрема, абзац восьмий пункту 4.12 згаданої Програми передбачає реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом, з урахуванням практики держав членів НАТО та ЄС.

Тому, у ході підготовки проекту Концепції реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом, захисту державних інформаційних ресурсів, систем електронного врядування, технічного і криптографічного захисту інформації з обмеженим доступом, яку передбачається внести на розгляд до РНБО України, будуть опрацьовуватись питання щодо:

- введення нових категорій інформації з обмеженим доступом – поряд з державною таємницею ввести службову таємницю;

- розмежувати на законодавчому рівні критерії обмеження доступу до різних видів секретної інформації;

- удосконалення процедури обмеження доступу до секретної інформації та його зняття.

З урахуванням цього, у процесі напрацювання нових підходів пропонується понизити (там, де доцільно) грифи обмеження доступу до певного кола секретної інформації оперативного характеру, яка стосується здійснення органами і підрозділами СБУ конфіденційного співробітництва.

УДК 343.4

Семенюк О. Г.
кандидат юридичних наук
Служба безпеки України

ЧУЖА ТАЄМНИЦЯ ЯК ПРЕДМЕТ ЗЛОЧИНУ

Будь-якій таємній інформації властива персоніфікованість, тобто приналежність конкретному суб'єктові права. Вона поєднана з наявністю його інтересу або обов'язку в збереженні таємниці, обумовлена тим, що збереження в таємниці конкретних відомостей здійснюється з метою унеможливлення настання потенційної шкоди, яка може бути завдана власнику таємної інформації від її поширення.

Шкода може виражатися у нанесенні як матеріальних, так і моральних, у тому числі й політичних збитків. Крім того, метою обмеження доступу до інформації є не лише намагання запобігти шкоди, а й бажання отримати певні переваги (перемога у військовій битві, можливість отримати певний зиск від володіння секретами вироблення конкурентоздатної продукції). Втрата таких переваг внаслідок несанкціонованого витоку прихованої інформації також розглядається як завдання збитків (упущення вигоди). Розмір збитків залежить від цінності такої інформації, під якою слід розуміти рівень її значущості для інтересів конкретного суб'єкта інформаційних відносин.

Виходячи з цього, нами пропонується покласти в основу класифікації таємної інформації суб'єкта, якому безпосередньо буде завдано шкоду внаслідок її несанкціонованого витоку (розголошення або втрати матеріальних носіїв такої інформації), а всю таємну інформацію поділяти на таємницю фізичної особи, комерційну та державну таємницю.

Так як власником таємної інформації можуть виступати окремі фізичні особи, певні соціальні групи (сім'я, корпорація людей, що об'єдналися для досягнення значущих для них цілей) або держава, то цінність такої інформації для різних суб'єктів соціальних відносин є різною. При цьому уявлення щодо цінності інформації, змістовні критерії обмеження доступу до окремих її відомостей безпосередньо формує суспільство.

Так, укорінені в суспільній свідомості на конкретному історичному етапі уявлення щодо пристойності тих чи інших вчинків безпосередньо впливають на зміст таємниці приватного життя, сімейних відносин та більшості форм соціально-побутового спілкування. Предметом інформації, що приховується фізичною особою від сторонніх осіб, є такі дійсні чи вигадані дані про осіб, їх дії або дії щодо них, які особа бажає зберегти у таємниці і розголошення яких, на її думку, скомпрометує або принизить честь і гідність її чи близьких їй осіб. До таких відомостей, зокрема, можуть відноситися дані про інтимні сторони життя, захворювання, неблаговидні вчинки, злочинну діяльність тощо. Цінність таємниці тут полягає у можливості збереження поваги оточення до громадянина на тому самому рівні, що і до розголошення цих відомостей, а в окремих випадках збереження життя та здоров'я власника прихованої інформації.

Цінність комерційної таємниці виражається в тих можливих прибутках або збитках, що можуть бути отримані внаслідок її використання іншими, так як у цій сфері цінність інформації безпосередньо обчислюється у грошових одиницях.

Потреба держави у засекречуванні певних відомостей обґрунтовується необхідністю забезпечення національної безпеки, територіальної цілісності, незалежної внутрішньої та зовнішньої політики, відстоювання власних інтересів шляхом впливу на поведінку інших суб'єктів міжнародних відносин у бажаному для національних інтересів напрямку, громадського порядку або охорони здоров'я населення. При цьому обсяг відомостей, які приховуються державою, знаходиться у прямій залежності від стану політичної системи та збалансованості інтересів у суспільстві, здатності своєчасно реагувати на зміни, що відбуваються у політичній, економічній і соціальній сферах під впливом історично обумовлених закономірностей.

На наше переконання, спроба окремих науковців [1, с.20-21] обґрунтувати найбільшу суспільну цінність державної таємниці –

це намагання виправдати ситуацію, за якої держава безконтрольна в питаннях засекречування інформації, а сфера державно-владних повноважень виконує не тільки функцію охорони певних категорій відомостей від поширення, але й набуває політичного відтінку, перетворюючись в один із істотних елементів у механізмі державного управління.

Ми повністю поділяємо думку В.А.Ліпкана та В.Ю.Баскакова, що доречніше говорити не про соціальну цінність інформації, а про цінність для її власника, оскільки така інформація може не мати жодної соціальної цінності для суспільства, а для її власника має значну цінність через невідомість іншим [2, с. 97].

Поступове усвідомлення того, що будь-яка таємниця має значну цінність для її власника, призводить до того, що застосовані до охорони державної таємниці заходи безпеки беруться сьогодні за зразок під час запровадження механізмів охорони банківської таємниці, захисту персональних даних, інших інформаційних масивів. При підборі кандидатів на роботу у комерційні структури, де циркулює конфіденційна інформація, активно використовуються детектори брехні, здійснюються тривалі перевірки благонадійності майбутніх працівників, вживаються безпрецедентні заходи із забезпечення безпеки інформації.

На цьому тлі вражає безвідповідальне ставлення держави до збереження у таємниці історії хвороб або інших матеріальних носіїв інформації, в яких відображаються відомості про стан здоров'я, факт звернення за медичною допомогою, діагноз, а також про відомості, одержані при медичному обстеженні фізичної особи. Жахливий стан фінансування закладів охорони здоров'я зводить нанівець спроби забезпечити надійну охорону такої інформації, а наміри уряду перевести історії хвороб в електронний документообіг несуть пряму загрозу їх потрапляння у мережу Інтернет, знижує рівень її захищеності від стороннього втручання.

Конституція України 1996 року визнала людину, її життя і здоров'я, честь і гідність, недоторканість і безпеку найвищою соціальною цінністю (ст. 3). Проте стан захищеності таємної інформації про фізичну особу та реальні можливості її правового захисту у випадку несанкціонованого розголошення свідчать про суттєве відставання правового регулювання цих суспільних відносин від задекларованої у Конституції її значущості.

Виходом із цієї ситуації є найскоріше законодавче вироблення єдиного для всіх видів таємниць комплексу правових, ор-

ганізаційних, режимно-секретних, адміністративних та кримінально-правових заходів охорони таємної інформації. Держава зобов'язана взяти на себе формування ефективного механізму захисту різних видів таємниці, що ґрунтується на принципі гарантування державою безпеки особистості, суспільства, держави.

Одним із напрямків реалізації цієї потреби повинна стати відмова від диференціації кримінальної відповідальності за розголошення таємної інформації або втрати її матеріальних носіїв залежно від її власників. Для цього нами пропонується ввести до юридичного обігу в якості предмета злочину узагальнююче поняття «чужа таємниця», яке має охоплювати всі види таємної інформації, а саме: таємницю фізичної особи, комерційну та державну таємниці. За таких умов кримінальна відповідальність повинна наступати не за розголошення державної, слідчої, лікарської таємниць, таємниці усиновлення тощо, а за розголошення чужої таємниці або втрату її матеріальних носіїв. З огляду на поширеність і суспільну небезпеку такого явища, як протиправне заволодіння чужою таємницею з метою її подальшого використання на шкоду інтересам її власника, нами пропонується встановити кримінальну відповідальність за протиправне заволодіння такою інформацією.

Ще не так давно державна власність визнавалася більш важливою цінністю, ніж особиста (приватна). Так, за Кримінальним кодексом України 1961 року, розкрадання державного або суспільного майна в особливо великих розмірах (стаття 86-1) каралося позбавленням волі на строк від десяти до п'ятнадцяти років із конфіскацією майна та засланням на строк до п'яти років або смертною карою з конфіскацією майна. В той же час, за крадіжку індивідуального майна, яка завдала значної шкоди потерпілому, або вчинену за попередньою змовою групою осіб або повторно (частина друга статті 140), призначалося покарання у вигляді позбавлення волі на строк до п'яти років з конфіскацією майна або без конфіскації.

Із прийняттям у 1991 році Закону України «Про власність» приватна, колективна та державна форми власності були визнані рівноправними. Стаття 13 Конституції України проголосила рівність усіх суб'єктів права власності перед законом і забезпечення захисту їх прав державою. Кримінальний кодекс України 2001 року відмовився від розмежування відповідальності за про-

типравні посягання на різні форми власності та встановив кримінальну відповідальність за крадіжку чужого майна (стаття 185), чим фактично урівняв соціальну цінність усіх форм власності.

Саме в напрямку уніфікації підходів до кримінального переслідування й покарання винних за порушення правил поводження з чужою таємницею повинно просуватися кримінальне законодавство України, а науковці мають спрямувати свої дослідження на пошук аргументів для обґрунтування єдиної природи таємниці та рівноправності всіх її видів.

Література

1. Слободанюк И.А. Развитие уголовного законодательства об ответственности военнослужащих за посягательства на режим сохранности государственной и военной тайны. Монография в авторской редакции – М.: Военный университет, 2005. – 182 с.

2. Ліпкан В.А. Адміністративно-правовий режим інформації з обмеженим доступом в Україні : [Монографія] / В.А.Ліпкан, В.Ю.Баскаков / За заг. Ред. В.А.Ліпкана. – К.: ФОП О.С.Ліпкан, 2013. – 344 с.

УДК 65.012.8 (477)

Сидоренко С. М.
Національна академія СБ України

ЗАХИСТ СЕКРЕТНОЇ ІНФОРМАЦІЇ НАТО В РУМУНІЇ ЯК УМОВА ПРИЄДНАННЯ ДО АЛЬЯНСУ

Захист секретної інформації НАТО, є і буде залишатися одним з актуальних інтересів для Румунії, як необхідної складової приєднання до Альянсу, так і після становлення повноправним членом НАТО. Після приєднання до НАТО, виникнення будь-яких порушень безпеки секретної інформації може потягнути за собою припинення її надходження, що унеможливить ефективну участь у відповідних заходах Альянсу. Отже, в першу чергу, мова йде про національні стратегічні інтереси. Всі фактори, які можуть сприяти забезпеченню захисту секретної інформації, мають знаходитися у суворій відповідності згідно з вимогами чинного законодавства. Розуміння потреби у захисті секретної інформації може бути створено лише в рамках інформування спільноти, з

урахуванням зазначеного обізнаність і залучення громадян країни – це концепція, без якої успіх у діях буде не повним.

Служба безпеки НАТО /NATO Office of Security (NOS) – це установа відповідальна за забезпечення координації безпеки в рамках Альянсу. Її фахівці добре відомі своїми знаннями та професіоналізмом, надають консультативні послуги в оцінках прогресу Румунії щодо застосування стандартів захисту секретної інформації. Вже станом на 2003 рік система захисту секретної інформації Румунії оцінюється NOS як така, що відповідає вимогам Альянсу.

Будь-який "витік" секретної інформації НАТО має стримуватись шляхом застосування захисних заходів, передбачених національними стандартами. Всі особи, залучені до таких заходів, несуть не лише юридичну відповідальність, а й моральну щодо можливої шкоди Румунії, що може вплинути на перспективи Євроатлантичної інтеграції.

Рішення про створення складної і скоординованої національної системи захисту секретної інформації, зосередженої на життєздатності та ефективності національної безпеки є абсолютно новим і виникло в результаті наміру Румунії вступити в НАТО, і задля цього задовольнити відповідні вимоги НАТО. Згідно закону no.182/2002 “Про захист секретної інформації”, у зв'язку з логічним і прагматичним аналізом в сфері доктрин НАТО, застосовуються заходи для захисту національної секретної інформації. Що стосується національної безпеки Румунії, було створено установу (ORNISS) яка має повноваження по реалізації заходів захисту секретної інформації з дотриманням чинного законодавства, прав і свобод людини і громадянина. Завдання ORNISS полягає в єдиному забезпеченні заходів щодо захисту секретної інформації на національному рівні задля створення ефективної системи захисту інформації (спільно з іншими установами). Основні інтереси ORNISS полягають у створенні бездоганного та ефективного функціонування систем, здатних забезпечити належний захист секретної інформації.

НАТО встановлює свої стандарти щодо відповідності персоналу, якому надається доступ до секретної інформації, задля чого забезпечуються достатні гарантії щодо лояльності, надійності і чесності особи. Особи, які працювали у колишній службі безпеки щодо захисту політичної системи, не можуть мати доступу до секретної інформації НАТО, оскільки їх діяльність є сум-

нівною щодо лояльності, надійності та чесності. Упередження румунської влади щодо цих аспектів обговорювалося на найвищому рівні держави. В результаті такого підходу, який пов'язаний з політичним рішенням, така вимога була відображена в нормах про захист секретної інформації у договорі Організації Північноатлантичного Договору з Румунією.

Доступ до інформації може бути наданий лише після того, як спеціальні служби безпеки SRI, SIE, MApN, MAI, MJ, SPP і STS, кожна в своїй галузі, здійснили перевірку. Перевірка задля безпеки спрямована на виявлення і оцінку ризиків у галузі безпеки секретної інформації, обумовлених наданням доступу до цієї категорії інформації певній особі. Перевірка безпеки здійснюється у зв'язку з можливим доступом особи до секретної інформації а не для морального осуду особи. Оцінка ризиків майбутніх відносин є вкрай важливою. Негативна оцінка при перевірці не є засуджуючим фактором і стосується лише відносин доступу до секретної інформації, яка може зазнати ризиків щодо безпеки викликаних, наприклад, певними аспектами життя та діяльності близьких людей або деяких проблем зі здоров'ям. Перш ніж приймати рішення про надання чи не надання доступу особі, національний орган безпеки ORNISS відповідально аналізує висновки перевірки, для прийняття обґрунтованого висновку. Оскільки ці дані стосуються особи і повинні бути захищені у відповідності до закону та враховуючи, що ORNISS не має прямого відношення до перевірки, ORNISS не оприлюднює результати перевірки, а лише приймає рішення щодо надання або відмову в доступі до секретної інформації. Умови, за якими особа може отримати доступ до секретної інформації, чітко передбачені законом, так само як і зміст про безпеку, і вони доступні для будь-якої заінтересованої фізичної або юридичної особи. З цієї точки зору, керівники установ, що вимагають доступу до секретної інформації для одного із своїх службовців мають достатньо даних щоб приступити до першої оцінки, заснованої на звіті про зайнятість, що відповідає встановленим критеріям по відношенню до працівника.

Основні етапи, які повинні бути охоплені перевіркою. До призначення особи на посаду, що вимагає доступу до секретної інформації певного ступеня секретності (національної категорії або інформації НАТО), він/вона повинен дати згоду на здійснення перевірки. Особа заповнює спеціальну форму анкети щодо безпеки, і погоджується на здійснення перевірки. Керівник устано-

ви вимагає від ORNISS почати процедуру перевірки з дотриманням норм для надання доступу до секретної інформації НАТО, або дотримання процедур, за якими видається рішення про видачу свідоцтва про безпеку щодо національної секретної інформації. ORNISS вимагає від установ, відповідальних за проведення перевірки, провести перевірку щодо безпеки і на основі їх висновків приймає рішення про надання доступу або видачу сертифіката. Установа може володіти секретною інформацією, у разі створення таких умов: наявна структура безпеки і відповідні працівники з питань безпеки, які поряд з керівниками відповідних установ та згідно закону здійснюють важливі функції в галузі безпеки секретної інформації (аналог РСО в Україні); інше вимога відноситься до ефективного застосовування захисних системи. Важливо мати на увазі, що для доступу до секретної інформації, зокрема перевірки персоналу або видачі сертифікату про безпеку, обов'язковою умовою є знання необхідних принципів безпеки.

Уповноважені служби безпеки здійснюють перевірку з дотриманням правової процедури, враховуючи строки надання відповіді, наприклад, у випадку національної секретної інформації термін надання відповіді від 9 до 21 тижня. Водночас, навіть в ці терміни не завжди можна переконатися в тому, що вимоги перевірки для доступу до секретної інформації були дотримані, і це одне з пріоритетних завдань по відношенню до будь-якого іншого рішення. У зв’язку з цим, закон дозволяє владі при проведенні перевірки щодо безпеки перевищувати встановлені терміни і здійснювати додаткову перевірку, якщо наявні очевидні деякі ризики безпеки.

Проблема безпеки секретної інформації є важливою для інтересів Румунії, і якщо хто-небудь займає посаду у сфері захисту інформації повинен відноситись до цього з повною відповідальністю.

Одним з основних принципів організаційної політики в галузі кадрового управління і з урахуванням новизни проблеми та конкретних вимог, ORNISS обирає для вивчення осіб з урахуванням перспектив і майбутніх можливостей. Підбір персоналу було засновано на принципі двозначності, згідно з яким ORNISS приймає на роботу компетентний персонал, чий професіоналізм конкурентоспроможність і чия лояльність перевірена спеціальними заходами перевірки. З цієї точки зору, закон вимагає, щоб усі співробітники ORNISS, які безпосередньо беруть участь у діяльності щодо національної безпеки, повинні бути перевірені відносно безпеки і мати відповідний дозвіл з урахуванням ступеня

секретності. Крім того, особи, що належать до персоналу ORNISS не мають права займатися політичною діяльністю.

Абсолютно новою для Румунії є проблема співпраці підприємців (недержавних юридичних осіб) з Альянсом. Це новий вид діяльності щодо промислової безпеки, підхід до якого тільки формується, оскільки Румунія не мала відповідного попереднього досвіду роботи. У зв'язку з цим, існують деякі неясності з якими підприємцям доводиться стикатися. У цьому контексті, ці технічні питання поступово будуть вирішуватись. Таким чином, промислова безпека охоплює всі заходи щодо захисту секретної інформації, яка поширюється в промисловій сфері і пов'язана з веденням переговорів, підписанням секретний контрактів тощо. Промислова безпека складається із політичної безпеки щодо проведення переговорів, укладання та виконання секретних контрактів з додаткової безпеки секретних контрактів, які пов'язані з передачею секретної інформації в межах секретних контрактів. Участь у переговорах щодо укладення секретних контрактів допускається на основі дозволу щодо промислової безпеки видане для наукових досліджень, яке підтверджує дотримання мінімальних заходів безпеки передбачених стандартами Альянсу. Проведення секретного контракту здійснюється на основі перевірки щодо безпеки, а також наданні дозволу на певне наукове дослідження.

По суті, здійснюється перевірка щодо безпеки працівників, менеджерів та керівників, перш ніж вони братимуть участь у переговорах, підписанні секретних контрактів, які вимагають доступу до секретної інформації. У той же час об'єкт (будівля, кімната тощо), в якому відбуватиметься (ведення переговорів, аналіз документів, виробництво і т.п.) мають бути захищеним у відповідності з конкретними стандартами, з урахуванням наявних загроз безпеки.

Таким чином, "Промислова безпека" створює сприятливу основу для економічного розвитку, сприяє приватним господарюючим суб'єктам під час переговорів і укладання секретних контрактів, тобто договорів, які відносяться до національної безпеки, шляхом створення та забезпечення заходів щодо захисту секретної інформації від втрати, поширення, зміни або несанкціонованого знищення.

Отже, захист секретної інформації НАТО є і буде залишатися одним з актуальних інтересів для Румунії і розцінюється як необхідна умова приєднання та становлення повноправним членом НАТО. Небезпека виникнення будь-яких порушень щодо захисту

секретної інформації НАТО може стати передумовою до припинення її надходження, що унеможливить ефективну участь Румунії у відповідних заходах Альянсу. Приєднання Румунії до НАТО розглядалось з точки зору національних стратегічних інтересів. Будь-який "витік" секретної інформації НАТО стримувався шляхом застосування захисних заходів, передбачених національними стандартами. Всі особи, залучені до таких заходів несли не лише юридичну відповідальність, а й моральну щодо можливої шкоди Румунії, яка могла вплинути на перспективи Євроатлантичної інтеграції.

Література

1. Страны мира. Краткий политико-экономический справочник/Под общ. ред. И.С.Иванова. М. 1997. С. 336

2. За матеріалами інтерв'ю з професором доктором наук Маріусом Петреску – генеральним директором ORNISS, для журналу "Gândirea militara românească" 21.10.2003 р. http://www.orniss.ro/en/news.html)

3. Закон Румунії "Про вільний доступ до інформації, що представляє суспільний інтерес", http://www.publicinfo.ro/INITIAT/Legea%20accesului%20engl.pdf

4. http://www.publicinfo.ro/INITIAT/NormeMetodologiceLegeLiberAccesInformatie-engl.pd

5. http://www.orniss.ro/en/index.html

6. http://www.orniss.ro/en/legislation.html, http://www.sri.ro/

УДК 003.5

Сніцаренко П. М.
доктор технічних наук, старший науковий співробітник
Національний університет оборони України
імені І.Черняховського
Саричев Ю. О.
кандидат технічних наук, старший науковий співробітник
Національний університет оборони України
імені І.Черняховського

ТЕРМІНОЛОГІЧНІ ОСНОВИ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ У ВОЄННІЙ СФЕРІ

Висока динаміка подій в сучасному світі та потреба адекватного реагування на виклики і загрози, зокрема Україні, спричи-

няє нагальну потребу удосконалення інформаційного забезпечення державного управління як головної складової в меті забезпечення інформаційної безпеки держави. Важливо, що при цьому інформаційне забезпечення ґрунтувалося на єдиній методології, в основу якої покладено відповідний термінологічний базис.

Аналіз показує, що інформаційне забезпечення державного управління є складним та багатогранним, а його термінологічне визначення, а також споріднених із ним понять, сьогодні носить дискусійний характер, значна частина дефініцій, які вживаються в публікаціях, мають змістову суперечливість або однобічно відображають сутність. Отже, на сьогодні необхідного термінологічного базису немає, а тому відсутня і стала методологія, що шкодить практиці, у тому числі у воєнній сфері. У той же час потреби військової практики, в першу чергу стосовно координації з питань створення ефективної інформаційної інфраструктури, потребують однозначного оперування термінами і поняттями щодо інформаційного забезпечення у воєнній сфері. Тому існує актуальне наукове завдання розробки відповідної термінологічної основи.

