**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
**ІНСТИТУТ МОДЕРНІЗАЦІЇ ЗМІСТУ ОСВІТИ**
**МІНІСТЕРСТВО ІНФОРМАЦІЙНОЇ ПОЛІТИКИ УКРАЇНИ**
**НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ**
**НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ІНФОРМАТИКИ І ПРАВА НАЦІОНАЛЬНОЇ АКАДЕМІЇ ПРАВОВИХ НАУК УКРАЇНИ**

# АКТУАЛЬНІ ПРОБЛЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ

**IX Всеукраїнська науково-практична конференція**

**Збірник тез наукових доповідей**
**(Київ, 30 березня 2018 року)**

*Електронна версія*

Київ
2018

УДК 341.123(045)(0.034.2PDF)

**Організаційний комітет конференції:**

***Кудінов С.С.*** – голова організаційного комітету конференції, ректор Національної академії СБ України, кандидат юридичних наук, доцент; ***Золотухін Д.Ю.*** – співголова, заступник Міністра інформаційної політики України; ***Пилипчук В.Г.*** – співголова, директор Науково-дослідного інституту інформатики і права НАПрН України, доктор юридичних наук, професор, член-кореспондент Національної академії правових наук України, заслужений діяч науки і техніки України; ***Спірін О.М.*** – співголова, в.о. директора Інституту модернізації змісту освіти Міністерства освіти і науки України, доктор педагогічних наук, професор; ***Фальченко С.Л.*** – проректор з наукової роботи Національної академії Служби безпеки України, кандидат юридичних наук, доцент; ***Довгань О.Д.*** – перший заступник директора Науково-дослідного інституту інформатики і права НАПрН України, доктор юридичних наук, старший науковий співробітник; ***Чорний Р.Л.*** – директор науково-організаційного центру Національної академії Служби безпеки України, кандидат юридичних наук, старший науковий співробітник; ***Мамченко С.М.*** – директор Навчально-наукового інституту інформаційної безпеки Національної академії Служби безпеки України, доктор педагогічних наук, професор; ***Муратов О.Є.*** – заступник директора центру – начальник організаційно-наукового відділу Науково-організаційного центру Національної академії Служби безпеки України, кандидат технічних наук, старший науковий співробітник; ***Панченко В.М.*** – заступник директора інституту (з навчальної і наукової роботи) Навчально-наукового інституту інформаційної безпеки Національної академії Служби безпеки України, кандидат технічних наук, старший науковий співробітник; ***Дашковська О.В.*** – старший науковий співробітник відділу модернізації вищої освіти Інституту модернізації змісту освіти Міністерства освіти і науки України, кандидат хімічних наук, доцент; ***Макобрій О.О.*** – головний спеціаліст сектору стратегічних комунікацій Міністерства інформаційної політики України; ***Давидова Т.О.*** – старший науковий консультант організаційно-наукового відділу Науково-організаційного центру Національної академії Служби безпеки України, кандидат юридичних наук

**Актуальні** проблеми управління інформаційною безпекою держави : зб. тез наук. доп. наук.-практ. конф. (Київ, 30 березня 2018 р.) [Електронне видання]. – Київ : Нац. акад. СБУ, 2018. – 408 с.

У збірнику висвітлюються актуальні проблеми забезпечення інформаційної та кібернетичної безпеки України та науково-практичні підходи до їх вирішення. Розглядаються питання формування системи забезпечення кібернетичної безпеки України, розвитку стратегічних комунікацій в Україні, удосконалення вітчизняного законодавства у сфері охорони державної та службової інформації, 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 поділяти думку авторів.

# ВСТУПНЕ СЛОВО
## ректора Національної академії Служби безпеки України кандидата юридичних наук, доцента, Кудінова Сергія Сергійовича

Уже традиційно Національна академія Служби безпеки України зустрічає учасників щорічної всеукраїнської науково-практичної конференції *«Актуальні проблеми управління інформаційною безпекою держави»*.