Останнім часом в Міністерстві оборони України зроблено перші кроки у цьому важливому напрямі – розроблено та введено в дію військовий стандарт ВСТ 01.004.004 – 2014 (01). "Інформаційна безпека держави у воєнній сфері. Терміни та визначення", яким визначено, що "*інформаційне забезпечення у воєнній сфері* – сукупність заходів органів військового управління усіх рівнів, дій військ (сил) та інших суб'єктів інформаційної діяльності з метою створення (формування) і використання в інформаційному просторі воєнної сфери необхідних інформаційних ресурсів для реалізації процесів управління в інтересах оборони держави".

Між тим, застосування такого визначення стикається з тією особливістю, що у воєнній сфері існує декілька видів інформаційної діяльності із явними ознаками інформаційного забезпечення, які історично військовою практикою адміністративно рознесені, а тому не пов'язані ні єдиною методологією, ні єдиною координацією. Наприклад, цими ознаками характеризуються такі види забезпечення діяльності військових формувань як "розвідка" або "морально-психологічне", але входять вони до різних груп класифікації.

На наш погляд, з метою досягнення системної координації процесів розвитку інформаційної інфраструктури з єдиних пози-

цій забезпечення інформаційної безпеки у воєнній сфері, розрізненість таких споріднених понять потребує їх об'єднання в окрему (рамкову) класифікаційну групу. Для цього слід вважати доцільними наступні визначення видів інформаційного забезпечення у воєнній сфері.

Іміджеве – комплекс заходів, що здійснюється із застосуванням засобів масової інформації для висвітлення діяльності національних збройних сил, з метою формування позитивної громадської думки в суспільстві та на міжнародному рівні, а також сприяння зростанню престижу військової служби серед населення держави.

Морально-психологічне – сукупність заходів, які здійснюються з метою формування, підтримання та поновлення у особового складу морально-бойових і психологічних якостей, морально-психологічного стану військ (сил) на рівні, необхідному для успішного виконання завдань за призначенням.

Моніторинг загроз – комплекс заходів, що реалізує безперервний процес отримання інформації воєнного характеру на основі даних усіх видів воєнної розвідки, з метою оцінки та прогнозування розвитку воєнно-політичної та воєнно-стратегічної обстановки в регіоні, а також висвітлення умисних загрозливих дій державі в космічному, повітряному, наземному, надводному та підводному просторах.

Інформаційно-аналітичне – комплекс заходів, що реалізує процеси створення інформаційних продуктів на основі використання статичних інформаційних ресурсів, проведення розрахунків, моделювання ситуацій, аналізу і синтезу документованих даних та інформації з метою підтримки прийняття рішень органами військового управління всіх рівнів.

Організаційно-управлінське – комплекс організаційно-розпорядчих заходів, які реалізуються шляхом документообігу органами військового управління, командирами (начальниками) з метою формування (обґрунтування) і прийняття рішень, доведення їх до підлеглих, організації виконання та контролю.

Радіоелектронний захист – комплекс заходів щодо гарантування стійкості роботи радіоелектронних складових інформаційних засобів, інформаційних систем та інших носіїв інформаційних ресурсів в умовах радіопротидії з боку противника та взаємного електромагнітного впливу.

Дезінформаційне – комплекс заходів щодо введення противника в оману шляхом відволікаючих демонстративних дій, імітації, скритності основних дій з використанням макетів військових об'єктів, залистування та розповсюдження хибної інформації (чуток) на території, яку контролює противник.

Навігаційне – 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.

Топогеодезичне (*геоінформаційне*) – комплекс заходів щодо підготовки та доведення до органів військового управління всіх рівнів топографічних та спеціальних (тематичних) карт (у тому числі електронних), фотодокументів місцевості, а також астрономо-геодезичних та гравіметричних даних для здійснення просторової синхронізації при управлінні військами (силами) та зброєю в ході виконання ними поставлених задач.

Гідрометеорологічне – комплекс заходів щодо збору, аналізу та доведення до військ (сил) інформації про гідрологічну та метеорологічну обстановку на основі здійснення гідрологічних, метеорологічних та аерологічних спостережень і розроблення відповідних прогнозів.

Інформаційно-технічний вплив – комплекс акцій та атак, якими реалізується цілеспрямоване деструктивне електронне втручання в процес функціонування об'єктів інформаційної інфраструктури противника.

Інформаційно-психологічний вплив – цілеспрямоване інформаційне втручання у свідомість (підсвідомість) керівного та особового складу військ і населення противника з метою внесення змін у поведінку та (або) світогляд, які підривають їх морально-психологічний стан.

Запропоновані термінологічні визначення можуть бути використані при розробці методологічних основ реалізації інформаційного забезпечення державного управління у воєнній сфері з системних позицій забезпечення інформаційної безпеки, що дозволить розвивати інформаційну інфраструктуру держави, зокрема у воєнній сфері, виходячи із єдиної ідеології.

УДК 343.98: 343.45

Тищенко Є. Ф.
кандидат юридичних наук, доцент
Національна академія СБ України

ВИКОРИСТАННЯ СПЕЦІАЛЬНИХ ЗНАНЬ У КРИМІНАЛЬНИХ ПРОВАДЖЕННЯХ ПРО ЗЛОЧИНИ У СФЕРІ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ

Розслідування розголошення державної таємниці та втрати її матеріальних носіїв завжди відносилося до підслідності слідчих вітчизняних спецслужб. С.С. Кудінов зазначив, що лише протягом 2009-2013 р.р. слідчими СБ України розслідувалось понад 140 проваджень, кваліфікованих за ст.ст. 328, 329, 422 Кримінального кодексу України. Викликає занепокоєння те, що за даними Головного слідчого СБ України із зазначеної кількості до суду з обвинувальними актами (висновками) було направлено лише близько 35 % кримінальних проваджень [1]. Існує кілька причин низької результативності розслідувань таких проваджень, однією з яких є проблеми з використанням спеціальних знань. Вчені-криміналісти зазначають, що нині виникло багато нових науково-практичних напрямів, впровадження яких, перш за все у формі експертизи, настійно потребує судочинство. Щодо багатьох видів експертиз існують лише уривчасті й суперечливі відомості в періодичній юридичній літературі та інших публікаціях, а щодо деяких – відомості відсутні взагалі [2]. На нашу думку, це твердження можна повністю віднести до вперше на законодавчому рівні легалізованої у ст. 518 Кримінального процесуального кодексу України 2012 р. (далі – КПК) [3] – «експертизи щодо законності віднесення інформації у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку до державної таємниці, зміни ступеня секретності цієї інформації та її розсекречування, підготовки висновку щодо завданої національній безпеці України шкоди у разі розголошення секретної інформації чи втрати матеріальних носіїв такої інформації». Вважаємо, що цю багатослівну назву доцільно скоротити до словосполучення, більш широкого за змістом і лаконічнішого за формою – «експертиза з питань державної таємниці».

Безперечно, позитивним є те, що у КПК з 2012 р. вперше у вітчизняному кримінальному процесі з'явилася спеціальна Глава 40. «Кримінальне провадження, яке містить відомості, що становлять державну таємницю». Водночас низка питань стосовно деяких організаційних аспектів зазначених кримінальних проваджень не повністю вирішені.

Так, у ч. 1 ст. 518 КПК України законодавець визначив, що проведення експертиз з питань державної таємниці покладається на посадових осіб, які виконують функції державного експерта з питань таємниць відповідно до закону у сфері державної таємниці. Ми вважаємо, що це законодавче положення викликає ряд проблем. Указом Президента України від 01.12.2009 р. № 987 «Про Перелік посадових осіб, на яких покладається виконання функцій державного експерта з питань таємниць» визначено близько 140 посад, з призначенням на які особа автоматично набуває статус державного експерта з питань таємниць. Це, як правило, посади міністрів, їх заступників, перших керівників ряду важливих підприємств, установ та організацій тощо. На призначення таких посадовців часто й суттєво впливають політичні чинники. А через це у деяких випадках посади залишаються вакантними протягом тривалого часу. За відсутності призначеної посадової особи у міністерстві (відомстві тощо) відсутній і державний експерт з питань таємниць, що унеможливлює проведення зазначеної експертизи.

Крім цього, не завжди особи, котрих призначають на посади, зайняття яких передбачає виконання функцій державного експерта з питань таємниць, є висококваліфікованими фахівцями як в певних галузях знань за лінією роботи міністерств чи відомств, так і в питаннях охорони державної таємниці. Саме через це у деяких випадках, судову експертизу з питань державної таємниці, державні експерти з питань таємниць проводять не особисто, а задіюють можливості наявних при них експертних комісій з питань таємниць, і лише формально підписують висновки, підготовлені останніми (хоча після цього державні експерти й беруть на себе передбачену законом персональну юридичну відповідальність).

У разі виконання державними експертами з питань таємниць функцій судового експерта, на них поширюються повноваження, які КПК передбачено для експертів, зокрема: 1) вони мають усю сукупність прав, обов'язків і несуть встановлену законом кримі-

нальну, адміністративну чи дисциплінарну відповідальність; 2) одночасно вони відповідно до Закону України «Про судову експертизу», повинні: а) мати вищу освіту (у п. 1 ч. 1 ст. 102 КПК вимагається зазначати у висновку експерта його освіту, спеціальність); б) пройти підготовку в державних спеціалізованих установах і отримати кваліфікацію експерта з певної спеціальності у порядку, передбаченому законом «Про судову експертизу" (у п. 2 ч. 1 ст. 102 КПК вимагається зазначати у висновку експерта свідоцтво про присвоєння кваліфікації експерта, стаж експертної роботи); в) бути атестованими відповідно до їх функцій та у порядку, визначеному наказом Міністерства юстиції України від 09.12.2014 р. № 2083/5 «Про затвердження Положення про Центральну експертно-кваліфікаційну комісію при Міністерстві юстиції України та атестацію судових експертів».

Метою атестації експерта є оцінка професійного рівня фахівців, які залучаються до проведення експертиз або беруть участь у розробках теоретичної та методичної бази експертизи. Залежно від спеціалізації їм присвоюється кваліфікація експерта з правом проведення певного виду експертизи. Відповідно до ст. 9 цього ж закону Міністерство юстиції України веде Реєстр атестованих судових експертів державних і підприємницьких структур та громадян. Органи досудового слідства і суди зобов'язані доручати проведення судових експертиз переважно фахівцям, внесеним до Реєстру.

Протягом часу, що минув з моменту прийняття нового КПК, СБ України, як правоохоронний орган спеціального призначення, так і не ініціювала, а Міністерство юстиції України не організувало виконання вимог, названих у п.п. «б» і «в» попереднього абзацу, через що жоден із державних експертів з питань таємниць досі не набув сукупності нормативних вимог до судових експертів. Тому висновки, дані такими експертами у кримінальних провадженнях, не повною мірою відповідають критеріям допустимості доказів. Через це, згідно з положеннями ст.ст. 86-89 КПК, такі докази можуть бути визнані недопустимим, що призведе до заборони їх використання при прийнятті процесуальних рішень, на них не зможе посилатися суд при ухваленні судових рішень.

Підсумовуючи викладене можна зазначити, що з метою забезпечення виконання визначених ст. 7 КПК таких засад кримінального провадження, як верховенство права і законність, діяль-

ність державних експертів з питань таємниць повинна бути якнайшвидше приведена у відповідність до вимог чинних законодавчих і підзаконних нормативних актів.

Література

1. Кудінов С.С. Актуалізація досліджень проблем криміналістичного забезпечення злочинів у сфері охорони інформації з обмеженим доступом // Досудове розслідування: актуальні проблеми та шляхи їх вирішення : Матеріали постійно діючого наук.-практ. семінару, 17 жовт. 2014 р. – Х. : Право, 2014. – Вип. 6. – С. 55.

2. Експертизи в судочинстві України : наук.-практ. посіб. / за заг. ред. В. Г. Гончаренка, І. В. Гори. – К. : Юрінком Інтер, 2015. – 504 с. – С. 6-7.

3. Кримінальний процесуальний кодекс України. Відомості Верховної Ради України, 2013, № 9-10, № 11-12, № 13, ст. 88 (із змінами станом на 02.07.2015 р.).

УДК 681.3..34

Шлапаченко В. М.

кандидат юридичних наук, старший науковий співробітник

Національна академія СБ України

РОЗВІДУВАЛЬНА ДІЯЛЬНІСТЬ ЯК ОСНОВНА ЗАГРОЗА ЗБЕРЕЖЕННЮ ДЕРЖАВНОЇ ТАЄМНИЦІ

Кожна держава світу має власні інтереси, що обумовлюють її політичну та економічну стратегією і у значній мірі підкріплюються потенціалом збройних сил та поінформованістю спецслужб. Не дивно, що ці інтереси, які прийнято називати національними, не завжди узгоджуються з інтересами інших держав чи іноземних організацій. Шляхи досягнення та конкретні заходи, спрямовані на забезпечення цих національних інтересів, по суті, і складають ту сферу інформації, яка виходячи з її важливості, визнається секретною.

У здобуванні секретів інших держав та захисті власних зацікавлена будь-яка країна, тому це є одним з пріоритетних завдань її спецслужб, що проводять розвідувальну діяльність. Така діяльність передбачає комплекс заходів, які здійснюється ними з використанням спеціальних сил та засобів і спрямовані на отримання важливої (необхідної) для іноземної держави розвідувальної ін-

формації, яку неможливо отримати офіційним шляхом та яка, як правило, становить державну таємницю.

Зауважимо, що відповідно до законодавчого визначення державної таємниці (ст. 1 закону «Про державну таємницю») шкоду національній безпеці може завдати лише її розголошення, хоча при розкритті терміна «охорона державної таємниці» зазначається, що спрямованість цієї діяльності полягає в запобіганні не тільки розголошенню секретної інформації, але і втратам її матеріальних носіїв.

Закон України «Про основи національної безпеки України» (2003 р.) серед загроз національним інтересам і національній безпеці виокремлює вже не лише розголошення державної таємниці, а й розвідувально-підривну діяльність іноземних спецслужб (ст. 7).

Те, що суттєвої шкоди національній безпеці може завдати не тільки розголошення державної таємниці, але і втрата її матеріальних носіїв та розвідувальна діяльність іноземних спецслужб (шпигунство), є, по суті, очевидним, проте в узагальненому вигляді, як перелік загроз збереженню державної таємниці, в жодному із законів України це сьогодні не визначено. Лише Кримінальний кодекс України, що бере під захист найголовніші соціальні цінності, виділяє зазначені дії в окремі склади злочинів. Їх аналіз дозволяє стверджувати, що основною загрозою збереженню відомостей, які становлять державну таємницю, є можливість їх витоку в результаті:

- розголошення особами, яким ці відомості були довірені або стали відомі у зв'язку з виконанням службових обов'язків (статті 328, 422 КК);
- втрати матеріальних носіїв, що їх містять (статті 329, 422 КК);
- розвідувальної діяльності (шпигунства) іноземних спеціальних служб та будь-яких інших неурядових організацій (статті 111, 114 КК).

Якщо розглядати ці загрози як чинники що впливають на стан державної безпеки в інформаційній сфері очевидно, що рівень їх небезпечності є далеко не однаковим.

Зрозуміло, що втрата матеріальних носіїв які містять секретні відомості, та їх розголошення, як різновиди витоку, небезпечні перш за все тим, що важлива інформація, яка назавжди, або на певний час, виходить з під контролю держави, за певних обста-

вин може стати відомою конкурентам (потенційним противникам) України на міжнародній арені – іноземним державам (чи потужним іноземним недержавним організаціям) чи своїм громадянам з кримінального середовища, та бути використана ними на шкоду державній безпеці України.

Сама по собі втрата носія секретної інформації, як матеріальної цінності (так само як його знищення чи спотворення інформації), навряд чи становитиме загрозу державній безпеці, так як у більшості випадків ця інформація має здатність до відновлення, а її носії мають дубльовані екземпляри.

Щодо розголошення секретних відомостей, то своєчасне реагування відповідних державних органів на такі факти, як правило, дозволяє зупинити подальше розповсюдження інформації, максимально локалізувати сферу її обігу, скомпрометувати її достовірність або достовірність джерела поширення та, зрештою, уникнути тяжких наслідків.

На відміну від лише ймовірної можливості потрапляння відомостей, що становлять державну таємницю, до іноземних держав (чи інших небажаних респондентів) в результаті їх розголошення або втрати, розвідувальна діяльність забезпечує вибіркове, планомірне, а за певних умов – систематичне і гарантоване отримання секретної інформації.

Крім того, якщо ефективним застосуванням режимних та профілактичних заходів можна суттєво знизити загрозу витоку згаданих відомостей шляхом втрати та розголошення, то застосування цих заходів як протидії шпигунству дає значно менший ефект і є явно недостатнім.

Відтак, можемо констатувати, що розвідувальна діяльність є найбільш небезпечним видом витоку відомостей, що становлять державну таємницю, і становить найбільшу загрозу їх збереженню.

Таким чином, визначаючи розвідувальну діяльність як основну загрозу збереженню державної таємниці, діяльність по її протидії (тобто контррозвідувальну) слід розглядати як основну у цій сфері, а заходи по охороні державної таємниці, спрямовані на запобігання розголошенню секретної інформації та втрати її матеріальних носіїв – як її складову.

КОНЦЕПТУАЛЬНІ ЗАСАДИ ТА МЕХАНІЗМИ ФУНКЦІОНУВАННЯ НАЦІОНАЛЬНОЇ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ УКРАЇНИ

УДК 340.5 : 004

Баранов О. А.
доктор юридичних наук, с.н.с.
Науково-дослідний інститут інформатики і права
Національної академії правових наук України

ПРАВОВІ КАТЕГОРІЇ КІБЕРБЕЗПЕКИ

В останні 10-15 років широке використання в самих різних сферах життєдіяльності соціуму комп'ютерних і телекомунікаційних технологій, у тому числі інтернет-технологій, разом з великою кількістю переваг створило умови для виникнення чималої кількості загроз. Це призвело до розуміння необхідності вирішення проблеми нейтралізації або мінімізації цієї нової сукупності загроз. З метою формування політики нейтралізації зазначених загроз в різних державах приймають або розробляють стратегії кібербезпеки (США, Німеччина, Франція, Канада та багато інших), яких вже налічується понад 50 [2-5].

Аналіз зазначених стратегій дозволяє констатувати, що на рівні національних та міжнародних стратегічних документів немає ні загальноприйнятого, ні однозначного визначення основних термінів. А це означає, що розрізняються як підходи не тільки до змісту відповідних стратегій, а й до змісту планів дій із забезпечення кібербезпеки. Однак транскордонний характер цієї проблеми настійливо диктує необхідність координації зусиль, як на національному, так і на міжнародному рівні.

У цих умовах актуальною є проблема визначення змісту саме правових категорій кібербезпеки. І цьому є кілька причин. По-перше, класична причина – визначення категорії дозволяє вичерпно окреслити предмет досліджень і дискусій, предмет правового регулювання, правові механізми, коло проблем які можуть бути при цьому зачеплені. По-друге, проблема кібербезпеки в силу

своєї специфіки є глобальною і тому найбільш ефективно може бути вирішена лише за умови об'єднання зусиль самих широких кіл міжнародних гравців, як на державному рівні, так і на рівні приватних корпорацій і асоціацій.

В роботі розглядаються такі засадничі для сфери кібербезпеки терміни як «кібернетичний простір» та «кібернетична безпека» в аспекті їх розуміння в якості правових категорій. Теоретичною та методологічною базою такого розгляду є уявлення кібернетичної безпеки як похідної від більш загального явища - інформаційної безпеки. Проведено порівняльно правовий аналіз інших юридичних термінів та запропоновані варіанти їх визначення.

Література

1. Canada's Cyber Security Strategy: For a stronger and more prosperous Canada [Електронний ресурс]. – Her Majesty the Queen in Right of Canada, 2010. – 14 с. – Режим доступу: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf.

2. Information systems defence and security: France's strategy [Електронний ресурс]. – French Network and Information Security Agency. – 2011. – с. 23. – Режим доступу:. http://www.gouvernement.fr/sites/default/files/fichiers_joints/livre-blanc-sur-la-defense-et-la-securite-nationale_2013.pdf.

3 The national strategy to secure cyberspace [Електронний ресурс]. – Washington, 2003. – 60 с. – Режим доступу: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

4. Cyber Security Strategy for Germany. –Berlin : Federal Ministry of the Interior. – 2011. – 15 с. – Режим доступу: http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile

УДК.681.5

Буяло О. В.

кандидат технічних наук, старший науковий співробітник,
Воєнно-дипломатична академія імені Є. Березняка

МОДЕЛЮВАННЯ ПРОЦЕСУ ОЦІНКИ РІВНЯ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Останніми роками у світі спостерігається стійка тенденція до зростання кількості надзвичайних подій різного походження.

Щотижня світові ЗМІ повідомляють про природні й техногенні катастрофи, збройні конфлікти, терористичні акти, тяжкі злочини, вчинені і злочинними організаціями, і окремими особами, акти піратства на морі тощо. І дедалі частіше в результаті таких надзвичайних подій жертвами стає велика кількість людей, а життєво важливим для існування держав системам, об'єктам і ресурсам завдається серйозна шкода.

З огляду на зазначені тенденції, у більшості провідних країн світу задля систематизації об'єктів, втрата або порушення нормального функціонування яких призведе до значних або навіть непоправних негативних наслідків для національної безпеки, введено термін «критична інфраструктура». До критичної інфраструктури зазвичай належать транспортні й енергетичні мережі, системи міжбанківських розрахунків і телекомунікації, а також об'єкти, необхідні для функціонування органів державної влади, служби реагування на надзвичайні ситуації та екстреної допомоги населенню, системи життєзабезпечення.

Військова агресія Російської Федерації на сході України суттєво змінили безпековий сектор у світі, який створювався протягом десятків років. Це зумовило перегляд провідними країнами світу підходів до питань колективної безпеки, до питання національної безпеки держав, в тому числі і захисту об'єктів критичної інфраструктури (об'єктів критичної інформаційної інфраструктури). Україна, як держава, яка безпосередньо стикнулася з викликами та загрозами гібридної війни, яку проводить Російська Федерація, відчула у повному обсязі недосконаліть підходів та механізмів захисту об'єктів КІ.

Запровадження системного наукового підходу до розв'язання проблеми захищеності об'єктів КІ, звичайно, виходить далеко за межі лише введення відповідного терміна. На першому місці – створення дієвого механізму координації зусиль органів влади, спрямованих на недопущення втрати чи завдання невиправної шкоди вузловим елементам критичної інфраструктури внаслідок дії негативних чинників будь-якого походження: техногенного, природного, соціально-політичного або будь-якої їх комбінації. Було б некоректно стверджувати, що в Україні не приділяється увага захисту важливих об'єктів, систем і ресурсів, які зазвичай належать до критичної інфраструктури. Навпаки, в Україні діє низка законодавчих актів, що визначають особливості

забезпечення захисту вказаної інфраструктури. Проте в державі досі відсутній загальний механізм управління захистом і безпекою названих об'єктів, спостерігаються непоодинокі випадки дублювання функцій і ресурсів, відсутність спільних підходів та узгодженості дій стосовно проблем національного масштабу. До того ж загрози таким об'єктам розглядаються в суто відомчому розрізі.

Усе це підтверджує необхідність упровадження низки суттєвих заходів на державному, регіональному й галузевому рівнях із правового й організаційно-методичного забезпечення, координації та консолідованого забезпечення ресурсами систем безпеки, спільного використання засобів безпеки, що знаходяться в підпорядкуванні окремих відомств. Зважаючи на сприятливі умови, що створюються під час модернізації безпекового сектору в Україні, впровадження науково обґрунтованої концепції захисту об'єктів КІ може стати серйозним внеском у зміцнення національної безпеки держави.

Проведений аналіз показав, що однією із задач забезпечення захисту об'єктів критичної інфраструктури (КІ) є проведення оцінки їх рівня безпеки. З метою вирішення цієї задачі в роботі розроблено математичну модель оцінки рівня безпеки об'єктів КІ.

Для узагальненої оцінки рівня безпеки об'єктів КІ пропонується використовувати комплексний показник інформаційної безпеки об'єкту Q. Підвищення безпеки об'єктів КІ, тобто перехід комплексного показника з одного рівня до наступного, вищого, здійснюється за допомогою вибору та реалізації відповідних організаційних рішень та комплексів програмно-технічних засобів або підвищення їх ефективності.

Математична модель побудована за допомогою марківських процесів. На онові матриці перехідних станів, можливо знайти ймовірність станів $p_1(k), p_2(k),...p_j(k)$ після кожного k- того кроку управлінських дій на комплексний показник Q.

Запропонований підхід дозволяє моделювати стан інформаційної безпеки об'єктів КІ у залежності від тих або інших дій на показники, які характеризують параметри обраного варіанту системи захисту інформації. Для цього достатньо задати збурення (дію) відповідної ймовірності у матриці переходів щоб оцінити наслідки дій, на рівень інформаційної безпеки об'єктів. Під дією обраних програмно-технічних засобів та управлінських рішень

значення показника може або покращитися, стати гіршим, або залишитися без суттєвих змін.

За допомогою запропонованої моделі можливо якісно та кількісно оцінити рівень інформаційної безпеки об'єктів КІ за обраними показниками, обґрунтовувати вимоги до системи захисту об'єктів КІ, а також оперативно приймати рішення щодо підвищення ефективності існуючих систем при зміні вимог до них.

Література

1. Леваков А. Информационная безопасность в США: проблемы и решения. [Електронний ресурс]. – Режим доступу http://freelance4.narod.ru/IS_USA.htm/.

2. Wolthusen, Stephen D., Modeling Critical Infrastructure Requirements, Proceedings of the 2011 IEEE Workshop on Information Assurance and Security, June 2012.

3. Бронштейн Н.Н., Семендяев К.А. Справочник по математике для инженеров и учащихся втузов. – М.: Наука, 1981. – 720 с.

УДК 343.346.8:004

Гавловський В. Д.

кандидат юридичних наук, старший науковий співробітник
Міжвідомчий науково-дослідний центр
з проблем боротьби з організованою злочинністю при
РНБО України

ДО ПИТАННЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ УКРАЇНИ

Величезні можливості сучасних інформаційних мереж, усе більше і більше, використовуються з протиправною, зокрема, злочинною метою. Вочевидь, що через відсутність державних кордонів, кіберпростір перетворився на майже ідеальне місце вчинення злочинів, інформаційні ресурси все частіше використовуються як засіб чи знаряддя злочину.

Виникли нові види злочинів: атаки хакерів на web-ресурси, Інтернет-шахрайства, поширення комп'ютерних вірусів і СПАМів, розповсюдження дитячої порнографії і виникнення кібертероризму. Тривожним симптомом стало те, що намітилося зростання цільових атак проти урядових структур інших держав,

компаній. Так, у 2015 році 29% корпоративних комп'ютерів піддалися атаці при роботі в мережі Інтернет. І цей показник, за прогнозами експертів, буде збільшуватися.

На сьогодні, на жаль, не можливо відобразити повну картину кіберзлочинності. Це пов’язано як з недосконалістю офіційної статистики, так й через високу латентність таких видів злочинів. Як свідчать наукові дослідження вітчизняних та зарубіжних науковців, лише 10-15 відсотків кіберзлочинів стають надбанням гласності. Це пов’язано з низкою причин. Серед них: організації, які постраждали від кіберзлочинів не схильні афішувати наслідки, заподіяні нападами, та недосконалість своїх систем захисту. Вони намагаються приховати напади, вирішуючи проблему власними силами. Не рідко банки просто відшкодовують потерпілим збитки і не заявляють про крадіжку до правоохоронних органів. Також бувають випадки, коли з хакерами домовляються «полюбовно», якщо вкрадена інформація представляє особливу значимість і правопорушник затриманий, але готовий до діалогу.

Характерною рисою кіберзлочинів є надмірно великі розміри нанесених збитків. Так, якщо сукупний збиток від кіберзлочинів по всьому світу за п’ять років, з 1997 р. по 2001 р., становив близько 1 млрд дол. США, то втрати від кібератак в 2015 році склали 158 мільярдів доларів. Тільки в США злочинці викрали 30 млрд доларів. У Росії втрати склали один мільярд доларів[1].

Якщо ж врахувати не тільки прямі збитки, заподіяні кіберзлочинами, але також непрямі, як наприклад, наслідки витоку даних, втрату робочих місць то втрати будуть значно більші.

PandaLabs, антивірусна лабораторія компанії Panda Security, протягом 2015 року виявила і знешкодила понад 84 мільйонів нових зразків шкідливих програм, що на дев'ять мільйонів більше, ніж за 2014 рік. Такий рівень означає, що кожен день протягом 2015 року з'являлося приблизно 230 000 нових зразків шкідливих програм [2].

В Україні, відповідно Єдиному звіту про кримінальні правопорушення, у 2014 році зареєстровано 418 кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку. У 2015 році – 556 кримінальних правопорушень, що на 24,8 % більше. За січень 2016 року обліковано вже 132 кримінальні правопорушення, що становить 23,7 % від минулого цілого року.

За даними МВС України, кількість кримінальних правопорушень, що вчиняються з використанням високих інформаційних технологій (ст.ст. 176, 185, ч. 3,4 ст.190, 200, 229, 231, ч.3,4,5 ст. 301, 361–363-1 КК України)з кожним роком також зростає. Так в 2015 році було зареєстровано 4166 скоєних кримінальних правопорушень, у 2014 році 3862.

Серед найбільш резонансних кібератак в Україні слід відмітити хакерські атаки 23 грудня 2015 року на обленерго в Івано-Франківську, коли через дії хакерів були знеструмлені Івано-Франківськ та частина Прикарпаття.

В січні поточного року фахівці Державної служби спеціального зв'язку та захисту інформації України запобігли можливій хакерській атаці на аеропорт «Бориспіль», виявивши одну з робочих станцій в аеропорту інфіковану вірусом "Блек Енерджі".

В Україні, за даними компанії служби безпеки України, кожна 5 кампанія зазнавала збитків від кібератак, а більше 70% компаній малого і середнього бізнесу в Україні не захищені від кібер-атак або захищені слабо.

Слід відмітити, що досвідчені хакери, які викрадають інформацію з баз даних великих компаній або грошові кошти з рахунків, використовують схеми, які кожен раз перекроюють до невпізнання, а так як фахівців в таких розслідуваннях вкрай мало, довести вину не завжди можливо. До того ж вирок багато в чому залежить від компетентності суддів. Справи, пов'язані з кіберзлочинами, складають вкрай малу частку від загального обсягу судової практики, тому для багатьох суддів залишаються «екзотикою». В Україні в 2015 році судами першої інстанції із 71 кримінального провадження було розглянуто 45, що становить 63%.

Фахівці впевнені в тому, що в майбутньому втрати від дій кіберзлочинців будуть лише збільшуватися. Також будуть збільшуватися й доходи від злочинної діяльності в мережі Інтернеті, які, за даними The Guardian, оцінюється в $ 388 мільярдів щорічно, тоді, як дохід від наркобізнесу оцінюється в $ 288 млрд.

Глава комітету з питань внутрішніх справ британської Палати, Кіт Ваз зазначив «Ми не виграємо війну проти кримінальної онлайн-активності. Ми занадто спокійно ставимося до інтернет-війн, тому що їх жертви заховані у віртуальному просторі. Загроза атаки хакерів в Великобританії серйозніше, ніж ядерний удар». На його думку, держава не до кінця розуміє рівень кіберзагрози, а покарання за такі злочини не є достатніми [3].

Все більше фахівців, з метою протидії кіберзлочинності, вважає, що в першу чергу необхідно посилити кримінальну відповідальність за ці злочини.

В Україні також ведуться пошуки шляхів підвищення ефективності боротьби з кіберзлочинністю в різних напрямах. Одним з них є вдосконалення правового регулювання протидії даним суспільно небезпечним діянням.

Чи не головною проблемою сучасного правового регулювання досліджуваного виду кримінальних правопорушень є те, що санкції відповідних статей КК України передбачають максимальне покарання у вигляді позбавлення волі на строк не більше п'яти років (за винятком ч. 2 ст. 361 та ч.2 ст. 362), що не дозволяє віднести їх до категорії тяжких. Це, у свою чергу, унеможливлює проведення оперативними підрозділами оперативно-розшукових заходів з метою виявлення та припинення злочинів, що вчиняються у сфері використання комп'ютерних технологій. Адже оперативно-розшукова діяльність може здійснюватися лише з метою виявлення та припинення тяжких та особливо тяжких злочинів. Крім того, ні слідчий, який проводить досудове розслідування даної категорії злочинів, ні прокурор, який є процесуальним керівником такого розслідування, не можуть надати оперативним підрозділам доручення на проведення негласних слідчих (розшукових) дій в межах відповідного кримінального провадження. Адже ст. 246 КПК передбачає, що негласні слідчі (розшукові) дій можуть бути проведені лише у межах провадження щодо тяжких та особливо тяжких злочинів.

З нашого погляду, існує два шляхи виходу з цього становища. Перший полягає у тому, аби, враховуючи значну суспільну небезпеку вказаної категорії злочинів, внести зміни до КК України, збільшивши у санкціях відповідних статей термін покарання таким чином аби їх можна було віднести до категорії тяжких та особливо тяжких. Другий – внести зміни до Закону України «Про оперативно-розшукову діяльність», зазначивши, що така діяльність може проводитися з метою попередження, виявлення і припинення тяжких, особливо тяжких та окремих, визначених цим законом злочинів. Далі потрібно подати перелік злочинів, виявлення та припинення яких може здійснюватися методами ОРД. До цього переліку можуть увійти не лише злочини, що вчиняються у сфері використання електронно-обчислювальних машин

(комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, а й інші кримінально карані діяння, суспільна небезпека яких зумовлює необхідність застосування оперативно-розшукових заходів. Відповідні зміни потрібно внести і до ст. 246 КПК України.

Література

1. Мировые потери от кибератак в 2015 году составили $158 млрд млрд / [Электронный ресурс]. – Режим доступа:
http://seansi-zdorovja.ru/post/586/mirovyye-poteri-ot-kiberatak-v-2015-godu-sostavili-158-mlrd.html

2. 84 миллиона новых образцов вредоносных программ, на 9 миллионов больше, чем в 2014 году / [Электронный ресурс]. – Режим доступа:
http://www.tadviser.ru/index.php

3. Киберпреступность наносит больше ущерба, чем наркоторговля / [Электронный ресурс]. – Режим доступа:
http://www.securitylab.ru/news/442691.php

УДК 004.056.53

Даник Ю. Г.
доктор технічних наук, професор
Житомирський військовий інститут імені С. П. Корольова

ОРГАНІЗАЦІЙНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ КІБЕРОБОРОНИ ДЕРЖАВИ. ОСНОВНІ НАПРЯМИ

На сьогоднішній день в сучасних конфліктах бойові та інші (економічні, політичні, енергетичні, інформаційні та кібернетичні) дії є взаємоузгодженими за цілями і задачами, комплексне ведення яких дозволяє реалізувати асиметричні підходи з синергетичним результатом (ефектом). В сучасній класифікації війн такі конфлікти отримали назву "гибрідні". "Гібридну" війну в загальних рисах можна визначити як сукупність заздалегідь підготовлених та оперативно реалізованих дій військового, дипломатичного, економічного характерів, спрямованих на досягнення стратегічних цілей. Ведення дій у кіберпросторі суттєвим чином впливає на стратегію, оперативне мистецтво, тактику а також форми та способи застосування сил і засобів оборонного сектору держави в інтересах забезпечення воєнної безпеки держави.

З метою підвищення обороноздатності та забезпечення національних інтересів у кіберпросторі збройні сили (ЗС) розвинених держав світу проводять комплекс організаційних та технічних заходів, спрямованих на оперативне адекватне реагування на виклики та загрози, які пов'язанні з появою новітніх розробок та інтенсивним розвитком апаратних та програмних засобів кібернетичної зброї. Відповідно до цього розвитку трансформуються і системи кібернетичної безпеки. До організаційних заходів відноситься: формування системи забезпечення кібербезпеки, створення кіберкомандування та кібервійськ; створення системи підготовки висококваліфікованих фахівців у сфері кібербезпеки; організаційне, законодавче та технічне забезпечення дій кіберпідрозділів; наукове супроводження, розроблення та впровадження новітніх технологічних розробок. З точки зору технічних заходів проводяться кібернавчаня, дослідження відповідними лабораторіями вірусології з розробки нових видів наступальної, оборонної та розвідувальної кіберзброї з врахуванням соціотехнічної складової тощо. Для проведення кібернавчань використовуються різноманітні кіберполігони, які дозволяють відпрацьовувати практичні навички з реагування на різні виклики і загрози в кіберпросторі. Але потребують створення інтегровані кіберполігони, які будуть охоплювати в повному обсязі технічну і соціотехнічну сфери.

Станом на кінець 2015 року згідно з офіційними заявами військові кібернетичні компоненти вже створені та повноцінно функціонують у США (U.S. Cyber Command); Великобританії (Cyber Security Operations Centre); ФРН (Internet Crime Unit та Federal Office for Information Security); Австралії (The Cyber 9 security operations centre); Естонії (Таллінський кіберцентр НАТО); Індії; Ізраїлі та багатьох інших країнах. Зокрема з 2013 року в ЗС РФ розпочав роботу спеціальний підрозділ з кібербезпеки на який, крім визначених питань, покладено завдання організації взаємодії з військами інформаційних операцій.

Досвід ведення антитерористичної операції в Донецькій та Луганській областях, а особливо підготовчий етап організації сепаратистського руху, доводить, що наявність таких спецпідрозділів дозволяє мати певну перевагу. Ці підрозділи залучаються для виконання розвідувальних та наступальних дій шляхом здійснення у явному чи прихованому вигляді інформаційних та кібернетичних операцій в українському сегменті кіберпростору.

Зазначене породжує низку новітніх загроз національним інтересам України у сфері оборони, що зумовлює нагальну потребу коригування державної воєнної політики у галузі інформаційної та кібернетичної безпеки. Тому необхідна дієва "дорожня карта", яка регламентує проведення комплексу організаційних та технічних заходів із забезпечення кібероборони держави.

До першочергових організаційних заходів мають бути віднесені такі, як:

- упорядкування нормативно-правової бази з питань забезпечення кібернетичної безпеки держави та її гармонізація з міжнародним законодавством. На даний час в Україні прийнято та діє низка нормативних документів, пов'язаних із забезпеченням кібербезпеки держави, але ряд стратегічних документів не затверджено (наприклад Закон України "Про основні засади забезпечення кібербезпеки України");

- створення державної міжвідомчої координаційної структури та кібернетичного командування в її складі. Її відсутність стримує формування національної системи забезпечення кібернетичної безпеки. Як наслідок, не налагоджена міжвідомча взаємодія, централізоване управління та чіткий розподіл обов'язків і повноважень між наявними кіберпідрозділами різних відомств проводить до неефективних дій щодо захисту кіберпростору держави;

- організація системи підготовки, ефективного розподілу, науково-методичного та кадрового забезпечення відомств висококваліфікованими фахівцями з кібернетичної безпеки.

- Технічні заходи пов'язані з розгортанням науково-промислового потенціалу для задоволення потреб кібероборони за єдиним задумом і планом.

Створення національної системи кібербезпеки держави з технічної точки зору потребує наявності відповідного кібернетичного полігону для відпрацювання технологій виявлення кібератак та протидії ним, ліквідації наслідків застосування кіберзброї та відновлення нормальних режимів функціонування мереж управління військами та зброєю, розробки в лабораторіях вірусології навчальних та бойових програмних агентів. Структурно він повинен включати в себе підсистеми кібернетичної розвідки і аналізу, кібернетичного впливу, кібернетичного захисту та навчального об'єкту тестування у вигляді автоматизованої системи управління а також інші засоби, які працюють у кіберпросторі, такі як: технічні засоби розвідки, діючи макети систем управління військами і зброєю тощо.

Цільове застосування засобів кібернетичного полігону дозволить проводити практичну підготовку висококваліфікованих фахівців спеціалізованих підрозділів у галузі інформаційної та кібернетичної безпеки держави, моделювання кібератак на навчальні об'єкти з критичною інфраструктурою, виявлення вразливих місць систем захисту локальних мереж, відтворення комп'ютерних мереж військового призначення з метою перевірки рівня їх захищеності тощо. В подальшому при повноцінному розгортанні кіберполігону та набуття досвіду фахівцями з кібербезпеки з'явиться можливість створення потужного кіберцентру і залучення цієї структури до цілодобового оперативного чергування в національній системі забезпечення кібернетичної безпеки України.

Таким чином, реалізація зазначених організаційних та технічних заходів дозволить в найкоротші терміни створити дієву систему кібероборони та забезпечення кібербезпеки держави.

Література

1. Даник Ю. Г. Особливості формування системи кібернетичної безпеки України в контексті розвитку систем кібернетичної безпеки провідних країн світу / Ю. Г. Даник, Ю. М. Супрунов // Труди університету : зб. наук. праць. – К. : НУОУ, 2011. – № 7 (106). – С. 5–21.

2. Даник Ю. Г. Деякі підходи до формування системи підготовки кадрів для системи кібернетичної безпеки України / Ю. Г. Даник, Ю. М. Супрунов // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем: зб. наук. праць. – Житомир : ЖВІ НАУ, 2011. – Вип. 5 – С. 5–22.

3. Даник Ю. Г. Особливості забезпечення національної безпеки у високотехнологічному суспільстві. [Електронний ресурс] / Ю. Г. Даник, О. О. Труш. – Режим доступу до статті: http://ifs.kbuapa.kharkov.ua/e–book/db/2010–1 /doc/5/02 .pdf.

4. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. – К.: ДУТ, 2015.– 288 с.

5. Даник Ю. Г. Національна безпека: запобігання критичним ситуаціям : монографія / Ю. Г. Даник, Ю. І. Катков, М. Ф. Пічугін. – К. : МО України ; Житомир : Рута, 2006. – 388 с.

УДК 351.746.1+004.9: 340.13(043.2)

Довгань О. Д.
кандидат юридичних наук, старший науковий співробітник
Науково-дослідний інститут інформатики і права
Національної академії правових наук України

СТВОРЕННЯ СИСТЕМИ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ УКРАЇНИ: ПРАВОВІ КОЛІЗІЇ

Надійна робота мереж передачі даних і обчислюваних сервісів завжди були запорукою суспільного добробуту та економічної стабільності. На функціонування ключових інформаційних систем загального користування впливають багато факторів: Інтернет-атаки; порушення, викликані фізичним впливом; вихід з ладу програмного та апаратного забезпечення; людські помилки тощо. Перераховані явища наочно демонструють, наскільки сучасне суспільство залежить від стабільної роботи інформаційних систем.

Тому, забезпечення цілісності, достовірності та конфіденційності інформації в кіберпросторі стало однією з найважливіших проблем XXI-го століття. Саме тому захист кіберпростору стає головним завданням держави, економіки та суспільства, як на державному, так і на міжнародному рівні.

Кібербезпека все частіше розглядається як стратегічна проблема державного рівня, зачіпає всі верстви суспільства. Державна політика кібербезпеки повинна служити засобом посилення безпеки та надійності інформаційних систем держави.

Реальна ситуація, що склалася у сфері кібербезпеки України є такою: кібернетичні атаки на інформаційні ресурси держави стали невід'ємним компонентом гібридної війни, що її розв'язала Росія. Починаючи з середини 2013 року російські безпекові органи проводять масштабну кібероперацію «Армагедон», метою якої є отримання даних про плани та оцінки українських органів державної влади щодо розвитку конфлікту на Сході України та дій владних структур у зв'язку з цим [1].

На сьогодні є ціла низка законів України та інших нормативних документів різних рівнів які загалом охоплюють проблеми забезпечення кібербезпеки держави: Закони України «Про інформацію»; «Про основи національної безпеки України»; «Про Державну службу спеціального зв'язку та захисту інформації

України»; «Про державну таємницю»; «Про захист інформації в інформаційно-телекомунікаційних системах» та інші. Але зазначена нормативно-правова база не охоплює всі основні елементи, необхідні для ефективної протидії кіберзлочинам усіх рівнів складності. Однією з важливих проблем у цій сфері є вже неодноразово вказана термінологічна невизначеність.