Цього року ми продовжуємо роботу конференції за трьома актуальними для нашої держави напрямами, а саме: державно-правові проблеми забезпечення інформаційної та кібернетичної безпеки; захист інформації з обмеженим доступом; стратегічні комунікації.

Так, одне з найбільших аналітичних агентств світу McKinsey за підсумками минулого року визначило ключові пріоритети, що впливають сьогодні на світові тенденції, зокрема Big Data, тобто аналітика масивів даних, і кібербезпека. Власне, технології Big Data спричинили появу нових загроз національній безпеці в інформаційній сфері, оскільки хакери досить успішно застосовують їх у своїх злочинних цілях. І ми ще два роки тому передбачали таку загрозливу тенденцію, коли під час конференції говорили про проблеми захисту державних електронних інформаційних реєстрів.

Україна продовжує вживати рішучих заходів на напрямі протидії сьогоденним загрозам і формування національної системи кібернетичної безпеки. Зокрема, у жовтні 2017 року підписано Закон України «Про основні засади забезпечення кібербезпеки України», яким визначені об’єкти кібербезпеки, кіберзахисту та критичної інфраструктури, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, а також повноваження суб’єктів їхнього забезпечення та засади координації їхньої діяльності. У січні 2018 року на базі СБ України спільно з НАТО відкрито перший Ситуаційний центр забезпечення кібербезпеки, ключовими можливостями якого є запобігання кібератакам, встановлення їхнього походження та формування пропозицій із протидії їм. У лютому цього року Державною службою спеціального зв’язку та захисту інформації відкрито Центр реагування на кіберзагрози, який порівнюють із першою лінією оборони держави від кіберагресій. Водночас шляхи реалізації нових законодавчих норм потребують подальшого наукового вивчення.

За останні роки, внаслідок російської агресії, фіксується суттєве збільшення посягань на схоронність державної таємниці з боку іноземних спецслужб, переважно Російської Федерації, їхніх представників та осіб, які співпрацюють з маріонеточними «ЛНР-ДНР». Тому особливої актуальності набувають питання правових та організаційних засад охорони державної таємниці в районах проведення антитерористичної операції (сьогодні – операція об'єднаних сил). Зокрема, наукового вирішення потребують проблеми організації взаємодії та координація суб'єктів охорони державної таємниці, допустимих рамок обмеження прав і свобод людини та громадянина у процесі охорони державної таємниці при здійсненні контррозвідувальних та оперативно-розшукових заходів тощо. Науково обґрунтувати необхідно також питання інституалізації суб'єктів стратегічних комунікацій, запровадження системи підготовки та підвищення кваліфікації фахівців у цій сфері.

Для нас, як вищого навчального закладу, зазначені завдання є дороговказом при формуванні освітніх програм. Так, сьогодні Академією здійснюються заходи із запровадження нової спеціальності – «256.04 Національна безпека (забезпечення державної безпеки в інформаційній сфері)», що дасть змогу укомплектувати сектор безпеки та оборони висококваліфікованими фахівцями зі спеціальною підготовкою.

Крім того, відповідно до потреб оперативно-службової діяльності СБ України запроваджено підвищення кваліфікації фахівців за напрямом контррозвідувального забезпечення кібербезпеки держави. Продовжується здійснення підвищення кваліфікації співробітників із захисту персональних даних та стратегічних комунікацій – і на сьогодні проведено вже дванадцять потоків для різних категорій співробітників СБ України. Щиро дякуємо всім провідним науковим установам і вищим навчальним закладам, які долучаються до співпраці з нами в цій сфері.

Сподіваюся, що цьогорічна дискусія стане ще більш конструктивною за попередні і сприятиме подальшому вдосконаленню державної політики у сфері забезпечення інформаційної та кібернетичної безпеки України.

# ДЕРЖАВНО-ПРАВОВІ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ УКРАЇНИ

*УДК 621.395*

**Автушенко О.С.**
кандидат педагогічних наук, доцент
доцент спеціальної кафедри № 2
ІСЗЗІ НТУУ «КПІ ім. Ігоря Сікорського»
**Дяченко С.В.**
курсант
ІСЗЗІ НТУУ «КПІ ім. Ігоря Сікорського»

## РОЗВИТОК ТА ПЕРСПЕКТИВИ ВИКОРИСТАННЯ IP-ТЕЛЕФОНІЇ

Всього за кілька років технологія IP-телефонія значно еволюціонувала і поширення її сьогодні істотно відрізняється від колишнього. З одного боку, це обумовлено розвитком апаратних рішень, зокрема появою потужних магістральних і транзитних маршрутизаторів, потужних високошвидкісних телекомунікаційних каналів. З іншого боку, не можна не відзначити і появи таких якісно нових технологій, як динамічна маршрутизація з урахуванням якості обслуговування (QoS) в мультисервісних IP-мережах і протокол резервування ресурсів для контролю якості обслуговування транзитних маршрутизаторів (RSVP).

У даний час якість обслуговування є однією з найбільш актуальних проблем IP-телефонії. Для належної передачі голосового трафіку необхідно мінімізувати тимчасові затримки – сумарна величина затримки в мережі IP-телефонії не повинна перевищувати 50 мс. Цей фактор має навіть більш важливе значення, ніж забезпечення доставки всіх пакетів, так як, завдяки використанню сучасних звукових кодеків і адаптивної екстраполяції, користувач IP-телефонії далеко не завжди здатний помітити погіршення якості сигналу внаслідок випадання окремих пакетів. У разі ж затримки трафіку виникає дуже неприємний ефект луни.

Сучасне обладнання для передачі голосу за допомогою протоколу IP (VoIP) дозволяє забезпечувати пріоритет передачі голосового трафіку над передачею звичайних даних, отримувати прийнятну якість звукового сигналу при сильному стисненні, ефективно гасити відлуння і різні шуми.

В кінці 90-х років минулого століття одна з серйозних проблем забезпечення високої якості звукового сигналу була викликана тим, що для передачі голосового трафіку використовувалися канали загального користу-

вання. Сьогодні ж телекомунікаційні оператори, які спеціалізуються на наданні послуг IP-телефонії, застосовують тільки виділені канали з пріоритетом голосового трафіку над трафіком даних, що гарантує високу якість передачі мови. При цьому використовується відразу кілька варіантів маршрутизації голосового трафіку для кожного з тисяч напрямків [1, 2], а в разі виникнення будь-яких проблем трафік миттєво перенаправляється на інші канали.

Взагалі використання IP-телефонії дає наступні переваги:

дозволяє добитися значної економії на послугах міжміського та міжнародного зв'язку через низькі тарифи при незмінно хорошій якості зв'язку. Сучасне обладнання шлюзу IP-телефонії дозволяють забезпечувати високу надійність зв'язку;

не потрібно вихід на міжнародну АТС. Ви телефонуєте на місцевий телефон доступу;

гарантована конфіденційність, тому що весь сеанс розмови закодовані в пакетах, передача яких здійснюється незалежно один від одного, а це означає, що таку передачу неможливо перехопити;

повний контроль над витрачанням коштів на міжміські і міжнародні переговори;

можливість інтеграції філій в єдину інформаційну структуру;

можливість збільшення кількості телефонних ліній, в умовах відсутності або обмеженої технічної можливості підключення традиційної телефонії;

можливість організації відео конференцій і нарад.

На сьогоднішній день IP-телефонія – це технологія, що дозволяє використовувати будь-яку IP-мережу як засіб організації та ведення телефонних переговорів. Її використовування дозволяє нарощувати кількість включених телефонів (абонентів) та каналів поштучно, по мірі необхідності, не закуповуючи обладнання із запасом на багато років вперед. Забезпечення зв'язку на пунктах управління здешевить послуги телефонії при використанні IP-мереж з організацією IP-телефонії.