Так, у Законі України «Про боротьбу з тероризмом» поняття комп'ютерний тероризм не згадується зовсім, а причетні до нього елементи прописані виключно як складники технологічного тероризму. Закон України «Про основи національної безпеки України» згадує про комп'ютерну злочинність і комп'ютерний тероризм, причому жоден із цих термінів не отримав визначення ані в цьому, ані в інших нормативних документах. У Доктрині інформаційної безпеки України (втратила силу на підставі Указу Президента України від 6 червня 2014 року № 504/2014) також згадувались комп'ютерна злочинність та комп'ютерний тероризм, але без жодних пояснень чи посилань (відсилань) до таких пояснень. Також мова йшла про кібератаки, але без спроб визначення даного поняття.

Тому, неунормованість понятійно-категоріального апарату, відсутність правового визначення зон відповідальності відомств, залучених до сфери забезпечення кібербезпеки, слабке координування їх діяльності щодо реагування та попередження кіберзлочинів, брак правового закріплення взаємовідносин урядових безпекових структур із бізнесом та ін. на тлі зростання кількості й масштабності (зокрема за наслідками) кіберзагроз вимагало створення комплексного нормативно-правового документа, що забезпечуватиме безпеку в кіберсфері. Таке рішення було прийнято (Указ Президента України від 10 грудня 2010 року № 1119/2010 «Про Рішення Ради національної безпеки і оборони України від 17 листопада 2010 року «Про виклики та загрози національній безпеці України у 2011 році»). Ним пропонувалося у 2-х місячний термін подати на розгляд Ради національної безпеки і оборони України пропозиції щодо створення єдиної загальнодержавної системи протидії кіберзлочинності та розробити і затвердити перелік об'єктів, що мають важливе значення для забезпечення національної безпеки і оборони України та потребують першочергового захисту від кібернетичних атак. Узагальнюючим документом мав стати Закон України «Про кібернетичну безпеку Украї-

ни», покликаний: зафіксувати основні терміни у сфері кібербезпеки; визначити поняття об'єкт критичної інфраструктури та механізм захисту об'єктів критичної інфраструктури; визначити принцип побудови Єдиної загальнодержавної системи протидії кібернетичним загрозам та її складових елементів; вирішити проблеми міжвідомчого координування та повноваження суб'єктів забезпечення кібернетичної безпеки держави. Було створено біля чотирьох варіантів проекту закону, але жодний на жаль не пройшов заключного обговорення та винесення на розгляд Верховної Ради України.

Крім закону, предметом якого має стати саме система кібернетичної безпеки, починаючи з 2012 року відповідно до міжнародних практик розроблялася і Стратегія забезпечення кібербезпеки України, яка мала чи має визначити ключові засади забезпечення кібербезпеки, пріоритети та основні етапи розвитку кібербезпекового сектору. Такий проект був створений фахівцями Національного інституту стратегічних досліджень. Ситуація з прийняттям аналогічна.

На сьогодні єдиним чинним стратегічним документом в межах даної проблематики є Стратегія національної безпеки України [2]. Вона визначила як основні загрози інформаційній безпеці: ведення інформаційної війни проти України; відсутність цілісної комунікативної політики держави, недостатній рівень медіакультури суспільства; кібербезпеці і безпеці інформаційних ресурсів: уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак; фізична і моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом; безпеці критичної інфраструктури: критична зношеність основних фондів об'єктів інфраструктури України та недостатній рівень їх фізичного захисту; недостатній рівень захищеності критичної інфраструктури від терористичних посягань і диверсій; неефективне управління безпекою критичної інфраструктури і систем життєзабезпечення. Пріоритетами забезпечення кібербезпеки і безпеки інформаційних ресурсів Стратегією визначено: розвиток інформаційної інфраструктури держави; створення системи забезпечення кібербезпеки, розвиток мережі реагування на комп'ютерні надзвичайні події (CERT); моніторинг кіберпростору з метою своєчасного виявлення, запобігання кіберзагрозам і їх нейтралізації; розвиток спроможностей правоохоронних органів щодо розслідування кіберзлочинів; забезпечення

захищеності об'єктів критичної інфраструктури, державних інформаційних ресурсів від кібератак, відмова від програмного забезпечення, зокрема антивірусного, розробленого у Російській Федерації; реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом, захист державних інформаційних ресурсів, систем електронного врядування, технічного і криптографічного захисту інформації з урахуванням практики держав - членів НАТО та ЄС; створення системи підготовки кадрів у сфері кібербезпеки для потреб органів сектору безпеки і оборони; розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, інтенсифікація співпраці України та НАТО, зокрема в межах Трастового фонду НАТО для посилення спроможностей України у сфері кібербезпеки.

Почалися відбуватися деякі зрушення з боку держави і робляться спроби створення повноцінної системи національної кібербезпеки. Про що свідчить і Указ Президента України № 449/2014 від 1 червня 2014 року [3] , яким уведено в дію рішення Ради національної безпеки і оборони України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України». Вказаним документом передбачено вдосконалення нормативно-правового забезпечення та попередження й нейтралізації потенційних і реальних загроз національній безпеці в інформаційній сфері, зокрема, розробити і внести на розгляд Верховної Ради України: законопроекти про внесення змін до деяких законів України («Про основи національної безпеки України», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про Службу безпеки України», «Про Державну службу спеціального зв'язку та захисту інформації України»), щодо приведення національного законодавства у відповідність із міжнародними стандартами з питань інформаційної та кібернетичної безпеки, вдосконалення системи формування та реалізації державної політики у сфері інформаційної безпеки України; проект Закону України про кібернетичну безпеку України; проект Стратегії кібернетичної безпеки України та ін.

Останні мають задати загальну логіку не лише подальшої нормотворчої діяльності, а й сутнісно сформулювати бачення Україною нових геополітичних умов існування держави, передусім щодо її ролі в глобальному та національному кіберпросторах.

Література:

1. «Питання створення «Огляду сектору кібербезпеки України»». Аналітична записка [Електронний ресурс]. − Режим доступу: http://www.niss.gov.ua/articles/1911/.

2. Стратегія національної безпеки України, затверджена Указом Президента України від 26 травня 2015 року № 287/2015 // Офіційне інтернет-представництво Президента України [Електронний ресурс]. − Режим доступу: http: //www.president.gov.ua.

3. Указ Президента України № 449/2014 від 1 червня 2014 року «Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України»» : http://www.president.gov.ua/documents/4492014-17157.

УДК 005.3

Заєць П. М.
Національна Академія СБ України

ГОТОВНІСТЬ УКРАЇНИ ДО ВИКЛИКІВ КІБЕРТЕРОРИЗМУ

В останнє десятиліття поняття кібертероризму стрімко вийшло за межі уяви фантастів, гіпертрофованих вправ на журналістському терені діячів від мас-медіа, та ін. Це питання ґрунтовно обговорюється на урядовому, науковому, побутовому та ін. рівнях. Загроза кібератак стала достатньо реальною, а її ризики оцінюються як достатньо високі, реалії їх входження в повсякденну дійсність стали питанням часу та місця. Використання мережевого інструментарію здатне вивести з ладу критичні компоненти національної інфраструктури (енергетичні потужності держави, зв’язок, транспортні, фінансові та інші засоби) задля примусу чи усунення уряду, цивільного населення невпинно стає реальною і зростаючою загрозою. Реальна оцінка відповідного ризику передбачає необхідність визначення успішного здійснення кібератаки та розміру можливих збитків. У цьому зв’язку доцільним є також врахування "людського фактору" та "інсайдерської інформації". Слід мати на увазі наявність методів аналізу та управління ризиками і захистом інформації, які дають змогу адекватного оцінювання такого

перебігу подій, включно з кібертероризмом, проте фахівців, що володіють відповідними методами достатньо мало, як і тих, хто здатний застосувати ці методи в дії, на практиці. Нагальним стає постановка і рішення задач з аналізу і управління ризиками для адекватної оцінки реальності проявів кібертероризму, та підготовки фахівців у цій галузі.

Сучасні світові та українські реалії свідчать про те, що кібератаки можуть мати серозні наслідки. Як для України, крупні енергетичні об'єкти та водне обладнання з технологічної точки зору управляють своїми ресурсами використовують недосконалі в цьому відношенні засоби контролю та збору даних. Ці засоби вразливі до кібератак. Загрози кібертероризму існують для інших об'єктів національної інфраструктури.

Інформація про те, що грудневе "падіння" енергосистеми у кількох західноукраїнських областях було справою рук російських хакерів, не стала цілковитою несподіванкою.

Гіпотеза про те, що енергосистему Прикарпаття буцімто "ламали" за допомогою вірусу BlackEnergy, який ще в 2013 році використовувався для проникнення в системи НАТО і європейських урядів, була озвучена у The Washington Post ще на початку січня.

Але одна річ – здогади і витоки в пресі, а інша – посилання на офіційну заяву заступника міністра енергетики США Елізабет Шервуд-Рендал на зустрічі з представниками енергетичної галузі США. Яку вона зробила, посилаючись на результати розслідування, проведеного ФБР та Департаментом енергетики США – під наглядом Держдепу. Подібна увага до зламу української енергосистеми була викликана тим, що на думку експертів, і енергосистема США є вразливою до хакерських атак.

За даними слідства, щоправда, українську енергосистему руйнував не BlackEnergy, а щось інше, але за подією стоїть, ймовірно, те саме хакерське угруповання Sandworm, яке відзначилось і в попередньому випадку. Втім, подробиці не так важливі.

Ключовий висновок, який можна зробити з цієї події наступний – Росія розпочала кібератаки проти цивільного населення України. І, атакувавши один раз, цілком може повторити недружні дії. Бо хакерські атаки – це практично

ідеальний прийом ведення "гібридної війни", за допомогою якого можна завдати помітної шкоди противнику, залишаючись при тому поза зоною ймовірної відповідальності. Від дій хакерів держава завжди може відмежуватись, почати "розслідування їхньої діяльності", та що там – навіть знайти пару-трійку "членів Правого сектору", які, не особливо володіючи комп'ютером, вчинили масштабну хакерську атаку з російської території, щоб "підірвати добросусідські відносини".

Міністерство енергетики за результатами дослідження грудневої атаки прийшло до думки, що за нею стоять російські хакери. Такий же висновок висловила Елізабет Шервуд-Рендалл, заступник міністра енергетики США.

Атаки не були занадто складними технологічно, але радіти не варто. Хакери-професіонали використовують рівно той рівень технологій, який необхідний для досягнення мети. «Адже немає сенсу купувати Ferrari, щоб возити дітей в школу», - каже в розмові з НВ експерт центру кібербезпеки НАТО Кеннет Гірс

Але трьома обленерго – Київобленерго, Прикарпаттяобленерго і Чернівціобленерго – справа не закінчилася. Ще раніше були атаковані телеканали 1+1 та СТБ, потім – аеропорт Бориспіль і кілька енергокомпаній. Після цього послідувала атака на Укрзалізницю. Виробник рішень у сфері інформаційної безпеки Trend Micro, чий центральний офіс знаходиться в Токіо, заявив про ще одну атаку на велику українську видобувну компанію, не називаючи її імені. Жертви кібератак вкрай неохоче говорять про ці факти, бажаючи всіляко їх приховати.

По-перше, для протидії кіберзагрозам потрібен певний координуючий орган. Звичайно, бюрократія – це зло, але розмитість цього завдання між СБУ, МВС, Держслужбою спеціального зв'язку призводить до того, що винних у подібних проколах знайти, як правило неможливо. Себто коли потрібно освоювати кошти на нові системи захисту інформації – зацікавлених відомств є багато, а коли комусь треба відповісти за росіян, які потрошку керують нашою енергосистемою – винних немає.

По-друге, зважаючи на те, що далеко не кожну хакерську атаку можна вчасно зупинити, критичні об'єкти української інфраструктури мають бути не тільки забезпечені резервними

джерелами живлення (якими вони ніби й так забезпечені – але тільки теоретично) але й повинні мати план по відключенню від глобальних інформаційних систем в разі виникнення подібної ситуації – там, де це можливо. А також мінімальний досвід в реалізації подібних дій. Не хотілось би, звичайно, повторювати досвід радянської системи цивільної оборони – з її нічними сиренами і мистецтвом ховатись від ядерного вибуху в "обладнаних протиатомних щілинах", але мінімальне тренування для диспетчерів і чергових у критичних сферах інфраструктури не завадить.

В будь-якому разі, з початком подібних кібертерористичних атак, які рано чи пізно може повторити не тільки Кремль, але й менш організовані злочинці, наш світ стає ще трохи менш безпечним місцем. До чого варто підготуватись.

В умовах «гібридної» війни для нашої держави важливим та необхідним залишається розробка й схвалення національної стратегії забезпечення кібербезпеки, створення захищеного національного сегменту кіберпростору; побудова ефективної та оперативної протидії будь-яким мережевим кібератакам, запобігання втручанню у внутрішні справи України і нейтралізація посягань на її інформаційні ресурси з боку інших держав, особливо РФ; посилення обороноздатності держави у кіберпросторі; зниження рівня уразливості об'єктів кіберзахисту; забезпечення повноправної участі України в загальноєвропейській та регіональних системах забезпечення кібербезпеки за участі НАТО; приєднання до міжнародної системи боротьби з кіберзлочинністю та кібертероризмом, забезпечення ефективної міжнародної співпраці у сфері забезпечення кібербезпеки.

Як результат слід наголосити, що фахова підготовка фахівців з кібербезпеки та керівного складу органів державного управління з цих питань для потреб як силових структур, так і виробничої та банківської сфери має проводитись у єдиній системі освіти України, а спеціальна підготовка офіцерського складу СБ України з питань інформаційної і кібербезпеки має проводитись на курсах підвищення кваліфікації.

УДК 004.652

Зайцев О. В.
кандидат технічних наук, доцент
Воєнно-дипломатична академія імені Є. Березняка
Новохатній Ю. В.
Воєнно-дипломатична академія імені Є. Березняка

СЕМАНТИЧНА ІНТЕГРАЦІЯ ІНФОРМАЦІЇ З ВІДКРИТИХ ДЖЕРЕЛ ІНТЕРНЕТ В ЗАДАЧАХ ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

У зв’язку з ймовірністю російської інформаційної агресії проти України, інформаційні підрозділи мають максимально ефективно використовувати наявні ресурси для забезпечення кібернетичної безпеки України. Одним з відкритих джерел інформації про РФ у визначених законодавством України сферах та напрямах інформаційної діяльності (ІД) для забезпечення кібернетичної безпеки є глобальна комп’ютерна мережа Інтернет. У ході використання інформаційного поля (ІП) Інтернет збільшуються обсяги інформації, що призводить до зниження загального рівня інформованості, багаторазово ускладнюється аналітична діяльність підрозділів [1, 2].

Аналіз інформаційного наповнення сучасних комп'ютерних систем, узагальнення динамічних інформаційних масивів надвеликих потоків інформації, що безперервно з'являються в глобальному мережевому середовищі, потребує нових підходів, які б забезпечували виявлення найбільш важливих фрагментів в інформаційних потоках, орієнтацію на конкретних споживачів або на цільові групи. Різнорідність завдань і постійно зростаючі обсяги інформації з відкритих джерел спричиняють подальші дослідження для забезпечення комплексної обробки та аналізу інформації. Проблема інтеграції даних полягає в такому логічному об'єднанні інформації, що належить різнорідним джерелам, яке б забезпечувало єдиний простір для оперування інформацією.

Головними завданнями інтеграції інформації є формування повного і несуперечного набору на основі множини різнорідних вхідних даних, отриманих з різних джерел. Семантична складова процесу інтеграції є однією з найважливіших та найскладніших, оскільки проблеми синтаксису та структури загалом вирішують на технічному та технологічному рівні. Семантичну інтеграцію можна реалізувати різними засобами, такими, як тезауруси, словники даних, семантичний аналіз даних, онтології [3, 4].

Сьогодні інформацію можна отримати з відкритих джерел, реклами, фірмових, банківських, урядових звітів, баз даних, від експертів шляхом аналізу або спеціальної обробки даних, текстів. Велику цінність мають доступні бази даних органів державної влади: бази даних державних і статистичних органів, торгово-промислових палат, органів приватизації тощо. Останнім часом поширюються бази даних на основі архівів ЗМІ та мас-медіа. Багатовимірне ІП Інтернет можна умовно розділити на веб-простір, "глибинний веб", бази даних та соціальні медіа [1, 2].

На цей час розвиток методів і засобів адаптивного агрегування та узагальнення потоків інформації з глобальних комп'ютерних мереж для підтримки інформаційної діяльності в різних прикладних сферах є досить актуальною проблемою. Процеси адаптивного агрегування та узагальнення потоків інформації передбачають розв'язання таких проблем, як інтеграція значень, інтеграція синтаксису, інтеграція структури, семантики даних. Проблеми інтеграції на рівні синтаксису та структури великою мірою досліджено, і для їх вирішення розроблено низку методів та засобів. Проблема інтеграції семантики – це відсутність єдиного підходу та інструментарію для її практичної реалізації. Пропонується використовувати комбінований підхід до вирішення завдань формування та аналізу критеріїв інтеграції різнорідних наборів даних, а саме: на основі метаданих, на основі контекстуального аналізу та на основі онтологій.

Для семантичної інтеграції на основі метаданих пропонується комплексно використовувати як схему Захмана так і метод дублінського ядра. Відповідно схеми Захмана, для визначення категорій метаданих (критеріїв семантичної інтеграції) та порядку визначення їх збігу, використовуються знання експертів. За неможливості використати знання експертів застосовують методи на основі дублінського ядра. Його застосовують для формалізації та уніфікації даних, що підлягають інтеграції, зокрема їх семантичного наповнення. Особливістю цього варіанту є те, що поняття збігу значень не завжди може бути виконано без участі експерта. Для цього необхідно сформувати спеціальні таблиці відповідності значень метаданих, які дають змогу робити висновки про відповідність змісту окремих елементів дублінського ядра.

Метод контекстуальної семантичної інтеграції використовується у разі інтегрування як структурованих (реляційних) даних, так і слабкоструктурованих – поданих у довільних форматах. Метод ґрунтується на змістовому порівнянні інформаційного напов-

нення наборів даних. Метод контекстуального аналізу дає змогу перевірити критерії семантичної інтеграції на формальному рівні і не потребує безпосередньої участі експерта. Особливістю цього методу є необхідність формування тезаурусу для набору даних, який містить певний інформаційний ресурс. Через неоднорідність форматів та структур даних, що підлягають інтеграції, створення наборів ключових термінів може бути досить трудомістким та залежати від конкретних умов використання.

Метод інтеграції на основі онтологій передбачає використання тезаурусу та метаданих, але є більш загальнішим за них та враховує більше аспектів семантики даних. Критерії семантичної інтеграції у цьому випадку можна сформулювати як послідовність вимог до елементів двох онтологій даних. Перевірити критерії семантичної інтеграції даних можна як на формальному, так і на експертному рівні.

Для застосування онтологій під час опису розподілених у просторі інформаційних ресурсів можна використати підходи на основі єдиної онтології та на основі множин онтологій. Перевагою першого підходу є однотипність визначення та інтерпретації концептів всіх вхідних наборах даних, однозначності в даних. Проблемою такого підходу є складність формування єдиної глобальної онтології. Перевагою другого підходу є відносна автономність засобів опису семантики кожного вхідного набору та відсутність потреби переходу від специфічних способів концептуалізації даних до уніфікованих. Однак застосування множини розподілених в просторі онтологій породжує проблеми узгодженого застосування локальних онтологій.

Тому під час описання розподілених у просторі інформаційних ресурсів пропонується використовувати гібридний підхід, комбінуючи при цьому спільні та окремі онтології. Семантику інформаційного ресурсу, що підлягає інтеграції, описує окрема онтологія, але для сумісності локальних онтологій створюють глобальні розподілені словникові ресурси.

Література

1. Додонов А.Г. Конкурентная разведка в компьютерных сетях / А.Г. Додонов, Д.В. Ландэ, В.В. Прищепа, В.Г. Путятин – К.: ИПРИ НАН Украины, 2013. – 250 с.

2. Додонов А.Г. Компьютерные сети и аналитические исследования / А.Г. Додонов, Д.В. Ландэ, В.Г. Путятин. – К.: ИПРИ НАН Украины, 2014. – 486 с.

3. Берко А.Ю. Методи інтеграції синтаксису різнорідних даних у системах електронного контент-бізнесу / А.Ю. Берко // Інформаційні системи та мережі: Вісник Національного університету Львівська політехніка. – 2008. – № 621. – С. 19–28.

4. Wache H. Ontology-Based Integration of Information – A Survey of Existing Approaches / H. Wache, T. Vogele, U. Visser, H. Stuckenschmidt // Proceedings of the IJCAI-01 Workshop on Ontologies and Information Sharing, Seattle, USA, August 4–5. – 2001. – P.108-118.

УДК 004.056

Ковальова Ю. В.
Державний вищий навчальний заклад
“Національний гірничий університет”

ПРОБЛЕМИ В СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ОБ’ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Стрімкий розвиток інформаційного простору та глобальна інтеграція «хмарної» інфраструктури (cloud computing) і «програмного забезпечення як сервісу» (SaaS) викликали збільшення випадків порушення властивостей інформації в кібернетичному просторі. При цьому, незважаючи на динамічний розвиток сектору кібербезпеки дедалі більш чітко окреслюються проблеми забезпечення безпеки інформації в кібернетичному просторі технологічних об’єктів стратегічного призначення.

Зазначене підтверджують події, що відбулися за останні роки в кіберпросторі України та стали однією з важливих складових гібридної війни. Зокрема, в 2015 році Україна посіла перше місце в Європі за ризиками зіткнення з кіберзагрозами [1], а українці стали жертвами таких кампаній, як CosmicDuke, MiniDuke, Agent.btz, Epic Turla, TeamSpy, BlackEnergy і Red October [2]. В результаті реалізації потужної кібернетичної атаки було частково припинено енергопостачання споживачів Прикарпаттяобленерго Причиною масштабної аварії, в даному випадку, стало втручання в роботу автоматизованої системи контролю і управління енергообладнанням [3]. Подібного типу загроза також може бути реалізована через наявність вразливостей інтелектуальних мереж Smart Grid, побудованих на базі інтелектуальних лічильників (Smart Meter).

Кібератака на розподілену автоматизовану систему Прикарпаттяобленерго є одним з перших випадків, коли за допомогою атаки в кібернетичному просторі вдалося припинити електропостачання майже цілого регіону країни. Наявність подібних фактів зміщує акценти поняття «ефективності ведення хакерської атаки» у військову площину та вказує на потенційну вразливість інформаційної інфраструктури стратегічних технологічних об'єктів в кібернетичному просторі.

Виходячи з викладеного в ході планування заходів з протидії кіберзагрозам, на нашу думку, особливу увагу слід приділити захисту інформації, що обробляється в автоматизованих системах критичної інфраструктури.