Важлива сторона застосування IP-телефонії – використання вже наявних комп'ютерних мереж. Раніше, щоб організувати зв'язок з об'єктом, доводилося купувати і встановлювати спеціальне каналоутворююче обладнання для підключення телефонних абонентів, або прокладати додаткові абонентські лінії. Тепер, з впровадженням IP-телефонії, достатньо підключити абонентський пристрій до комп'ютерної мережі і провести програмні налаштування. Тут важливий ще один момент: більшість систем автоматизації та комунікацій, на сьогоднішній день, будується з використанням Інтернет технологій: IP-протокол Інтернету. У зв'язку з цим, комп'ютерна мережа поширюється на все більшу кількість об'єктів. А це означає, що немає необхідності купувати спеціальне обладнання для орга-

нізації телефонних каналів зв'язку. Таким чином, оптимізується і приводиться до єдиної технології, а це завжди зручніше і дешевше.

**Література**

1. Maximum Transmission Unit (MTU). Мифы и рифы [Електронний ресурс]. – Режим доступу: https://habrahabr.ru/post/226807/.
2. Аспекты технологии IP-телефонии [Електронний ресурс]. Режим доступу: http://sciarticle.ru/stat.php?i=1395809787.

*УДК 621.391:519.7:510.5*

**Аппілогов С. С.**
ІСЗЗІ КПІ ім. Ігоря Сікорського
**Волошин А. Л.**
кандидат технічних наук,
ІСЗЗІ КПІ ім. Ігоря Сікорського

## ПІДХОДИ ДО ЗАХИСТУ ANDROID-ПРИСТРОЇВ В СУЧАСНИХ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ ДЕРЖАВНИХ ОРГАНІВ УКРАЇНИ ВІД ЗЛОВМИСНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Одним з центральних завдань забезпечення інформаційної і кібернетичної безпеки України є створення умов для безпечної обробки, зберігання та передачі державних інформаційних ресурсів в сучасних спеціальних інформаційно-телекомунікаційних системах (СІТС). Аналізуючи особливості функціональних задач, що вирішуються сучасними СІТС та склад використовуваних в їх складі технічних засобів, необхідно відмітити постійно зростаючий обсяг мобільних платформ (планшетних комп'ютерів, смартфонів, тощо). Це пов'язано, насамперед, з відносно невисокою вартістю, широким функціональним діапазоном, прийнятними масо-габаритними, експлуатаційними та ергономічними показниками такого обладнання. Все більшу популярність на сьогоднішній день отримують мобільні платформи, що використовують операційні системи сімейства Android (далі – Android-пристрої). Такі пристрої знаходять застосування як у якості індивідуальних засобів зберігання персональної інформації, так і як пристрої віддаленого доступу посадових осіб державних органів до ресурсів розподілених СІТС.

Широке поширення Android-пристроїв викликало підвищений інтерес до них з боку аматорських та професійно організованих хакерських груп. Так, лише протягом 2017 року зареєстровано значне підвищення активності та поширення зловмисного програмного забезпечення, спрямованого

на несанкціоноване керування такими пристроями, отримання персональних даних їх власників та використання пристроїв в злочинних цілях.

В доповіді розглядається найбільш поширене наступне зловмисне програмне забезпечення, що поширюється на Android-пристроях:

1). Зловмисне програмне забезпечення Goolian, для якого є вразливими біля 74% всіх використовуваних Android-пристроїв у світі (порядку 1,5 млрд. пристроїв).

2). Зловмисне програмне забезпечення HummingBad, яке на сьогодні поширене на біля 4,3 % всіх використовуваних Android-пристроїв (понад 85 млн. пристроїв).

3). Зловмисне програмне забезпечення StageFright, що становить актуальну загрозу для біля 48% всіх використовуваних Android-пристроїв у світі (порядку 950 млн пристроїв).

4). Зловмисне програмне забезпечення QuadRooter's, яке використовує вразливості системного програмного забезпечення процесорів Qualcomm та може бути застосовано в близько 45 % (900 млн) існуючих Android-пристроїв.

Зазначене зловмисне програмне забезпечення, як правило, непомітно для власника завантажується на Android-пристрій при встановленні програм з неофіційних каталогів та інших мережевих розташувань невідомого (сумнівного) походження, а при розгортанні на пристрої отримує рут-права та повний доступ до даних, що зберігаються на пристрої, а також до його мікрофону та камери. Як наслідок, воно може самостійно встановлювати програмні додатки, залишати позитивні відгуки їх авторам, а також завантажувати відповідні рекламні повідомлення. Крім того зловмисне програмне забезпечення може використовувати дані автентифікації власника пристрою в інших програмних додатках для виконання дій від його імені.

Складність протидії зазначеному зловмисному програмному забезпеченню полягає в особливостях застосування програмних патчів, які враховують вразливості Android-пристроїв, їх кінцевими споживачами. Так, розробник операційної системи Android компанія Google випускає патчі досить оперативно (як правило, протягом 48 годин), але випуск оновлень для Android-пристроїв здійснюється їх виробниками, а їм деколи потрібні місяці, щоб випустити навіть самий екстрений патч. Крім того, пристрої старше 18 місяців з моменту випуску, швидше за все, взагалі не отримають ніяких оновлень через особливості їх підтримки виробниками.

В доповіді розглядаються основні підходи до протидії зловмисному програмному забезпеченню в середовищі Android-пристроїв та наводяться практичні рекомендації для мінімізації ризику їх ураження для пристроїв, що використовуються для обробки, зберігання та передачі державних інформаційних ресурсів в сучасних СІТС державних органів України.

**Література**

1. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» // Відомості Верховної Ради України. – 1994. – № 31.

2. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені постановою КМУ від 29.03.2006 № 373 // Офіційний вісник України. – 2006. – № 13.

3. 950 млн устройств на Android уязвимы перед новым багом // URL: https://xakep.ru/2015/07/28/950-mln-ustrojstv-na-android-uyazvimy-pered-novym-bagom (дата звернення 23.02.2018).

4. Вся правда о QuadRooter // URL: https://blog.avast.com/ru/vsya-pravda-o-quadrooter (дата звернення 23.02.2018).

5. Android-малварь HummingBad снова проникла в Google Play и была скачана миллионы раз // URL: https://xakep.ru/2017/01/24/hummingwhale (дата звернення 23.02.2018).

6. Android-вредонос Gooligan похищает токены аутентификации и заразил более 1 млн устройств // URL: https://xakep.ru/2016/12/01/gooligan (дата звернення 23.02.2018).

*УДК 351.746*

**Баланда А.Л.**
доктор економічних наук, професор,
професор СК-12 НА СБ України

## ІНФОРМАЦІЙНИЙ ОБМІН ЯК БАЗОВИЙ КОМПОНЕНТ ЗАБЕЗПЕЧЕННЯ МІЖНАРОДНОЇ ЕКОНОМІЧНОЇ БЕЗПЕКИ

Головною метою розвитку міжнародної економічної співпраці виступає не лише економічне зростання держав-учасниць світового співтовариства, але й формування і розбудова мирних взаємовідносин, зняття напруженості у міжнародних стосунках, а також створення дієвої системи міжнародної економічної безпеки. Під міжнародною економічною безпекою пропонується розуміти систему договірних взаємовідносин міжнародного характеру та відповідних інституціональних структур, а також створених ними умов, за яких кожній державі-учасниці світового співтовариства гарантується можливість вільно обирати та упроваджувати власну стратегію захисту національних економічних інтересів. У процесі забезпечення міжнародної економічної безпеки між державами, міжнародними організаціями виникає ряд певних взаємовідносин, розвиток яких потребує безперервного і конструктивного інформаційного обміну.

Загострення більшості світових проблем економічного характеру, які ми спостерігаємо сьогодні зумовлює значну актуалізацію загроз для стало-

го людського розвитку. Дані проблеми, за виключенням питань, пов'язаних із колективною безпекою, залишалися поза сферою уваги як національних урядів, так і міжнародних організацій майже до середини минулого століття. І лише у другій половині XX століття почала складатися повноцінна глобальна інфраструктура міжнародного інформаційного обміну щодо проблем міжнародної економічної співпраці, що пов'язане, насамперед, зі зміною підходів відносно ролі держави у внутрішній та зовнішній економічній політиці. Так, виходячи з новітньої та досить популярної на той час концепції «governance», наявність певного набору ринкових механізмів регулювання, перетворювали державу з провідного гравця на ринку в рівноправного його учасника [1].