Література

1. CERT-UA, Команда реагування на кіберзагрози в Україні.

2. Форум з кібербезпеки, Kaspersky Lab, Венгрия, 20.11.2015.

3. The Washington Post, Hackers suspected in attack that blacked out parts of Ukraine, 05 Jan 2016.

УДК 351.86:004.056

Козюра В. Д.
кандидат технічних наук, доцент
Національна академія СБ України
Хорошко В. О.
доктор технічних наук, професор
Національний авіаційний університет України
Шелест М. Є.
доктор технічних наук, професор
Національний авіаційний університет України

КІБЕРНЕТИЧНА БЕЗПЕКА ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА: АНАЛІЗ ПРОБЛЕМИ

Формування та розвиток сучасного інформаційного суспільства базується на синтезі двох технологій: комп'ютерної та телекомунікаційної й визначається двома простими, але дуже змістовними законами: 1) Гордона Мура - «…кількість транзисторів у процесорах збільшуватиметься вдвічі кожних півтора роки…», який фактично пояснює виникнення нових специфічних за фор-

мою і способами суб'єктів і об'єктів інформаційної інфраструктури, а також гарантоване зростання швидкості обчислень і об'ємів оброблюваної інформації; 2) Роберта Меткалфа - «…цінність мережі знаходиться у квадратичній залежності від кількості вузлів, які є її складовими», тобто основу сучасного інформаційного суспільства становлять мережі різного функціонального призначення, а також новітні інформаційно-текомунікаційні (ІТ) технології, які:

- стали важливою складовою суспільного розвитку світової економіки у цілому й разом з тим значною мірою змінили механізми функціонування суспільних інститутів та інститутів державної влади;

- увійшли до числа найбільших суттєвих факторів, які впливають на формування сучасного високоорганізованого інформаційного середовища.

Поступове поєднання інформаційно-телекомунікаційних систем (ІТС) і мережевих технологій, які в процесах обробки, передачі та зберігання інформації використовують електромагнітний спектр і діють як єдине ціле, а також відповідного програмного забезпечення призвело до формування кіберпростору – високорозвиненої моделі об'єктивної реальності, у якій відомості про особи, предмети, факти, події, явища і процеси подані у деякому математичному, символьному або будь-якому іншому виді, розміщуються в пам'яті фізичних пристроїв, перебувають у постійному русі по сукупності ІТ систем і мереж.

Про важливість кіберпростору свідчить поява концепції ведення кібервоєн у ньому, створення у збройних силах ряду країн світу (США, Росія, Китай та інші) спеціальних структур, призначених для ведення такої боротьби і реалізуючих комплекс заходів, спрямованих на здійснення управлінського та/або деструктивного впливу власних інформаційних ресурсів шляхом використання спеціальних апаратно-програмних засобів.

Такий стан справ дає можливість говорити про наступні проблеми:

1) поява зовсім нових загроз безпеці як для об'єктів критично важливої інфраструктури держави, так і для громадян та суспільства в цілому. Це потребує переходу на вищий ступінь досліджень, спрямованих на всебічний аналіз методів, засобів, тактики та стратегії дій у кіберпросторі;

2) безпрецедентне розголошення персональних даних, важливих корпоративних ресурсів, конфіденційної інформації та ін-

формації, що становить державну або іншу, передбачену законом таємницю;

3) трансформація безпекового сектору держави за напрямами:

- пошуку і добування інформації шляхом вдосконалення способів й методів організації і проведення атак на ІТС, захищені криптосистеми протиборчих сторін та автоматизації усіх супутніх цьому процесів;

- обміну інформацією шляхом розробки принципово нових ІТС спеціального призначення;

- захисту власного інформаційного ресурсу від внутрішніх та зовнішніх кібервтручань та загроз.

Найбільший інтерес з позиції класифікації кібернетичних втручань і загроз становить схема, запропонована Конвенцією Ради Європи по боротьбі з кіберзлочинністю:

1) інциденти, спрямовані проти конфіденційності, цілісності й доступності комп'ютерних даних і систем, що реалізуються через:

- несанкціонований доступ в інформаційне середовище;

- втручання в дані;

- втручання в роботу системи;

- незаконне перехоплення ;

- незаконне використання комп'ютерного й телекомунікаційного устаткування;

2) шахрайство та підробка, пов'язані з використанням комп'ютерів, що полягають у:

- підробці документів із застосуванням комп'ютерних засобів;

- шахрайстві із застосуванням комп'ютерних засобів.

3) інциденти, пов'язані з розміщенням у мережах протиправної інформації;

4) інциденти відносно авторських і суміжних прав.

Представлена схема дає можливість:

по-перше, умовно об'єднати зазначені типи дій у дві укрупненні категорії – втручання та загроза, спрямовані безпосередньо на порушення нормального функціонування ІТС та підключених до них комп'ютерів (тип 1) , а також «традиційні» протиправні дії (типи 2, 3, 4), що або пов'язані з комп'ютером, або вчинені за його допомогою;

по-друге, зробити висновок про те, що зазначені дії у кіберпросторі вийшли за межі окремих країн й набули при цьому істотну фінансову підтримку та якісні комунікації;

по-третє, формалізувати зазначені типи дій, представивши їх моделлю, яка міститиме три головні етапи: 1) вивчення певного об'єкта; 2) проведення нападу на нього; 3) приховання слідів нападу. Крім того, як мінімум, в кожному етапі повинні бути дві стадії – стадія інформаційного обміну й власне стадія нападу. Останні, у свою чергу складатимуться з операцій щодо обміну даними, рекогносцировки, скасування й складання карти дій, а також з операцій одержання доступу, розширення повноважень, крадіжки інформації, бомбування, знищення слідів, створення «чорних ходів» і відмови в обслуговуванні.

Таким чином, характерними ознаками, які нині уособлюють поняття кібербезпеки, є сукупність активних захисних і розвідувальних дій, що в процесі інформаційного протиборства зусиллями організованих кіберугрупувань розгортається навколо інформаційних ресурсів та ІТС та які спрямовані на досягнення і утримання потенційними протиборчими сторонами перемоги у протидії новим загрозам безпеці для власних об'єктів критично важливої інформаційної інфраструктури.

Останнім часом такі дії займають чітке місце у геополітичній конкуренції переважної більшості країн світу, що, в свою чергу, обумовлює нові завдання їх службам безпеки та збройним силам й виводить на перший шлях проблему інформаційного протиборства.

УДК 004.621.3

Козюра В. Д.
кандидат технічних наук, доцент
Національна академія СБ України
Хорошко В. О.
доктор технічних наук, професор
Національний авіаційний університет України

ДЕЯКІ ПИТАННЯ ЩОДО СТВОРЕННЯ СИСТЕМИ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ В УКРАЇНІ

Кількість деструктивних інцидентів у сфері комп'ютерних та Інтернет-технологій за період з 2005 по 2015 рік збільшилася

приблизно у 2,7 рази. Саме тому найбільш пріоритетним напрямом керівництво України вважає реформування системи забезпечення інформаційної безпеки. У проекті Доктрини інформаційної безпеки України (2014 р.) одним з головних напрямів визначено забезпечення конфіденційності, цілісності та доступності інформації в національних інформаційних ресурсах від кібернетичних атак шляхом створення в інформаційно-телекомунікаційних системах (ІТС) комплексних систем захисту інформації з підтвердженою відповідністю.

Враховуючи таке вже зараз у Адміністративному та Кримінальному кодексах України до переліку протиправних дій у кіберпросторі віднесено:

- несанкціоноване втручання в роботу комп'ютерів та ІТС;
- несанкціонований збут або розповсюдження інформації з обмеженим доступом;
- створення та використання шкідливих програмних та технічних засобів;
- несанкціоновані дії з інформацією, яка обробляється в комп'ютерах та комп'ютерних мережах;
- здійснення незаконного доступу до інформації в ІТС;
- незаконне виготовлення чи розповсюдження копій баз даних тощо.

Протидіяти таким діям на теренах України спроможні:

- центральні органи виконавчої влади, які реалізують державну політику у сфері інформатизації та телекомунікацій, захисту державних інформаційних ресурсів в ІТС, а також криптографічного та технічного захисту інформації;
- органи державної влади, підприємства, організації (зокрема приватні) та установи, які експлуатують об'єкти критично важливої інфраструктури або здійснюють господарську діяльність у сфері захисту інформації в ІТС;
- Національний банк України, який формує та реалізує державну політику із забезпечення інформаційної та кібербезпеки банківських установ;
- підрозділи спеціального призначення, що виконують завдання із забезпечення кібернетичної безпеки;
- оператори (провайдери) телекомунікацій тощо.

Все це, з огляду на тенденції розвитку національного кібернетичного простору, потребує від України координації зусиль

державного і приватного секторів у протидії новим викликам в інформаційній сфері та вказує на необхідність подальшого секторального вироблення принципів і механізмів реагування на можливі комп'ютерні інциденти.

Серед підрозділів та формувань спеціального призначення найбільше навантаження в ході вирішення завдань кібернетичного лягає на:

- Державну службу спеціального зв'язку та захисту інформації (ДССЗЗІ) України , що реалізує державну політику в сфері захисту інформації в інформаційно-телекомунікаційних мережах;
- Службу безпеки (СБ) України, що реалізує державну політику в сфері охорони інформації з обмеженим доступом, яка є власністю держави;
- Міністерство внутрішніх справ (МВС) України, що здійснює досудове слідство у справах про злочини у сфері інформаційних технологій;
- Міністерство оборони (МО) України, що планує та реалізує заходи протидії і нейтралізації кіберзагроз національним інтересам України у воєнній сфері, впровадження новітніх інформаційних технологій у сфері оборони;
- Службу зовнішньої розвідки України (СЗР).

З моменту здобуття незалежності Україна прагне створити комплексну систему протидії внутрішнім і зовнішнім загрозам власному кібернетичному простору, однак існує низка проблем, що заважають нашій державі це зробити:

- деградація науково-технічного потенціалу, нерозвиненість інноваційної системи в інфосфері та низький рівень конкурентоздатності в ній;
- значна уразливість інфосфери через надмірно широке впровадження до неї іноземних програмних та матеріально-технічних засобів;
- непрозорість розподілу обов'язків між відомствами, правоохоронними органами та силовими структурами, які спеціалізуються на проблемах кіберзахисту та їх незадовільне кадрове забезпечення;
- відсутність загальнонаціонального координаційного центру, який був би спроможним узгоджувати та координувати діяльність правоохоронних органів, силових структур і відомств щодо протидії реальним загрозам інформаційному та кіберпростору України;

− відсутність єдиного понятійно-термінологічного поля кібербезпеки України, як головної складової інформаційної безпеки, та системних нормативно-правових документів, які б регламентували діяльність відомств, правоохоронних і силових структур у сфері кіберзахисту.

Такий стан фактично є каталізатором для реалізації втручань і загроз в інфосферу України, результатом чого може стати порушення управління державою, її інституціями та окремими об'єктами критично важливої інформаційної інфраструктури. Це вимагає від керівництва країни формування надійної системи кібернетичної безпеки шляхом започаткування низки міжвідомчих, а можливо й міждержавних ініціатив на кшталт:

− проведення аналізу ІТ ринків та організації взаємодії ІТ мереж;

− визначення понятійно-категорійного апарату і потенційних загроз власній кібернетичній безпеці;

− формування критеріїв віднесення об'єктів кіберпростору до критично важливої інформаційної та кіберінфраструктури;

− удосконалення механізмів надання взаємодопомоги у технічних і методологічних аспектах випереджувального виявлення джерел, фіксації та оперативного обміну інформацією про факти здійснення кібератак;

− вироблення та реалізації єдиної науково-технічної політики щодо захисту державних інформаційних ресурсів та ІТ інфраструктури від деструктивного кібервпливу;

− створення нової сучасної навчально-наукової бази для підготовки фахівців;

− розробки єдиних механізмів аудита та сертифікації програмно-апаратних комплексів, використовуваних у державних та військових системах управління;

− модернізації існуючих та розробки нових захищених інформаційних технологій;

− організації міжвідомчої взаємодії та координації державних органів при оцінюванні реальних і потенційних загроз в інформаційній сфері, а також вироблення та реалізації заходів щодо їх усунення;

− удосконалення міждержавних консультативних механізмів з питань законодавчого забезпечення і регулювання діяльності у сфері боротьби з кіберзлочинністю і кібертероризмом та внесення змін до низки існуючих нормативно-правових актів України;

− створення міжнародного експертного центру з питань регулювання взаємовідносин у галузі телекомунікацій та зв'язку тощо.

Було б раціональним удосконалити організаційно-правові норми міжнародної взаємодії з питань боротьби з кіберзлочинністю і кібертероризмом та запропонувати світовій спільноті внести зміни і доповнення до низки існуючих міжнародних нормативно-правових документів.

У результаті це дасть можливість:

− провести огляд кібербезпекової сфери держави, що дозволив би більш чітко визначити сучасний стан її нормативного забезпечення та основних проблем, які мають бути вирішені вже найближчим часом;

− розробити на підґрунті моделей розвитку світового кібернетичного простору власну модель та реалізувати її;

− впорядкувати політику України у сфері інформаційної та кібербезпеки і виробити так звані загальні правила поведінки у кіберпросторі;

− визначитись з розбіжностями між військовими та цивільними об'єктами в інформаційному та кіберпросторах і сформулювати вимоги щодо безпеки для ключових доменів;

− визнати міжнародним злочином проведення кібератак і кібероперацій на об'єкти інформаційної та кіберінфраструктури України, які спроможні привести до виникнення техногенних катастроф або надзвичайних ситуацій.

УДК 004.621.3

Козюра В. Д.
кандидат технічних наук, доцент
Національна академія СБ України
Хорошко В. О.
доктор технічних наук, професор
Національний авіаційний університет

КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ ТА ЗЛОЧИННІСТЬ

Проблема комп'ютерної злочинності та розробка механізмів протидії привернула до себе увагу провідних криміналістів як України, так і зарубіжних країн ще з часів широкого впрова-

дження комп'ютерної техніки, що спричинило цілий комплекс негативних наслідків та загострило ситуацію із забезпеченням інформаційної безпеки даних, що містяться в базах даних окремих комп'ютерів і комп'ютерних систем.

Нині висока технологічна злочинність набуває швидких темпів. Інтернет дозволяє злочинцям швидко отримувати прибуток з відносно невеликим ризиком бути спійманим. Знаходячись у мережі Інтернет, можна порушувати закон на відстані, швидко і незалежно від місця перебування. Злочинцям легко ошукати безліч людей, приховувати докази і награбоване. Вони стали значною загрозою для світового суспільства. Дуже часто, навіть виявивши втручання або інформаційні та фінансові втрати, власники організацій та фірм не завжди повідомляють про них правоохоронні органи, не бажаючи зашкодити репутації фірми.

В Україні комп'ютерна злочинність ще не набула значних масштабів, але її прояви вже зафіксовані. Так, 16-20 листопада 2001 року зазнала вірусної атаки обчислювальна мережа генеральної дирекції ВАТ «Укртелеком», яка налічує понад 700 комп'ютерів та десятки серверів. Як наслідок, це вивело з ладу систему корпоративної електронної пошти, а також тимчасове відключення Інтернету. Збитки становили понад 1 млрд. грн.

Злочини, які кояться у сфері комп'ютерних технологій, кваліфікуються за ознаками статей Кримінального кодексу України: 163 – «Порушення таємниці листування, телефонних розмов, телеграфної та іншої кореспонденції, що передається засобами зв'язку або через комп'ютер»; 190 – «Шахрайство»; 191 – «Привласнення, розтрата майна або заволодіння ним шляхом зловживання службовим становищем»; 231 – «Незаконне збирання з метою використання або використання відомостей, що становлять комерційну таємницю»; 358 – «Підробка документів»; 361 – «Незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку»; 362 – «Несанкціоновані дії з інформацією, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї»; 363 – «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».

На сьогодні ще більш небезпечним є те, що сучасні інформаційні технології в своїй злочинній діяльності використовують організовані злочинні угруповання, які вийшли на принципово новий якісний рівень свого розвитку. Злочини у сфері інформаційних технологій вчиняються, як правило, високоорганізованими злочинними угруповуваннями. Інтереси організованих злочинних угруповувань, переважно спрямовані на крадіжку та «відмивання» грошей здобутих злочинним шляхом, фінансові махінації, в першу чергу в кредитно-фінансовій сфері, де активно використовуються автоматизовані системи.

Найбільш небезпечним злочином, який представляє загрозу є – кібертероризм.

Нині під кібертероризмом західні та вітчизняні фахівці розуміють суспільну небезпечну діяльність, що свідомо здійснюється в інформаційному просторі окремими особами або організованими злочинними угруповуваннями з терористичною метою та реалізується ними через заздалегідь сплановані й політично вмотивовані кібератаки на інформаційні ресурси з використанням високих технологій. До його основних особливих рис вони відносять: високу ефективність кібератак; просторово-часову невизначеність джерела кібератаки та його віддаленість від об'єкта атаки; часову невідповідність між власне кібератакою й процесом її підготовки тощо. Спектр прояву кібертероризму достатньо широкий – від прийняття хибних рішень або розповсюдження паніки, до проникнення в канали і системи зв'язку тощо.

Все частіше злочинці використовують Інтернет для продажу наркотиків, зброї та трансплантантів. Вони через захищені чат канали заключають угоди, а за допомогою Інтернет – банків «відмивають» свої прибутки.

Треба відмітити, що за прогнозами провідних науковців у галузі інформаційної безпеки, вже найближчими роками можливе стрімке зростання кіберзлочинців. Це змушує світове товариство терміново вжити відповідних заходів як на законодавчому, так і організаційних рівнях.

Література

1. Кримінальний кодекс України : Закон України від 05.04.2001 №2341 – III [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua.

2. Убытки «Укртелекома» от вирусной атаки – более 1 млн. грн. [Електронний ресурс]. – Режим доступу : http://news.finance.ua.

УДК 351.865

Лук'янчук Р. В.
Інститут законодавства Верховної Ради України

ДЕРЖАВНІ ГАРАНТІЇ ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ В УМОВАХ СЬОГОДЕННЯ

Забезпечення кібербезпеки на державному рівні, в умовах сьогодення, та з урахуванням постійної інформаційної експансійної політики з боку РФ, є одним із пріоритетних та першочергових завдань в контексті національної безпеки країни.

Такий стан справ викликає потребу створення Національної системи кібербезпеки, в якій буде чітко визначено підрозділи, що займатимуться питаннями кібербезпеки та здійснюватимуть боротьбу з кіберзлочинністю. Зокрема, необхідно узгодити питання взаємодії та координації зусиль, спрямованих на здійснення заходів по боротьбі з кіберзлочинністю таких служб та установ, як СБУ, Держава служба спеціального зв'язку та захисту інформації, підрозділи МВС, на які покладено функції по здійсненню певних заходів з кібербезпеки. Ситуація, за якої, в наш час, відбуваються постійні посягання на суверенітет та інформаційний простір держави через здійснювані кіберзлочини – це пряме свідченння того, що в країні існує необхідність створення конкретної структури, яка буде визначена головною відповідальною інституцією за кібербезпеку та відповідно до функціонування якої і буде в подальшому скоординовано роботу всіх підрозділів.

Постійний моніторинг огляду здійснюваних кібернападів на деякі установи та організації нашої країни свідчить про необхідність посилення заходів та прискорення прийняття відовідних нормативних документів. Такі заходи є актуальними і тому, що значне розповсюдження кібертехнологій та кібератак на інформаційні ресурси інших країн здійснюється з використанням інфомраційних ресурсів України. Саме тому для нашої держави важливо ствати активним учасником міжнародних дискусій щодо писилення бортьби у зазначеній сфері. Скоординована співпраця з іншими державами та взаємодія сприятиме ефективному впровадженню дієвих механізмів боротьби з кібератаками, а досвід успішних країн допоможе здійснювати якісні заходи щодо впровадження необхідних кроків.

Важливість такої співпраці підтерджується й тим, що Україна перша з позаблокових країн, яка розпочала з НАТО експертні консультації з питань кібербезпеки. Наша держава виступила першою з країн-партнерів, що внесла конкретні пропозиції стороні НАТО щодо започаткування співробітництва у сфері кібернетичного захисту. Це в свою чергу спонукало НАТО виробити програмні основи співпраці з іншими країнами-партнерами.

Також було створено Трастовий фонд Україна – НАТО з кібербезпеки. Також, в рамках цього фонду, було повідомлено про те, що румунська державна компанія Rasirom, яка створена з метою протидії російським хакерам, надасть Україні допомогу по захисту від нападу кіберзлочиниців зі сторони РФ [3].

Ще одним важливим кроком у 2015 році у налагоджені співпраці з Румунією стала ратифікація угоди між Кібенетом Міністрів України та урядом Румунії «Про взаємну охорону інформації з обмеженим доступом».

Увага інших держав до проблеми кібервійни України з Росією постійно підтверджується відповідними заходами. Так, Центром НАТО з кіберзахисту, що займається дослідницькою і навчальною діяльністю у сфері кібербезпеки, а також посиленням інформаційної безпеки країн альянсу було видано книгу про кібервійну між Україною та Росією під назвою «Cyber War in Perspective: Russian Aggression against Ukraine». Як зазначається у книзі, конфлікт в Україні є благодатним ґрунтом для кібервійни, Росія і Україна відстоюють власні геополітичні інтереси, і кожна з країн володіє високим рівнем професіоналізму у сфері інформаційних технологій і злому комп’ютерних мереж. Експерти вказують на те, що поняття «кібератака» вийшло за рамки тільки інформаційної війни. Тепер воно включає цифрову пропаганду, DDoS-кампанії, дефейси web-сайтів, витоки інформації внаслідок атак активістів, а також використання шкідливого ПЗ для шпигунства [1].

Але питання забезпечення кібербезпеки на державному рівні все ще залишається досить актуальним. Нормативно - правове регулювання потребує значного перегляду існуючих законодавчих актів та прийняття ряду нових, що необхідні для врегулювання питань з проблем боротьби з кіберзлочинністю.

Позитивним є те, що у 2015 році та на початку 2016 року вже було здійснено деякі заходи: створення в Державній службі спеціального зв’язку та захисту інформації України Національно-

го центру кіберзахисту та протидії кіберзагрозам; у Національній поліції - Департаменту кіберполіції. Такі установи мають здійснювати гарантоване забезпечення безпеки нашої країни та притидіяти кримінальним правопорушенням, що стосуються кіберзлочинності [2].

Наступним важливим кроком, з урахуванням викликів, що постають перед нашою державою, стало ухвалення на черговому засіданні РНБО Стратегії кібербезпеки. Стратегія передбачає розвиток національної системи забезпечення захисту кіберпростору, запобігання, виявлення і нейтралізації кіберзагроз. Також у стратегії йдеться про координацію, взаємодію і розподіл повноважень і відповідальності органів сектору безпеки і оборони України у питаннях кібербезпеки, кіберзахисту і протидії кібертероризму та кіберзлочинності. Відповідно до Стратегії передбачається створення єдиної бази даних про кіберзагрози і системи постійного обміну інформацією.

Саме тому, з метою забезпечення кібернетичної безпеки України необхідно створити цілісну Національну систему кібернетичної безпеки ключовими завданнями якої є: формування та реалізація державної політики в сфері кібернетичної безпеки; моніторинг кібернетичного простору з метою своєчасного виявлення, запобігання і нейтралізації кібернетичних загроз; виявлення, попередження та припинення кібернетичних злочинів; кібернетичний захист національної критичної інформаційної інфраструктури тощо. Відповідно до таких завдань потребує удосконалення чинне законодавство щодо визначення поняття кібербезпеки та її складових, а також врахування при розробці нормативних документів міжнародних рекомендацій та досвіду зарубіжних країн.

Література

1. Про затвердження Річної Національної програми співробітництва Україна - НАТО на 2015 рік: Указ Президента України від 23 квітня 2015 року №238/201 // Офіційний вісник України. - 2015. - №34.

2. Про рішення Ради національної безпеки і оборони України від 28 серпня 2014 року «Про невідкладні заходи щодо захисту України та зміцнення її обороноздатності»: Указ Президента України від 24 вересня 2014 року №744/2014 // Офіційний вісник Президента України. - 2014. - №40.

3. Угода про реалізацію Трастового фонду Україна - НАТО з питань кібербезпеки між Службою безпеки України та Румунською службою інформації від 23 липня 2015 року // Офіційний вісник України. - 2015. - №79.

УДК 621.391

Меленті Є. О.
кандидат технічних наук
Інститут підготовки юридичних кадрів для
Служби безпеки України
Національного університету «Юридична академія України імені
Ярослава Мудрого»

МОЖЛИВІ ШЛЯХИ ПІДВИЩЕННЯ РІВНЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ УКРАЇНИ

На зламі тисячоліть людство переживає бурхливий розвиток комп'ютерних та інформаційних технологій. Ця тенденція сколихнула всі сфери життєдіяльності суспільства. Постійне розширення сфери застосування комп'ютерної техніки обумовлене значними досягненнями науки у галузі комп'ютерних знань.

Однак, як свідчить світовий досвід, невпинно поширюються загрози, пов'язані з криміналізацією інформаційної сфери, у тому числі – глобальної мережі Інтернет, відкритість якої спричиняє високу уразливість від злочинних посягань [1]. Пропорційно розширенню всесвітньої мережі зростає кількість, так званих кіберзлочинів: спам, торгівля людьми, розкрадання електронних банківських рахунків, несанкціоноване ознайомлення, копіювання інформації з обмеженим доступом. Міжнародна правоохоронна практика свідчить про значне зростання рівня злочинних актів щодо інформаційних та інформаційно-телекомунікаційних систем, що утворює загрозу окремим організаціям, установам і фізичним особам, а також економіці та обороні кожної країни і суспільства в цілому [2, 3].

Злочинні дії можуть бути спрямовані на доступ до інформації, що відноситься до інформації з обмеженим доступом, з метою втрати її доступності, цілісності та конфіденційності. За умови успішних діянь зловмисника держава може зазнати значних втрат в економічній та оборонній сферах.

Загальноприйнятим визначенням кіберзлочинності є злочинність у так званому кіберпросторі. Автори «модельного закону» про кіберзлочинність Міжнародного Союзу Електрозв`язку (2009 р.) визначають кіберпростір як «фізичний і не фізичний простір, створений і (або) сформований таким

чином: комп`ютери, комп`ютерні системи, мережі, їхні комп`ютерні програми, комп`ютерні дані, дані контенту, рух даних, і користувачі» [2].

Злочини в кібернетичному просторі характеризується тим, що підготовка та скоєння злочину здійснюється, практично не відходячи від "робочого місця", злочини є доступними; оскільки комп'ютерна техніка постійно дешевшає; злочини можна скоювати з будь-якої точки земної кулі, у будь-якому населеному пункті, а об'єкти злочинних посягань можуть знаходитись за тисячі кілометрів від злочинця. Крім того, доволі складно виявити, від слідкувати, зафіксувати і вилучити криміналістично-значущу інформацію (при виконанні слідчих дій) для використання її в якості речового доказу. Усе це, безумовно, є перевагами для кіберзлочинців [3, 4].

У 2005 р. Україна ратифікувала Конвенцію Ради Європи про кіберзлочинність [5], яка класифікує, скоєні в кібернетичному просторі злочині.

Слід розуміти, що потенційний злочинець (шпигун) досить обізнаний в своїй області фахівець. Він для заволодіння інформацією з обмеженим доступом здатен не тільки використовувати спеціальні програмні засоби через глобальну, локальні мережі, бездротовий зв'язок, але й здатний застосовувати також сучасні технічні засоби розвідки.

Саме тому невід'ємною складовою інформаційної безпеки будь-якої держави є захист інформації з обмеженим доступом, зокрема технічний захист. Захист інформації здійснюється державою шляхом прийняття відповідних правових, організаційних, технічних та програмних заходів, спрямованих на недопущення витоку інформації з обмеженим доступом, неправомірного впливу на інформацію та неправомірного доступу до інформації.

До однієї з основних загроз безпеці інформації належить витік інформації технічними каналами. При цьому відбувається поширення інформативного сигналу через фізичну середовище від джерела корисного сигналу до приймача технічного засобу розвідки, що здійснює перехоплення інформації.

Використання в технічних засобах розвідки надчутливих широкосмугових приймачів, систем захисту від активних завад та досить швидких алгоритмів виділення корисного сигналу дозволяє потенційному зловмиснику досить успішно здобувати інфор-

мацію з обмеженим доступом, яка циркулює в інформаційних чи інформаційно-телекомунікаційних системах. Проте для унеможливлення несанкціонованого витоку даних технічними каналами необхідно вживати адекватних заходів, які були б спрямовані на неможливість або мінімізацію імовірності витоку інформації. З цією метою застосовуються технічні засоби захисту інформації.

На теперішній час кіберзлочинність становить для нашої держави більш серйозну небезпеку, ніж ще 5 років тому. Звичайно, щоб ефективно протистояти злочинам в кібернетичному просторі насамперед необхідно мати відповідну нормативно-правову базу та спеціальні підрозділи в правоохоронних органах для боротьби з кіберзлочинністю. Співробітники таких підрозділів повинні знати не тільки правові аспекти та законодавчі норми, але й володіти глибокими знаннями про технічну, так і про програмну сторону питання, володіти сучасними інформаційними технологіями, бути обізнаними у принципах роботи телекомунікаційних систем, мереж і пристроїв, які використовуються для скоєння правопорушень, а також бути в курсі останніх розробок у сфері IT-технологій.

Досвід останніх суспільно-політичних подій, що відбувалися в Україні, досить яскраво показав, що для забезпечення національної безпеки в інформаційному просторі необхідно більше приділяти уваги захисту важливих інформаційних ресурсів, баз даних держави, що містять інформацію з обмеженим доступом, контролю медійних та інтернет-ресурсів.

Таким чином, можна виділити декілька шляхів підвищення рівня кібернетичної безпеки України:

1) врегулювання нормативно-правової бази, яка б відповідала вимогам, що висуваються сучасним рівнем розвитку інтернет-технологій; адаптація (прийняття) відповідних законодавчих актів до правового поля провідних країн світу;

2) організація взаємодії і координація зусиль правоохоронних органів, спецслужб, судової системи, забезпечення їх необхідною матеріально-технічною базою; забезпечення висококваліфікованими фахівцями підрозділів боротьби з кіберзлочинністю в правоохоронних органах; залучення іноземних спеціалістів з інформаційної безпеки для обміну досвідом;

3) удосконалення технічного захисту інформації з обмеженим доступом в інформаційно-технічних системах, розголошення

якої загрожує національній безпеці та обороні країни; розробка (модернізація) та виробництво на державних підприємствах сучасних спеціальних програмних та технічних засобів для технічного захисту інформації;

4) проведення інформаційної роботи з населенням щодо підвищення рівня культури користування власними банківськими рахунками, грошовими картками, платіжними системами, особистими даними в мережі Інтернет та соціальних мережах.

Література

1. Зимовець В.В., Чувирін Д.Є. Кіберзлочинність в Україні: перспективи протидії // Боротьба з організованою злочинністю і корупцією (теорія і практика), 2006. – № 13. – С. 99–112.

2. Кіберзлочинність: проблеми боротьби і прогнози [Електронний ресурс]. - Режим доступу: http//:anticyber.com.ua›article_detail.php?id=140

3. Кіберзлочинність в Україні: перспективи протидії [Електронний ресурс] .Режим доступу: http: //5ka.at.ua/ load/pravo/ kiberzlochinnist _v_ukrajini_perspektivi_protidiji_referat.

4. Интернет-преступность: монография / Р.И. Дремлюга. – Владивосток: Изд-во Дальневост. ун-та, 2008. – 240 с.

5. Закон України від 7 вересня 2005 року “Про ратифікацію Конвенції про кіберзлочинність”.

УДК 351.863

Мовчан А. В.

доктор юридичних наук, старший науковий співробітник

Національна академія внутрішніх прав

КІБЕРНЕТИЧНА БЕЗПЕКА – ВАЖЛИВА СКЛАДОВА ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

У сучасних умовах кіберзлочинність стає однією з найбільших загроз національній безпеці України, зокрема, значного впливу на суспільне життя та економіку в нашій країні набули глобальні інформаційні мережі (передусім мережа Інтернет), які отримали в науковій літературі назву “кіберпростір”.

Водночас у законодавчих актах поняття кіберпростору практично не регламентовано, лише в проекті закону “Про основні засади забезпечення кібербезпеки України” кібернетичний

простір (кіберпростір) визначається як середовище, яке виникає в результаті функціонування на основі єдиних принципів і за загальними правилами інформаційних (автоматизованих), телекомунікаційних та інформаційно-телекомунікаційних систем; кібернетична безпека (кібербезпека) – як стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі [1].

Пріоритетами забезпечення кібербезпеки і безпеки інформаційних ресурсів є, насамперед: розвиток інформаційної інфраструктури держави; створення системи забезпечення кібербезпеки, розвиток мережі реагування на комп'ютерні надзвичайні події (CERT); моніторинг кіберпростору з метою своєчасного виявлення, запобігання кіберзагрозам і їх нейтралізації; розвиток спроможностей правоохоронних органів щодо розслідування кіберзлочинів; забезпечення захищеності об'єктів критичної інфраструктури, державних інформаційних ресурсів від кібератак, відмова від програмного забезпечення, зокрема антивірусного, розробленого у Російській Федерації; реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом, захист державних інформаційних ресурсів, систем електронного врядування, технічного і криптографічного захисту інформації; створення системи підготовки кадрів у сфері кібербезпеки для потреб органів сектору безпеки і оборони; розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, інтенсифікація співпраці України та НАТО у сфері кібербезпеки в рамках функціонування Трастового фонду НАТО, для посилення спроможностей України у сфері кібербезпеки [2].

Нині кіберпростір використовується злочинними та терористичними угрупованнями для незаконної торгівлі наркотиками, зброєю, боєвими припасами і вибуховими речовинами, розповсюдження дитячої порнографії, підготовки та здійснення терористичних актів і збройної агресії проти України, проведення різного роду екстремістської діяльності, порушення авторських прав, а також промислового (комерційного) шпигунства, конкурентної розвідки тощо. Джерелами кібернетичних загроз можуть бути міжнародні злочинні групи хакерів, окремі підготовлені у сфері інформаційних технологій злочинці, іноземні державні органи, терористичні та екстремістські угруповання, транснаціональні корпорації та фінансово-промислові групи тощо.

Сучасна кіберзлочинність характеризується високою латентністю; використанням новітніх технологій, сучасним апаратним та програмним забезпеченням; організованістю, міжрегіональними та міжнародними зв'язками; використанням інформаційних ресурсів, які територіально розташовані у різних країнах. Подальшій криміналізації кіберпростору сприяє низка характерних особливостей "віртуального" середовища: транснаціональність Інтернету (відсутність кордонів, митниць, територіальна роз'єднаність груп людей); уявна анонімність користувачів (як імена у мережі використовуються псевдоніми (ніки)); значна кількість користувачів, до яких легко можна довести свої ідеї, організувати їх для проведення якої-небудь акції, формувати громадську думку, навмисно дезінформувати, збирати інформацію; законодавча неврегульованість цього середовища [3, с. 160].

Останнім часом об'єктами кібератак та кіберзлочинів дедалі частіше стають інформаційні ресурси фінансових установ, підприємств транспорту та енергозабезпечення, державних органів, які забезпечують безпеку, оборону, захист від надзвичайних ситуацій, а також сервери їх офіційних Інтернет-представництв і електронної пошти. Кількість злочинів, що вчиняється у кіберпросторі, зростає пропорційно числу користувачів комп'ютерних мереж. За оцінками компанії Symantec Corp щорічно глобальна кіберзлочинність обходиться планеті в 114 млрд доларів [4].

Виділяються чотири групи відомостей, які найбільш часто піддаються нападу з використанням шкідливих програм: доступ до різних фінансових операцій (онлайн-банкінг, платіжні картки, електронні гроші), інтернет-аукціонів тощо; доступ до поштових скриньок, які є складовою частиною ICQ-акаунтів, як і всі знайдені на комп'ютері адреси електронної пошти; паролі, коди доступу до інтернет-пейджерів, сайтів тощо; паролі, коди до онлайн-ігр [3, с. 160]. За даними Української міжбанківської асоціації членів платіжних систем, у 2015 році зареєстровано 1089 випадків шахрайства з банкоматами, 2771 фальшивий дзвінок для виманювання грошей, 38 сайтів виуджували інформацію про доступ до банківських карток [5].

В умовах глобальної нестабільності значного розповсюдження набуло використання кіберпростору для здійснення конкурентної розвідки та промислового (комерційного) шпигунства. Завдяки високим технологіям шпигувати за чужими промисло-

вими секретами стало набагато простіше, ніж 10–15 років тому. Подальший розвиток науково-технічного прогресу, збільшення потоку патентів і жорсткість конкурентної боротьби роблять викрадення чужих комерційних таємниць особливо прибутковою і перспективною справою. Як результат, втрати Німеччини від промислового шпигунства оцінюють у 20 млрд євро щорічно, втрати США – від 100 млрд доларів. Приміром, нещодавно суд у США засудив до тюремного ув'язнення сімейну пару китайського походження, яка здійснила крадіжку технологій гібридних силових установок у концерну General Motors з метою продажу Китаю для подальшого відтворення в автомобільній промисловості. Їм вдалося скопіювати близько 16 тис. документів і завдати шкоди концерну в розмірі 46 млн доларів [6].

Підсумовуючи викладене зазначимо, що в умовах глобальної нестабільності особливу занепокоєність викликає можливість застосування інформаційних технологій та можливостей кібернетичного простору в інтересах здійснення військово-політичного та силового протиборства, тероризму та проведення хакерських атак. Нині головним завданням держави є вжиття заходів, що дозволять протистояти протиправним діям у кіберпросторі, уникнути або зменшити негативні наслідки від реалізації кіберзагроз. Тому кібернетична безпека України в сучасних умовах є важливою складовою забезпечення національної безпеки України і потребує здійснення комплексу заходів організаційно-правового і технічного характеру.

Література

1. Про основні засади забезпечення кібербезпеки України : проект Закону України [Електронний ресурс] – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55657.

2. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України": Указ Президента України від 26 травня 2015 р. № 287/2015 / Офіційний вісник України. – 2015. – № 43. – С. 14. – Ст. 1353.

3. Мовчан А. В. Кібернетична безпека України в умовах глобальної нестабільності / А. В. Мовчан // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2015. – № 1. – С. 159–163.

4. Звіт: Глобальна кіберзлочинність щорічно обходиться в $ 114 млрд [Електронний ресурс]. – Режим доступу: http://project.ukrinform.ua/news/zvit_globalna_kiberzlochynnist_schorichno_obhodytsya_v_114_mlrd_51748/.

5. Шахрайств із банкоматами побільшало вдесятеро [Електронний ресурс]. – Режим доступу: http://gazeta.ua/articles/economics/_sahrajstv-iz-bankomatami-pobilshalo-vdesyatero/681102.

6. Автошпионы поплатились свободой [Електронний ресурс]. – Режим доступу: http://www.gazeta.ru/auto/2013/05/06_a_5313661.shtml.

УДК 316.659

Олешко О. А.
кандидат політичних наук, доцент
Воєнно-дипломатична академія імені Є. Березняка

ПРОБЛЕМА СТВОРЕННЯ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ В ІНФОРМАЦІЙНІЙ СФЕРІ

Сьогодні засоби масової інформації Російської Федерації агресивно та тенденційно висвітлюють ті чи інші події в нашій державі, її зовнішню політику, упереджено висвітлюють діяльність вищих посадових осіб держави, формуючи таким чином спотворене уявлення про ситуацію в Україні. Цей стан становить загрозу для національної безпеки України в інформаційній сфері особливо за умов відсутності дієвої системи забезпечення інформаційної безпеки.

Активна та наступальна позиція російських медіа дозволяє їм ефективно проводити інформаційні операції, які є складовими інформаційних війн з метою формування упереджених поглядів та контролю над масовою свідомістю населення як Російської Федерації, так і населення тимчасово окупованих територій України.

За допомогою цього здійснюється: маніпулювання суспільною думкою і політичною орієнтацією соціальних груп населення держави з метою створення політичної напруженості та хаосу; дестабілізація політичних відносин між партіями, дискредитація органів управління; провокація соціальних заворушень; завдання збитків життєво важливим інтересам держави в політичній, економічній, оборонній і в інших сферах тощо.

Ефективно протистояти інформаційним загрозам за сучасних умов може лише дієва система забезпечення інформаційної безпеки, яка повинна здійснюватися при узгодженій взаємодії всіх державних органів, недержавних структур і громадян.

Вважаємо, що для вирішення проблеми створення системи забезпечення національної безпеки України в інформаційній сфері було б доцільно здійснити ряд заходів:

– організація взаємодії правоохоронних структур України й інших держав в галузі виявлення, попередження і припинення злочинів в інформаційній сфері;

– створеннння ефективної багаторівневої системи забезпечення інформаційної безпеки, при ефективній координації діяльності органів державної влади на основі науково обґрунтованої моделі.

– розробка механізму узгодження діяльності органів державної і місцевої влади в забезпеченні інформаційної безпеки;

– прийняття законів, котрі регламентують побудову державної політики забезпечення інформаційної безпеки України [1-4];

– визначення функцій державних органів з питань, які пов’язані з різними аспектами забезпечення інформаційної безпеки України;

– створення системи захисту національних інформаційних і телекомунікаційних мереж і нормативно-правового забезпечення її безпечного функціонування;

– формування системи забезпечення інформаційної безпеки українського сегменту глобальних інформаційних та телекомунікаційних систем і мереж зв’язку тощо.

Література

1. Проект Закону України «Про інформаційний суверенітет та інформаційну безпеку України». [Електронний ресурс] – Режим доступу до сайту: http://uacm.kharkov.ua/ukr/index.shtml?ulaws/usuvetr.htm

2. Проект Указу Президента України «Про Доктрину інформаційної безпеки України»[Електронний ресурс]. – Режим доступу до сайту: http://comin.kmu.gov.ua/control/uk/publish/article?art_id=113319&cat_id=61025

3. Проект Концепції інформаційної безпеки України. [Електронний ресурс] – Режим доступу до сайту: http://mip.gov.ua/done_img/d/30-project_08_06_15.pdf

4. Проект Закону України «Про засади інформаційної безпеки України». [Електронний ресурс] – Режим доступу до сайту: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=51123

УДК 007.51:351.865

Слонов М. Ю.
кандидат технічних наук, доцент
Воєнно-дипломатична академія імені Є. Березняка

АЛГОРИТМ ВИЯВЛЕННЯ РАЦІОНАЛЬНИХ НАПРЯМІВ УДОСКОНАЛЕННЯ ФУНКЦІОНУВАННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ДЕРЖАВИ

Забезпечення кібернетичної безпеки держави є складною людино-машинною системою, функціонування якої зумовлено паралельним успішним існуванням низки окремих складних підсистем. Такі підсистеми будуть технічними (загальні та локальні сеті, сукупності комп'ютерів та сервісного чи периферійного обладнання – машинне наповнення), адміністративними (керівний склад та засоби управління – людино-машинне наповнення), виконавчими (безпосередньо виконавці – також людино-машинне наповнення).

Ураховуючи складності формалізації, а відповідно і аналітичної та практичної раціоналізації функціонування таких систем, корисним може бути функціонально-вартісний підхід [1]. Він дозволяє виявляти раціональні напрями удосконалення функціонування кібернетичної безпеки, причому у чисельному вигляді.

Застосування його базується на припущенні щодо прямої залежності між вартістю C_Σ системи, що досліджується, та рівнем виконання нею функціонального призначення, що може характеризуватися функціональною досконалістю P_Σ. Це стосується як системи в цілому, так і кожної її j-ї окремої частини. При цьому вирішується система рівнянь наступного типу:

$$\begin{cases} C_\Sigma = \sum\limits_{j=1}^{m} C_j = \min, \\ P_\Sigma = P_\Sigma\left[C_j\right] = \max. \end{cases} \qquad (1)$$

Розберемося з можливостями завдання значень P_j та C_j Рівень функціональної досконалості P_j в більшості випадків, і в даному випадку також, зручно описувати імовірністю виконання завдання. Вона стійко піддається формалізації [2] та дозволяє перейти на параметричний опис функціонування підсистеми.

Складніше з вартісними залежностями. Але за умовою виконання таких логічних умов:

$$\begin{aligned} &1. C(P) \geq 0, \\ &2. P_1 \geq P_2 \rightarrow C(P_1) \geq C(P_2), \\ &3. \lim_{P \to 0} C(P) = 0, \\ &4. \lim_{P \to 1} C(P) = \infty. \end{aligned} \qquad (2)$$

Можуть бути запропоновані поліноміальні залежності наступного вигляду:

$$\begin{aligned} &1. C_j(P) = A_j P \exp\left(\frac{B_j}{1-P}\right), \\ &2. C_j(P) = \frac{A_j P^{B_j}}{\ln\left(\frac{1}{P}\right)}, \qquad (3) \\ &3. C_j(P) = \frac{A_j P}{1-P}, \end{aligned}$$

де A_j та B_j – константи, що можуть бути підібрані емпірично.