Серед наявних базових механізмів, в основу яких покладається міждержавний інформаційний обмін доцільно виділити режими (механізми) управління трансакціями, запропонований Уільямоном [2]. Його відповідна адаптація надає додаткові можливості для використання у вирішенні актуальних проблем забезпечення міжнародної економічної безпеки:

- міжнародна організація, що самостійно управляє ресурсами для вирішення своїх завдань (ієрархічний механізм);
- міжнародна організація, що функціонує в якості консультанта і арбітра (гібридний (тристоронній) механізм);
- міжнародні двосторонні угоди без спеціалізованої наглядової організації (гібридний (двосторонній) механізм);
- рамкові міжнародні багатосторонні угоди (гібридний) (багатосторонній механізм);
- мережеві організації громадянського суспільства (гібридний дво- чи тристоронній механізм);
- групи країн «за інтересами» (гібридний дво- чи тристоронній механізм);
- відсутність спеціалізованих регуляторних організацій та довготермінових угод (ринковий механізм).

Відповідь на питання щодо специфікації прав власності в контексті проблематики міжнародної економічної безпеки дозволяє змоделювати всі можливі інституціональні варіанти відповідного глобального регулювання та сформулювати аргументи вибору конкретного варіанту.

Прикладом може слугувати Міжнародна система автоматичного обміну інформацією про фінансові рахунки (Директива про заощадження (EU STD), до якої Україна приєднується у 2020 році. Оскільки процес фінансово-економічної глобалізації створив сприятливі умови для оптимізації міжнародного податкового планування, в офшорних юрисдикціях накопичилася досить значна маса неврахованих коштів (за окремими оцінками – понад 30 трильйонів доларів). Для повернення виведені кошти «на історичну батьківщину» та оподаткувати їх уряди провідних європейських держав

запровадили ефективний механізм обміну інформацією щодо реальних власників грошей в офшорах [3].

Також Україна фактично вже приєдналася до Закону FATCA ***(Foreign Account Tax Compliance Act)***, який було прийнято у США в 2010 році. Унікальність цього закону полягає у тому, що всі зарубіжні країни повинні відправляти до американської податкової служби (IRS) інформацію щодо всіх рахунків громадян США, що відкриті в цих країнах. Якщо будь-яка країна відмовляється від цього, то всі доходи, отримані їх резидентами на території США оподатковуються американським податком на репатріацію прибутку у розмірі 30%. Таким чином, уряду США вдалося примусити всі країни, що «приєдналися» надавати необхідну інформацію або ж виплачувати податок.

«Єдиний Стандарт Звітності» (Common Reporting Standard – CRS) [4] почав розроблятися на рівні країн ОЕСР ще в 2014 році і на сьогодні до нього приєдналися біля 70 країн. Він передбачає щорічний автоматичний обмін фінансовою інформацією між країнами-учасницями. Україна на сьогодні до цього стандарту не приєдналася і судячи з усього робити це не планує, що створює додаткові можливості для нанесення значних збитків державі.

Таким чином, інформаційний обмін виступає одним з найбільш важливих факторів забезпечення міжнародної економічної безпеки. Фактично діючі на сьогодні механізми інформаційного обміну є продуктом історичного процесу виникнення проблем та їх вирішення засобами, якими володіють учасники міжнародних економічних відносин, що усвідомлюють масштаби ризиків та загроз. Однак тут існує значне протиріччя, яке полягає у тому, що політичні можливості прийняття раціональних рішень в економіці є досить обмеженими, а тому вони значно обмежують можливості інформаційного обміну.