Апроксимуючі вирази підбираються, виходячи з інтенсивності (пропорційності) зміни вартості системи разом зі зміною рівня її функціональної досконалості. Так, наприклад, для простішого випадку при використанні співвідношення (3.3) додаток вартості ΔC при збільшенні рівня функціональної придатності на ΔP буде складати:

$$\Delta C = A \frac{\Delta P}{(1-P)(1-P-\Delta P)}.$$

Наявність двох констант у співвідношеннях (3.1) та (3.2) дозволяє більш гнучко і точно за допомогою цих виразів описувати дійсні фізичні залежності. Коефіцієнт A_j має розмірність вартості. Можна його трактувати як таку вартість, яку замовник ще може сплатити за виконання функції всієї системи чи окремої ланки.

Коефіцієнт B_j характеризуватиме інтенсивність наближення вартості системи до максимального значення при $P_j \rightarrow 1$. Вибір

конкретного співвідношення залежіть від потрібної точності розрахунків, наявності відповідних експериментальних даних, вимог до аналітичного апарату.

Оскільки всі підсистеми функціонують паралельно, майже незалежно, імовірність виконання завдання обмежена заданим значенням $P_{зад}$, структурну функціонально-вартісну схему системи забезпечення кібернетичної безпеки держави можна представити у вигляді N окремих гілок, що зображене на рис. 1.

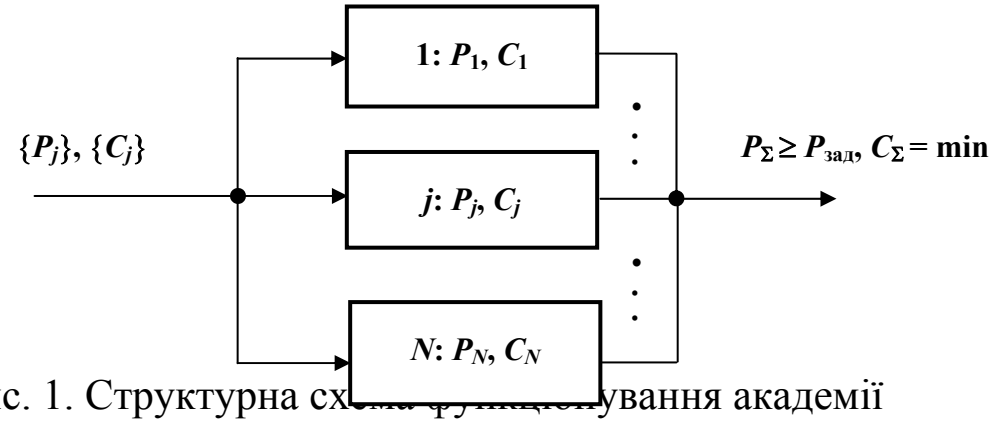

Рис. 1. Структурна схема функціонування академії

Система (1) для випадку опису поліноміальної вартісної залежності рівнянням (3.3) набуде наступного вигляду (за умовою N = 3):

$$\begin{cases} C_{\Sigma}(P_j) = \sum\limits_{j=1}^{3}\left(\dfrac{A_j P_j}{1-P_j}\right) = \min\limits_{0\le P_j\le 1}, \\ P_{\Sigma} = \prod\limits_{j=1}^{3} P_j \ge P_{зад}. \end{cases} \quad (4)$$

Методом множників Лагранжа система (4) зводиться до системи алгебраїчних рівнянь типу:

$$\begin{cases} \dfrac{A_1 P_1}{1-P_1} = \dfrac{A_2 P_2}{1-P_2}, \\ \dfrac{A_1 P_1}{1-P_1} = \dfrac{A_3 P_3}{1-P_3}, \\ P_{\Sigma} = P_1 P_2 P_3 \ge P_{зад}. \end{cases} \quad (5)$$

Рішенням системи (5) надає розподіл ймовірностей $P_j = 0, 1$; $j=\overline{1,N}$. Скористатися їм можна за двома напрямами.

По-перше, раціональний розподіл функціональної досконалості складових знов таки зворотно пропорційний значенню вартісного коефіцієнту A_j, тобто збільшення вартості окремої складової примушує збільшувати перш за все рівень функціональної досконалості більш дешевих складових.

По-друге, наявність конкретних значень ймовірностей P_j дозволяє перейти до параметричної раціоналізації кожної з підсистем.

Література

1. Слонов М.Ю. Функціонально-вартісна модель раціонального удосконалення навчального процесу // Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення з урахуванням досвіду АТО: VIII науково-практична конференція. Київ, 29 жовтня 2015 р. – Київ: Видавництво ВІТІ, 2015. – С. 186-187.

2. Большие технические системы: проектирование и управление / Л.М. Артюшин, Ю.К. Зиатдинов, И.А. Попов, А.В. Харченко. Под ред. И.А. Попова. – Харьков: Факт, 1997. – 400 с.

УДК 321.011:65.012.8

Солодка О. М.

кандидат юридичних наук, старший науковий співробітник

Національна академія СБ України

ЩОДО ВИЗНАЧЕННЯ ПОНЯТТЯ «ІНФОРМАЦІЙНИЙ СУВЕРЕНІТЕТ»

Суверенітет – це верховенство влади всередині країни та її незалежність від влади будь-якої іншої держави», «виняткове здійснення влади в певній державі без зовнішнього втручання, незалежність держави від інших держав у зовнішній і внутрішній політиці» [1].

Відтак, державний суверенітет має дві сторони:

1) внутрішню, яка відображає властивості державної влади відносно всіх інших організацій у політичній системі суспільства, її монопольне право на створення законодавства, управління і поширення повноважень в межах усієї державної території;

2) зовнішню, що відображає можливості держави як суб’єкта міжнародного права, неприпустимість втручання у внутрішньодержавні справи.

В інформаційній сфері, це проявляється у повноваженнях держави самостійно визначати свою інформаційну політику з урахуванням приписів міжнародного права в національному інформаційному просторі України. Відповідно, інформаційний простір України – це середовище, в якому здійснюється продукування, зберігання та поширення інформації, на яку розповсюджується юрисдикція України.

Вперше глобальна дискусія щодо інформаційного суверенітету мала місце після запуску Радянським союзом супутника у 1957 році, за допомогою якого інформація могла передаватись у будь-яку точку світу, тоді постало питання про загрозу можливості контролювати потоки інформації, яка надходить до широкого іноземного користувача та протидії радянській пропаганді.

Як вирішення десятирічної дискусії 15 листопада 1972 року ЮНЕСКО ухвалила «Декларацію керівних принципів з використання мовлення через супутники для вільного розповсюдження інформації, розвитку освіти і розширення культурних обмінів, основоположною ідеєю якої є те, що супутникове телебачення поважатиме суверенітет та рівність усіх держав, а кожна країна має право вирішувати питання контенту освітніх програм, які передаються супутником її громадянам» [2].

Єдине визначення інформаційного суверенітету, що міститься у національному законодавстві є 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» [3]. На нашу думку, таке визначення відображає технічну складову інформаційного суверенітету.

У Законі України «Про інформацію» (редакціях 2002 – 2011 рр.) [4] вказувалось, що основою інформаційного суверенітету України є національні інформаційні ресурси, до яких входить вся належна їй інформація, незалежно від змісту, форм, часу і місця створення, а Україна самостійно формує інформаційні ресурси на своїй території і вільно розпоряджається ними, за винятком випадків, передбачених законами і міжнародними договорами» (ст.53); у ст.54 зазначалось, що «інформаційний суверенітет України забезпечується: виключним правом власності України на інформаційні ресурси, що формуються за рахунок коштів держа-

вного бюджету; створенням національних систем інформації; встановленням режиму доступу інших держав до інформаційних ресурсів України; використанням інформаційних ресурсів на основі рівноправного співробітництва з іншими державами», проте у новій редакції Закону вказані положення не знайшли відображення.

Приймаючи нову редакцію Закону України «Про інформацію», що набула чинності 9 травня 2011р., законодавцем було враховано висновки експертів Ради Європи та вилучено поняття «інформаційний суверенітет», що, на їх думку «не належить до принципів, вжитих хоча б в одному договорі про захист прав людини» [5]. Вважаємо, що в даному випадку йдеться власне про недоречність визначення вказаного поняття саме у Законі України «Про інформацію», оскільки складність концепту інформаційний суверенітет та необхідність його забезпечення вимагає окремого нормативно-правового акту.

Загалом, аналіз стану правового регулювання питання забезпечення інформаційного суверенітету у національному законодавстві свідчить про суттєві прогалини, що ускладнює подальший розвиток та удосконалення законодавства в інформаційній сфері, процес формування та розвитку інформаційного суспільства.

Іноземна практика вказує на диверсифіковані підходи до правової регламентації вказаного питання, що обумовлено різного роду факторами – типом правової системи, видом державно-правового режиму, рівнем інформаційно-технологічного розвитку держави тощо.

Однією із засторог правової регламентації поняття «інформаційний суверенітет» вважають те що, воно може порушити принцип транскордонності права доступу до інформації, яке в інформаційному суспільстві є одним із фундаментальних прав людини і громадянина та включає свободу дотримуватися своїх поглядів, одержувати і передавати інформацію та ідеї без втручання органів державної влади і незалежно від кордонів (Загальна декларація з прав людини, Міжнародний пакт про громадянські та політичні права, Європейська конвенція про захист прав людини та основоположних свобод).

Проте, на сучасному етапі найбільший інтерес до концепту «інформаційний суверенітет» та вироблення механізмів його реального забезпечення спостерігається з боку таких світових лідерів

як Росія і Китай і скоріше, сприймається ними як можливість тотального контролю в інформаційній сфері, про що свідчить правотворча діяльність у напрямі чіткої регламентації усіх дій суб'єктів в інформаційному просторі, у тому числі і кібернетичному.

Література

1. Політологічний енциклопедичний словник / упоряд. В.П. Горбатенко; за ред.: Ю. С. Шемшученка, В.Д. Бабкіна, В.П. Горбатенка. – 2-ге вид., допов. і переробл. – К.: Генеза, 2004. – С. 643.

2. Декларація керівних принципів з використання мовлення через супутники для вільного розповсюдження інформації, розвитку освіти і розширення культурних обмінів [Електронний ресурс]. — Режим доступу http://zakon3.rada.gov.ua/laws /show/995_388

3. Закон України "Про Національну програму інформатизації" від 04.02.1998 // Сайт Верховної Ради України. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/559/2011.

4. Закон України "Про інформацію" від 2 жовтня 1992 р. // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 351.

5. Висновок експертів Ради Європи щодо проекту закону про інформацію [Електронний ресурс]. — Режим доступу: http://helsinki.org.ua /index.php?id=1173882959.

УДК 343.1

Тарасенко Д. І.

Інститут підготовки юридичних кадрів для Служби безпеки України Національного університету «Юридична академія України імені Ярослава Мудрого»

ЗАПРОВАДЖЕННЯ КОМП'ЮТЕРНОЇ ІНФОРМАЦІЇ ЯК ПРОЦЕСУАЛЬНОГО ДОКАЗУ У КОНТЕКСТІ ФУНКЦІОНУВАННЯ НАЦІОНАЛЬНОЇ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ УКРАЇНИ

Інформатизація сучасного суспільства виводить комп'ютерну інформацію на рівень чи не основного джерела отримання будь-яких відомостей. Слід зауважити, що за окремими підрахунками на сьогоднішній день вже діє принаймні 148 електронних реєстрів відкритих для публічного користування громадянами України. Ці реєстри створені урядовими інституціями та охоплюють широке коло послуг для громадян: переліки

юридичних осіб та фізичних осіб-підприємців, платників податку на додану вартість, реєстр громадських об'єднань, публічна кадастрова карта тощо [1]. Міністерством юстиції України опубліковано переліки єдиних та державних реєстрів з їх держателями [2], а також створено та введено в експлуатацію систему електронних сервісів [3], яка містить Державний реєстр речових прав на нерухоме майно, Державний реєстр актів цивільного стану, Єдиний реєстр підприємств, щодо яких порушено провадження про банкрутство, систему електронної звітності арбітражних керуючих, електронний суд.

Крім того, сучасний стан поширення комп'ютерних систем у суспільному житті, існуюча тенденція заміни особистої взаємодії на рівні фізичних контактів соціальною комунікацією за допомогою соціальних мереж виводить комп'ютерну інформацію у сучасному інформаційному суспільстві на рівень чи не основного джерела відомостей про особу [1, 2]. Розвиток системи електронного урядування, як єдиної інфраструктури міжвідомчої автоматизованої інформаційної взаємодії органів державної влади та органів місцевого самоврядування між собою, з громадянами і суб'єктами господарювання [4], виводить питання забезпечення кібернетичної безпеки держави на одну з перших позиції порядку денного діяльності Держави. Крім того, як свідчить проведене у 2014 році дослідження робочої групи з урядової політики в е-урядуванні значна кількість чинних нормативно-правових актів, що регулюють відносини у сфері інформаційних технологій, потребують відповідних змін та доповнень, оскільки вони не повністю узгоджуються між собою[3]. Враховуючи, що питання забезпечення кібернетичної безпеки держави тісно пов'язано із кримінальним переслідуванням слід звернути особливу увагу на питання законодавчого забезпечення кримінального переслідування у названій сфері.

У цьому контексті використання комп'ютерної інформації у доказуванні набуває значного обсягу, водночас Кримінальний процесуальний кодекс України не передбачає особливий статус комп'ютерної інформації як окремого процесуального джерела доказу. Комп'ютерна інформаціє за своєю суттю є складним явищем. Так, В.А. Мещеряков, досліджуючи комп'ютерну інформацію, називає її складною ієрархічною структурою, яка має такі рівні:

фізичний - рівень матеріальних носіїв інформації, де інформація надана у вигляді характеристик речовини або магнітного поля;

логічний - рівень представлення складних інформаційних структур (від байта до файлу) на підставі фізичного рівня;

семантичний - рівень смислового навантаження інформації [4, с. 18.]

Автором наголошувалось, що на прийняття рішення уповноваженим суб'єктом впливає семантичний рівень інформації (рівень доказу), у той час як законодавством встановлюються правила отримання фізичного рівня інформації - допустимість доказів (рівень процесуального джерела доказу) [5]. Семантичний рівень інформації не обмежується виключно її змістом, а також включає до себе і так звану метаінформацію (наприклад, змістом інформації під час телефонної розмови є текст розмови, а метаінформацією — відомості про належність голосів конкретним особам, час та тривалість розмови, місця знаходження абонентів, номери телефонів, номери IMEI мобільних терміналів тощо). Також слід враховувати, що метаінформація може бути встановлена та сприйнята уповноваженими суб'єктами не одразу та не безпосередньо, а як наслідок проведення додаткових слідчих (розшукових) дій: огляди, призначення експертиз, допити тощо.

Зважаючи не доступність засобів та легкість модифікації логічним постає питання забезпечення цілісності отриманої комп'ютерної інформації, а також підтвердження її автентичності. На сьогоднішній день загальновизнаними засобами підтвердження цілісності комп'ютерної інформації та підтвердження її автентичності є застосування геш-функцій та електронного цифрового підпису.

Проведені американськими криптографами N. Koblitz та A.J. Menezes дослідження вказують на необхідність розробки та запровадження стійких до пост-квантового криптоаналізу алгоритмів криптографічного захисту [6]. На слабкість діючих криптосистем до пост-квантового крипто аналізу, звертають увагу і вітчизняні науковці [7]. На сьогоднішній день в Україні розроблено та запроваджено відповідні державні стандарти криптографічного захисту – алгоритми «Калина» (ДСТУ 7624-2014) та «Купина» (ДСТУ 7564-2014), які розроблялись з урахуванням вимог стійкості алгоритмів до пост-квантової криптографії.

Таким чином, на сьогоднішній день в Україні створено всі передумови для запровадження у кримінальний процес процедур вилучення та забезпечення цілісності комп'ютерної інформації як самостійного процесуального джерела доказів.

Література

1. Цехан Д. М. Використання можливостей соціальних мереж у боротьбі зі злочинністю / Д. М. Цехан [Електронний ресурс]. – Режим доступу : http://inter.criminology.onua.edu.ua/?p=3453.
2. ФБР хоче стежити за соціальними мережами в реальному часі / [Електронний ресурс]. – Режим доступу : http:// www.bezpeka.com/ua/news/2012/01/03/fbi-releases-plans-to-monitor-social-networks.html.
3. Аналітичний звіт «Нормативно-правове забезпечення впровадження електронного урядування в Україні»/ [Електронний ресурс]. – Режим доступу : http:// etransformation.org.ua/2014/07/16/121.
4. Мещеряков В. А. Основы методики расследования преступлений в сфере компьютерной информации : автореф. дис. на соискание уч. степени докт. юрид. наук : спец. 12.00.09 «Уголовный процесс; Криминалистика и судебная экспертиза; Оперативно-розыскная деятельность» / В. А. Мещеряков ; воронежский государственный университет. – Воронеж., 2001. – 39 с.
5. Тарасенко Д. І. Доказ як результат суб'єктивного сприйняття інформації // Науковий вісник Ужгородського національного університету. Серія Право – 2014. – Випуск 29. Том 2 . – С. 196-201.
6. Neal Koblitz, Alfred J. Menezes A Riddle Wrapped in an Enigma/ [Електронний ресурс]. – Режим доступу : https://eprint.iacr.org/2015/1018.pdf.
7. Горбенко Ю. І., Р. С. Ганзя, Аналіз шляхів розвитку криптографії після появи квантових комп'ютерів / Ю. І. Горбенко, Р. С. Ганзя [Електронний ресурс]. – Режим доступу : http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe%3F21 COM%3D2%26I21DBN%3DUJRN%26P21DBN%3DUJRN%26IMAGE_FILE_DOWNLOAD%3D1%26Image_file_name%3DPDF/VNULPKSM_2014_806_9.pdf

УДК 341.824:338.47 (043.2)

Ткаченко О. П.
Національна академія СБ України

ОСОБЛИВОСТІ ОРГАНІЗАЦІЇ МІЖНАРОДНОГО СПІВРОБІТНИЦТВА ОРГАНІВ ТА ПІДРОЗДІЛІВ СБ УКРАЇНИ В КОНТЕКСТІ РОЗБУДОВИ НАЦІОНАЛЬНОЇ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ УКРАЇНИ

Служба безпеки України, у партнерстві із іншими правоохоронними органами нашої країни, органами державної влади та управління, а також приватним ІТ сектором, активно співпрацює із іноземними партнерськими спеціальними та правоохоронними органами, представництвами міжнародних організацій та фондів у сфері забезпечення інформаційної безпеки держави, протидії кіберзагрозам, зокрема кібертероризму.

Серед найактивніших іноземних партнерів Служби безпеки України у протидії кіберзагрозам виступають спецслужби таких країн-членів НАТО: США, Великої Британії, Румунії, Франції, Естонії, Німеччини, а також таких країн як Республіка Корея тощо. [1]

Аналіз отриманих у 2015 році матеріалів вказує на значну, у порівнянні з 2014 роком, активізацію міжнародного співробітництва по лінії протидії кіберзагрозам.

Зокрема, протягом вказаного періоду провідні міжнародні організації та структури (ОБСЄ, Рада Європи, НАТО, ООН,ЄС) вживають активних заходів щодо вироблення спільної міжнародної політики у сфері протидії кіберзагрозам.

Найбільш активною у цьому плані є ОБСЄ яка упродовж 2013-2015 років намагається втілити в життя затверджені наприкінці 2013 року так звані заходи зміцнення довіри у сфері забезпечення кібербезпеки.

Відповідні заходи відбуваються у рамках роботи неформальної Робочої групи ОБСЄ з питань ЗЗД з вироблення заходів зі зміцнення довіри у сфері інформаційно-комунікаційних технологій. До останнього моменту головною перепоною на шляху вироблення спільної позиції була політика Російської Федерації, яка через певні невідповідності національного законодавства (наприклад принцип екстериторіальності) не погоджувала спільні пропозиції.

Водночас, завдяки досягнутому компромісу із представництвом США при ОБСЄ та безпосередньої участі головуючої у 2016 році в ОБСЄ Німеччині, 12 лютого 2016 року, в ході чергового засідання вищезазначеної Робочої групи, комплекс заходів у сфері протидії кіберзагрозам, був погоджений всіма членами Робочої групи в т.ч. представником РФ при ОБСЄ. [2]

Служба безпеки України регулярно бере участь у засіданні вказаної групи. Позиція СБ України врахована при підготовці проекту спільних ЗЗД країн-членів ОБСЄ.

Співробітництво СБ України з Північноатлантичним альянсом у сфері забезпечення кібербезпеки упродовж 2014-2015 років значно активізувалося. Так, відповідно до рішення штаб-квартири НАТО в Брюсселі у вересні 2014 року створено Трастовий Фонд Україна-НАТО з питань кіберзахисту, спрямований на розширення можливостей України у сфері забезпечення кібербезпеки. Наразі в рамках вказаного Трастового Фонду реалізується низка проектів спрямованих на підвищення освітнього рівня та технічного оснащення спеціальних та правоохоронних органів держави у сфері кіберзахисту.

Окрім того партнерами з Північноатлантичного Альянсу запропоновано до реалізації низку проектів у сфері протидії кіберзагрозам головним партнером у яких виступає Служба безпеки України. Окрім того, Альянс направив до Служби безпеки України радника з питань кібербезпеки, який надає методичну та консультативну допомогу у цій сфері. [3]

Активним є і співробітництво Служби безпеки України з європейськими організаціями у сфері протидії кіберзлочинності.

Зокрема, представники ДКІБ СБ України регулярно беруть участь у роботі Комітету Конвенції Ради Європи з кіберзлочинності. В ході останнього засідання Комітету, яке відбулося у м.Страсбург у грудні 2015 року зусилля України щодо імплементації положень Конвенції у національне законодавство отримали позитивну оцінку країн-учасників Конвенції та керівництва Комітету [4].

Окрім того СБ України бере активну участь у проектах Ради Європи. Зокрема з вересня 2015 року регулярно беруть участь у засіданнях проекту «CyberCrime EAP», спрямованого на покращення рівня міжнародного співробітництва у сфері боротьби з транснаціональною кіберзлочинністю у країнах Східного Партнерства (Азербайджан, Білорусь, Вірменія, Грузія, Молдова, Україна).

Упродовж 2015 року значно активізувалося співробітництво СБ України з міжнародними партнерами в рамках Організації за демократію та економічний розвиток ГУАМ. Зокрема, саме Службою безпеки України ініційовано створення в структурі Секретаріату ГУАМ окремої Робочої групи з протидії кіберзагрозам. Вказана ініціатива підтримана всіма країнами членами Організації (Грузія, Азербайджан, Молдова). Наразі країнами-учасницями Робочої групи опрацьовується текст Меморандуму про співробітництво, для винесення на затвердження Раді керівників міністерств закордонних справ ГУАМ.

Вбачається, що одним з чинників, що заважає ефективному міжнародному співробітництву по лінії протидії загрозам в інформаційній сфері є розбіжність у законодавстві різних країн, особливо у визначенні, що є злочином, відповідальності за скоєні правопорушення.

Наступним суттєвим недоліком законодавчого характеру є невідповідність системи збору доказової бази, а також того, що саме є доказом в Україні та інших країнах світу. Найчастіше ця проблема виникає в ході документації комп'ютерних злочинів за результатами спільних операцій з правоохоронними та спеціальними органами Сполучених Штатів Америки, де, наприклад, документальне оформлення показів постраждалої сторони суттєво відрізняється від аналогічного в Україні і не може слугувати доказом в українському судочинстві [5].

Окрім того останнім часом з боку профільних структур Ради Європи, зокрема, Комітету Конвенції РЄ з кіберзлочинності озвучуються претензії до низки країн в т.ч. України щодо відсутності прогресу в імплементації окремих положень Конвенції в національне законодавство. На думку Ради Європи вказане заважає ефективному міжнародному співробітництву у сфері протидії кіберзагрозам.

В цьому контексті вбачається за доцільне звернути увагу на проблему функціонування контактного пункту 24/7 Конвенції Ради Європи з питань кіберзлочинності.

Вказаний пункт було створено в структурі СБ України за сприяння ФБР Сполучених Штатів Америки у 2009 році з метою оперативного обміну інформації щодо скоєних або запланованих злочинів у кіберпросторі. У 2011 році відповідно до прийнятого ВР Україною законодавчого акту вказаний пункт було передано до МВС України. [6]

З вказаного періоду часу іноземні партнерські спецслужби періодично висловлюють претензії щодо неможливості в режимі реального часу повідомити спецслужби України щодо виявлених кіберзагроз.

Наприкінці 2015 року Комітет Конвенції Ради Європи з кіберзлочинності провів тестування роботи вказаних контактних пунктів направивши пробне повідомлення про запланований злочин у кіберсфері з проханням надати певну інформацію. Україна опинилася в списку країн які взагалі не відповіли на запит Комітету.

Вбачається, що відсутність можливості доступу СБ України до вказаного контактного пункту 24/7 суттєво впливає негативним чином як на міжнародне співробітництво у сфері забезпечення кібербезпеки так і на імідж України як послідовного партнера у боротьбі із загрозами світового масштабу, зокрема кіберзагрозами.

Література

1. Організаційно-правові засади захисту національної інфраструктури України від кіберзагроз / [Довгань О.Д., Климчук О.О., Панченко В.М., Петров В.В., Хлевицький В.Б.]. - К. : Центр навч.-наук. та наук.-пр. видань НА СБ України, 2013.

2. Current report on the Cybersecurity building measures. [Електронний ресурс]. – Режим доступу : http://polis.osce.org/countries/details?item_id=4#ss-structure.

3. Указ Президента України “Про Про затвердження Річної національної програми співробітництва Україна – НАТО на 2016 рік" від 12 лютого 2016 року № 45/2016// Президент України [Електронний ресурс]. – Режим доступу : http://www.president.gov.ua/documents/452016-19779.

4. Cybercrime Convention Committee (T-CY) 14th Plenary Strasbourg, 1-2 December 2015, Abridged meeting report. [Електронний ресурс]. – Режим доступу: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680490af1.

5. Формування організаційно-правової системи захисту національної інфраструктури від кіберзагроз /Клімчук О.О., Панченко В.М., Петров В.В. – К.:НАН України, 2013р.

6. Дубов Д.В. Кібербезпека: світові тенденції та виклики для України : аналітична доповідь / Д.В.Дубов, М.А.Ожеван. – К.: НІСД, 2013. – 30 с.

УДК 343.543

Ткачук Н. А.
Національна академія СБ України

КІБЕРБЕЗПЕКА ЯК СКЛАДОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ ДЕРЖАВИ

Трансформація сучасних загроз національній безпеці та стрімка зміна безпекового середовища в контексті гібридної війни Російської Федерації проти України призвели до зміни пріоритетних напрямів забезпечення національної безпеки держави та перетворення кібербезпеки на один із її ключових елементів.

Беззаперечні факти агресії РФ в кіберпросторі України – кібератаки на державні інформаційні ресурси з метою блокування їх роботи [1] або розміщення недостовірної інформації [2], потужні атаки на критичну інформаційну інфраструктуру держави в секторі енергетики [3], а також численні факти використання кіберпростору для здійснення розвідувальної діяльності [4] – перетворили кіберпростір на ще один полігон ведення бойових дій, а завдання із кіберзахисту – на важливу складову забезпечення національної безпеки держави.

Нова редакція Стратегії національної безпеки України, затверджена Указом Президента України від 26 травня 2015 року № 287/2015, у відповідності до європейських кібербезпекових підходів вперше виділила кібербезпеку як самостійну складову національної безпеки України, відмежувавши її від сфери інформаційної безпеки [5].

Водночас, кібербезпека має тісний зв'язок з іншими елементами системи національної безпеки. Характерною особливістю кіберсфери є можливість реалізації загроз, які надходять з кіберпростору, у будь якому сегменті національної безпеки держави (інформаційному, військовому, екологічному та ін.), що пов’язано із проникненням інформаційно-телекомунікаційних технологій в усі без виключення сфери суспільного життя.

Наприклад, безпрецедентні кібератаки на автоматизовані системи управління ряду українських обленерго наприкінці 2015 року, що призвели до суттєвих перебоїв подачі електроенергії та знеструмлення тисяч домогосподарств [6], беззаперечно можна назвати не лише загрозою кібернетичній, а й енергетичній безпеці України.

Існує особливий зв'язок між кібернетичною та інформаційною безпекою держави. Із набуттям популярності Інтернет ЗМІ та соціальних медіа, як основного джерела отримання «достовірної інформації» [7], основні загрози інформаційній безпеці держави, зокрема, ведення інформаційної війни проти України та маніпулювання суспільною свідомістю шляхом поширення недостовірної, неповної або упередженої інформації, наразі реалізуються за допомогою кіберпростору.

Злам офіційних сайтів державних органів України з метою розміщення неправдивої та упередженої інформації, направленої на дискредитацію чинної влади та підвищення соціальної напруги свідчить, що кібератаки стають інструментом спеціальних інформаційних операцій ворожих спецслужб та можуть становити безпосередню загрозу інформаційній безпеці держави.

Зазначене продемонстрував злам російськими хакерами офіційного сайту Центральної виборчої комісії України під час проведення президентських виборів у травні 2014 року з метою розміщення інформації про, начебто, перемогу Д.Яроша, представника радикальних націоналістичних сил, що супроводжувалося миттєвим висвітленням «перемоги» російськими ЗМІ в контексті наративу про радикалізацію сучасної української влади [8].

Як зазначив Президент України П. Порошенко на засіданні РНБО України 27 січня 2016 року, – кіберпростір зараз перетворився на ще одне поле протистояння і боротьби за незалежність держави [9].

Вказане вимагає створення особливого механізму забезпечення кібербезпеки, здатного протидіяти сучасним викликам та загрозам кіберпростору. Такий механізм повинен реалізовуватись в рамках функціонування національної системи кібербезпеки України, розбудова якої на сьогодні є одним з ключових завдань безпекового сектору держави.

На нашу думку, національна система кібербезпеки є сукупністю суб’єктів забезпечення кібербезпеки, механізму їх взаємодії та координації, комплексу заходів кіберзахисту, що ними здійснюється, а також законодавства, що регламентує відносини в сфері забезпечення кібербезпеки.

Враховуючи, що ключовою особливістю кібербезпеки є тісний взаємозв’язок з усіма без виключення секторами національної безпеки держави та сферами суспільного життя, відмінною рисою національної системи кібербезпеки має стати пріоритет-

ність налагодження взаємодії між всіма її суб'єктами – державними органами, що здійснюють регулювання у сфері інформатизації та захисту інформації; органами внутрішніх справ; Збройними силами; органами безпеки; розвідувальними органами України та приватним сектором.

Для виконання завдань із забезпечення координації вказаної діяльності та оптимізації функціонування Національної системи кібербезпеки на нашу думку доцільно створити при РНБО України Національний координаційний центр кібербезпеки.

Література

1. Кибератаки в Украине. Кто и как осуществляет "штурм" сайтов [Електронний ресурс]. – Режим доступу : http://korrespondent.net/ukraine/3432734-kyberataky-v-ukrayne-kto-y-kak-osuschestvliaet-shturm-saitov.

2. Хакеры взломали сайт Нацгвардии, чтобы объявить о наступлении ПС [Електронний ресурс]. – Режим доступу : http://news.liga.net/news/politics/5091107-khakery_vzlomali_sayt_natsgvardii_chtoby_obyavit_o_nastuplenii_ps_.htm.

3. Хакери атакували низку українських обленерго [Електронний ресурс]. – Режим доступу : http://ua.korrespondent.net/ukraine/3611402-khakery-atakuvaly-nyzku-ukrainskykh-oblenerho-zmi.

4. Russian hackers target NATO, Ukraine and others: iSight [Електронний ресурс]. – Режим доступу : http://www.reuters.com/article/us-russia-hackers-idUSKCN0I308F20141014.

5. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» від 26 травня 2015 року № 287/2015 [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/287/2015.

6. Хакерские атаки на украинские облэнерго: комиссия при Минэнергоугля продолжит расследование [Електронний ресурс]. – Режим доступу : http://www.unian.net/1242874-x.html.

7. Соцмережі та новинні сайти дедалі більше витісняють традиційні ЗМІ [Електронний ресурс]. – Режим доступу : http://ipress.ua/news/sotsmerezhi_ta_novynni_sayty_vytisnyayut_tradytsiyni_zmi_25102.html.

8. Информация ОРТ о Ярошe-Президенте не ошибка, а провокация [Електронний ресурс]. – Режим доступу : http://www.ukrinform.ru/rubric-lastnews/1666930-informatsiya_ort_o_yaroshe_prezidente_ne_oshibka_a_provokatsiya_1636512.html.

9. Порошенко: кіберпростір перетворився наполе боротьби за незалежність України [Електронний ресурс]. – Режим доступу: http://www.unian.ua/politics/1248226-poroshenko-kiberprostir-peretvorivsya-napole-borotbi-za-nezalejnist-ukrajini.html.

ЗМІСТ

ВСТУПНЕ СЛОВО 3

ЕФЕКТИВНІ МЕХАНІЗМИ ВЗАЄМОДІЇ ТА КООРДИНАЦІЇ ДЕРЖАВНИХ ОРГАНІВ УКРАЇНИ В УМОВАХ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА

Аблазов І.В., Хамула С.В. Шляхи оптимізації державної інформаційної політики в Україні в умовах зовнішніх інформаційних впливів 6

Антонюк В.В. Державна інформаційна політика України у контексті забезпечення політичної безпеки 8

Горовий В.Г. Актуальні проблеми управління інформаційною безпекою держави 11

Ірха Ю.Б. Засоби масової інформації як суб'єкти протидії екстремізму в Україні 14

Кацалап В.О. Система стратегічних комунікацій Збройних сил України 18

Копан О.В., Мельник В.І. Інформаційно-психологічна війна як загроза інформаційній безпеці України 21

Крайнов В.О. Перспективні напрями удосконалення безпеки інформаційного середовища органів управління військами 24

Кудрявцев Г.В. Окремі питання діяльності військово-цивільних адміністрацій 27

Марущак А.І. Обмеження інформаційних прав громадян у зв'язку з виконанням функцій держави 30

Лашкет С.В., Матяш О.І. Громадська думка - інформаційний критерій ефективності реформ в Україні 33

Петров В.В. До аспектів становлення стратегічних комунікацій у сфері державних органів 37

Пилипчук В.Г. Система забезпечення інформаційної безпеки: проблеми формування і правового забезпечення 40

Пилипчук В.В. Комплексний підхід до забезпечення інформаційної безпеки 45

Сідак В.С. Історичні аспекти проблеми управління інформаційною безпекою держави 48

Соснін О.В. Проблеми безпеки в інформаційно-комунікаційній діяльності держави 52

Тиква В.Л. Сутність інформаційної безпеки держави, суспільства та особистості 56

Шопіна І.М. Взаємодія груп цивільно-військового співробітництва ЗСУ та суб'єктів громадянського суспільства у сфері забезпечення інформаційної безпеки 60

ПРАВОВІ ТА ОРГАНІЗАЦІЙНО-ТАКТИЧНІ АСПЕКТИ ПРОТИДІЇ РОСІЙСЬКІЙ ІНФОРМАЦІЙНІЙ АГРЕСІЇ ЯК СКЛАДОВІЙ ГІБРИДНОЇ ВІЙНИ

Андрусишин Ю.І., Радкович І. М. Психологічний захист особистості від маніпулятивних впливів в сучасних умовах інформаційного протиборства 65

Блавацька Н.М., Юрх Н.Г., Хохлачова Ю.Є., Іванченко Є.В. Управління інфокомунікаціями 68

Благодарний А.М. Особливості застосування заходів адміністративного попередження правопорушень в інформаційній сфері 70

Воскресенський В.Б., Скакун О.В., Сивобородько А.В. Портативні аналізатори спектру реального часу, як апаратні інструменти забезпечення контролю інформаційної безпеки на тактичному рівні 73

Гнатюк С.Л. Відновлення національного телерадіомовлення на тимчасово окупованих та звільнених територіях сходу України 77

Горєлов В.І., Грицюк В.М. Інформаційний вимір «гібридної війни» 80

Грищук Р.В. Спосіб оцінювання ефективності стартапу віртуальних спільнот у соціальних інтернет-сервісах за принципом критичної маси 84

Гуз А.М. Фальсифікація історії як засіб інформаційної війни Росії проти України 87

Євсєєв І.Г., Скрябін О.Л. Щодо залучення Збройних сил України в проведенні антитерористичної операції в Донецькій та Луганській областях у 2014 році: правовий аспект 91

Клименко С.В. Окремі питання кримінальної відповідальності за посягання на інформаційний суверенітет 94

Коропатнік І.М. Інформаційне забезпечення виконання бойових завдань підрозділів ЗСУ в зоні АТО групами цивільно-військового співробітництва 97

Косиєв О.А., Гриник Р.О. Інформаційна агресія як невід'ємна складова ведення гібридної війни 102

Красноступ Г.М. Прозорість медіа власності: сучасний стан та перспективи правового регулювання 104

Кудрявцев В.О. Врегулювання політичних конфліктів в умовах інформаційного протиборства (на прикладі придністровського конфлікту) 108

Куценко Д.В. Кримінальні процесуальні гарантії державної таємниці під час ініціювання питання про проведення негласних слідчих (розшукових) дій 111

Лещик Н.В. Вплив телевізійної інформації на моральне здоров'я суспільства та свідомість глядацької аудиторії 115

Ожеван М.А. Ескпертно-медійні мережі та їх роль в російських інформаційно-психологічних спецопераціях антиукраїнського спрямування 119

Олєйніков Д.О. Протидія окремим проявам інформаційної агресії в контексті ст.ст. 111 та 436 КК України..... 125

Панченко В.М. Інформаційне протиборство в умовах російської агресії проти України: оцінки західних експертів 128

Пилипенко В.М., Гриник Р.О. Особливості спецпропаганди Японії у Другій світовій війні..... 136

Присяжнюк М.М. Інформаційно-комунікаційні механізми формування іміджу України 138

Рогов П.Д., Ткаченко В.А. Стратегічні комунікації як основа підготовки та проведення інформаційних операцій..... 141

Романов М.С. Радіоелектронні засоби зв'язку та їх вплив на контррозвідувальний режим інформаційної безпеки держави 144

Савінова Н.А. Стратегії соціальних комунікацій як спосіб зниження соціальної напруги на макро-, мезо- та мікрорівнях 148

Стецишин Р.В. Проведення лекцій-бесід з молоддю, громадськістю та органами державної влади як ефективний засіб підвищення рівня правосвідомості та соціальної відповідальності населення 152

Титаренко Я.А. Особливості використання спеціальними службами Російської Федерації сил інформаційних операцій для проведення розвідувальної діяльності на території України..... 155

Тімков В.Ф. Методологічні аспекти поняття гібридної війни..... 159

Хаба Р.С. Наявні проблеми експертного оцінювання матеріалів, які поширюються в електронних, друкованих ЗМІ та Інтернеті 163

Черненко Т.В. Можливості протидії російській агресії в інформаційному полі Російської Федерації 165

Чеховська М.М., Лісовська О.Л., Крапівіна Н.В.
Інформування громадян про виникнення
надзвичайних ситуацій як фактор протидії негативним
інформаційним впливам..... 168

Шевченко М.О. Спеціальний технічний засіб
як предмет адміністративного правопорушення,
передбаченого ст. 195-5 КУпАП..... 171

РЕФОРМУВАННЯ СИСТЕМИ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ ТА СЛУЖБОВОЇ ІНФОРМАЦІЇ В КОНТЕКСТІ ЄВРОАТЛАНТИЧНОЇ ІНТЕГРАЦІЇ

Архипов О.Є. Економіко-вартісні аспекти
захисту інформації..... 176

Ботвінкін О.В. Правове та організаційне забезпечення
функціонування режиму виїзду громадян за кордон,
як складової загальнодержавної системи захисту
державної таємниці (друга половина XX століття)..... 180

Гордієнко С.Б. Система управління Інформаційною безпекою:
обґрунтування основних функцій 183

Гордієнко С.Г. Фундаментальність підготовки – необхідна
умова розуміння проблем захисту інформації
з обмеженнями у доступі та інтелектуальної власності в Україні 187

Драчук С.М. Організаційно-правова та науково-технічна
складова реформування системи охорони державної таємниці
та службової інформації в контексті
євроатлантичної інтеграції..... 190

Князєв С.О., Шлапаченко В.М. Шляхи удосконалення
нормативно-правового забезпечення процедури віднесення
інформації до категорії службової 194

Козій О.М. Формалізація подання інформаційних процесів 197

Михайлов А.А. Реформування системи охорони
державної таємниці та службової інформації
в контексті євроатлантичної інтеграції..... 199

Попутніков В.Б. Шляхи удосконалення правового та організаційного забезпечення охорони державної таємниці при здійсненні конфіденційного співробітництва 204

Семенюк О.Г. Чужа таємниця як предмет злочину 207

Сидоренко С.М. Захист секретної інформації НАТО в Румунії як умова приєднання до Альянсу 211

Сніцаренко П. М., Саричев Ю. О. Термінологічні основи інформаційного забезпечення у воєнній сфері 216

Тищенко Є.Ф. Використання спеціальних знань у кримінальних провадженнях про злочини у сфері охорони державної таємниці 220

Шлапаченко В.М. Розвідувальна діяльність як основна загроза збереженню державної таємниці 223

КОНЦЕПТУАЛЬНІ ЗАСАДИ ТА МЕХАНІЗМИ ФУНКЦІОНУВАННЯ НАЦІОНАЛЬНОЇ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ УКРАЇНИ

Баранов О.А. Правові категорії кібербезпеки 226

Буяло О.В. Моделювання процесу оцінки рівня безпеки об’єктів критичної інфраструктури 227

Гавловський В.Д. До питання підвищення ефективності забезпечення кібернетичної безпеки України 230

Даник Ю.Г. Організаційно-технічне забезпечення кібероборони держави. Основні напрями 234

Довгань О.Д. Створення системи кібернетичної безпеки України: правові колізії 238

Заєць П.М. Готовність України до викликів кібертероризму 242

Зайцев О.В., Новохатній Ю.В. Семантична інтеграція інформації з відкритих джерел Інтернет в задачах забезпечення кібернетичної безпеки 246

Ковальова Ю.В. Проблеми в сфері забезпечення кібернетичної безпеки об'єктів критичної інфраструктури 249

Козюра В.Д., Хорошко В.О., Шелест М.Є. Кібернетична безпека інформаційного суспільства: аналіз проблеми 250

Козюра В.Д., Хорошко В.О. Деякі питання щодо створення системи кібернетичної безпеки в Україні..... 253

Козюра В.Д., Хорошко В.О. Комп'ютерні технології та злочинність 257

Лук'янчук Р.В. Державні гарантії забезпечення кібернетичної безпеки в умовах сьогодення..... 260

Меленті Є.О. Можливі шляхи підвищення рівня кібернетичної безпеки України..... 263

Мовчан А.В. Кібернетична безпека – важлива складова забезпечення національної безпеки України..... 266

Олешко О.А. Проблема створення системи забезпечення національної безпеки України в інформаційній сфері 270

Слонов М.Ю. Алгоритм виявлення раціональних напрямів удосконалення функціонування кібернетичної безпеки держави..... 272

Солодка О.М. Щодо визначення поняття «інформаційний суверенітет»..... 275

Тарасенко Д.І. Запровадження комп'ютерної інформації як процесуального доказу у контексті функціонування національної системи забезпечення кібернетичної безпеки України 278

Ткаченко О.П. Особливості організації міжнародного співробітництва органів та підрозділів СБ України в контексті розбудови національної системи забезпечення кібернетичної безпеки України 282

Ткачук Н.А. Кібербезпека як складова національної безпеки держави 286

Електронна версія наукого видання на CD-ROM

АКТУАЛЬНІ ПРОБЛЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ

VII науково-практична конференція

Збірник матеріалів
(Київ, 18 березня 2016 року)

У двох частинах

Частина 1

Авторська редакція

Технічне редагування, макетування: *Вишневська О. С.*

Один електронний оптичний диск (CD-ROM)
Об’єм даних 1,8 Мб. Тираж 150 прим.

Видавець і виготовлювач
Національна академія Служби безпеки України,
вул. Трутенка,22, Київ, 03022
факс: (044) 257-30-35
E-mail: academy@ssu.gov.ua
Свідоцтво суб’єкта видавничої справи ДК № 99 від 23.06.2000