**Література**

1. Bevir M. (2011). Key Concepts in Governance. L.: SAGE Publications Ltd.

2. Williamson O. (1996). The Mechanisms of Governance. Oxford University Press.

3. The Multilateral Convention on Mutual Administrative Assistance in Tax Matters Amended by the 2010 Protocol. – [Електронний ресурс]. – Режим доступу: http://dx.doi.org/10.1787/9789264115606-en.

4. Common Reporting Standard. – [Електронний ресурс]. – Режим доступу: http://www.oecd.org/tax/automatic-exchange/common-reporting-standard/.

*УДК 351.865*
**Бєлай С. В.**
доктор наук з державного управління, професор
Київський факультет Національної академії
Національної гвардії України
**Корнієнко Д. М.**
кандидат юридичних наук
Київський факультет Національної академії
Національної гвардії України

# ІНФОРМАЦІЙНА БЕЗПЕКА СЬОГОДЕННЯ – НЕВІД'ЄМНА СКЛАДОВА ВОЄННОЇ БЕЗПЕКИ

Останні кризові події доводять, що інформаційна безпека набуває визначальну роль у воєнній сфері. Безпосередньо в військовій справі рівень інформаційного потенціалу все більшою мірою обумовлює оперативність та ефективність прийняття рішень, структуру і якість озброєнь, оцінку рівня їх достатності та взагалі – результат збройного протистояння.

Доктрина інформаційної безпеки України зазначає, що вагомою загрозою національним інтересам та національній безпеці України в інформаційній сфері є здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу Збройних Сил України та інших військових формувань, провокування екстремістських проявів, підживлення панічних настроїв, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні [1].

Стратегія національної безпеки України актуальними загрозами національній безпеці України в інформаційній сфері визначає ведення інформаційної війни проти України та відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства. Основними напрями державної політики щодо забезпечення інформаційної безпеки зазначає забезпечення наступальності заходів політики інформаційної безпеки на основі асиметричних дій проти всіх форм і проявів інформаційної агресії; створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них; протидія інформаційним операціям проти України, маніпуляціям суспільною свідомістю і поширенню спотвореної інформації, захист національних цінностей та зміцнення єдності українського суспільства; розробка і реалізація скоординованої інформаційної політики органів державної влади та ін. [2].

Воєнна доктрина України однією з головних тенденцій, що впливає на воєнно-політичну обстановку в регіоні довкола України визначає інформаційну війну Російської Федерації проти України. Воєнно-політичними

викликами, які можуть перерости в загрозу застосування воєнної сили проти України зазначає цілеспрямований інформаційний вплив з використанням сучасних інформаційних технологій, спрямований на формування негативного міжнародного іміджу України, а також на дестабілізацію внутрішньої соціально-політичної обстановки, загострення міжетнічних та міжконфесійних відносин в Україні або її окремих регіонах і місцях компактного проживання національних меншин. Одним з сценаріїв загрози воєнній безпеці України Воєнна доктрина визначає окрему спеціальну операцію Російської Федерації проти України із застосуванням військових підрозділів та/або частин, вогневих ударів, інформаційних, інформаційно-психологічних операцій (дій) у сукупності з використанням невоєнних заходів, у тому числі миротворчих сил за відсутності відповідного рішення Ради Безпеки ООН. Як основу кризового реагування на воєнні загрози та недопущення ескалації воєнних конфліктів Воєнна доктрина розглядає заходи і дії з 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 [3].

Таким чином, значущість інформаційної безпеки як складової воєнної безпеки України пояснюється залежністю реалізації найбільш важливих інтересів України у воєнній сфері від інформаційних загроз. З аналізу найбільш небезпечних загроз важливим національним інтересам України у воєнній сфері стає зрозумілим, що реалізаційною основою цих загроз є інформаційна.

За загальноприйнятою думкою поняття «інформаційна безпека» та «інформаційна війна» співвідносяться між собою так, як поняття «воєнна безпека» та «війна». Як свідчить досвід локальних війн та збройних конфліктів, в сучасній війні неможливо досягти поставлених цілей без постійного здійснення заходів інформаційної боротьби. У мирний час інформаційна боротьба стає важливою складовою потенціалу стримування противника. Крім того, значну небезпеку національним інтересам держави складає міжнародний інформаційний тероризм. Країни-члени НАТО та суміжні з Україною держави мають в збройних силах розвинені структури інформаційної боротьби, які оснащені сучасними засобами і технологіями інформаційного впливу і мають значний досвід ведення інформаційних операцій [4, с. 31].

Таким чином, ефективність своєчасного виявлення та нейтралізації розглянутих загроз національній безпеці в воєнній сфері істотно залежить від виваженості й активності заходів щодо забезпечення воєнної безпеки на інформаційному рівні.

**Література**

1. Про рішення Ради національної безпеки і оборони України від 29.12.2016 «Про Доктрину інформаційної безпеки України» : Указ Президента України 25.02.2017 № 47/2017 // База даних «Законодавство України/ ВР України. URL: http://zakon2.rada.gov.ua/laws/show/47/2017 (дата звернення 01.03.18).

2. Про рішення Ради національної безпеки і оборони України від 06.05.2015 «Про Стратегію національної безпеки України» : Указ Президента України від 26.05.2015 р. № 287/2015 // База даних «Законодавство України/ ВР України. URL: http://zakon5.rada.gov.ua/laws/show/287/2015 (дата звернення 01.03.18).

3. Про рішення Ради національної безпеки і оборони України від 02.09.2015 «Про нову редакцію Воєнної доктрини України» : Указ Президента України від 24.09.2015 № 555/2015 // База даних «Законодавство України/ ВР України. URL:http://zakon4.rada.gov.ua/laws/show/555/2015 (дата звернення 01.03.18).

4. Розробка форм і способів інформаційної боротьби при виконанні внутрішніми військами Міністерства внутрішніх справ України службово-бойових завдань (шифр «Концепт») : звіт про НДР (заключ.) 02.12.09 / Акад. ВВ МВС України ; кер. В. І. Воробйов; викон. : О. Д. Черкашин, В. Л. Петров, С. В. Бєлай [та ін.]. – Х., 2009. – 312 с. – Інв. № 160.

*УДК 351*

**Бєляков К. І.**
завідувач наукового відділу теорії, історії та філософії інформаційного права Науково-дослідного інституту інформатики і права НАПрН України, доктор юридичних наук, професор, Заслужений діяч науки і техніки України

## ЗАКОНОДАВСТВО В СЕКТОРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ТЕХНОЛОГО-ПРАВОВИЙ АНАЛІЗ

Аналіз динаміки інформаційного законодавства останніх років свідчить про його активізацію в напрямку інформаційної безпеки, як провідної інституції інформаційного права. Обумовлено це загостренням негативного інформаційного впливу та відповідних загроз національній безпеці країни в інформаційному секторі з боку РФ. Саме тому чинне національне законодавство було поповнено низкою правових актів спрямованих, по задуму їх авторів, на визначення інноваційних підходів до формування системи захисту та розвитку інформаційного простору в умовах глобалізації та вільного обігу інформації, створення розвиненого національного інформаційного простору і захист її інформаційного суверенітету. Йдеться про низку Указів Президента, що затверджували рішень РНБО : "Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації" та "Про до-

ктрину інформаційної безпеки України" (грудень 2016 р.); "Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)" (квітень 2017 р.) [1]; "Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації» (серпень 2017 р.). Останнім "здобутком" законодавця у сфері інформаційної безпеки став Закон України "Про основні засади забезпечення кібербезпеки України" (жовтень 2017 р.).

Зазначені акти визвали певну негативну рефлексію не лише засобів масової інформації, а й фахівців (практиків та науковців), як в галузі права, так й в інших напрямах пов'язаних з законотворчим забезпеченням інформаційної сфери.

Безумовно, ґенеза та новації законодавства в секторі інформаційної безпеки потребують детального, комплексного розгляду з погляду перспектив їх ефективної реалізації та можливих наслідків, що має слугувати предметом окремого дослідження та постійного моніторингу. Але в межах тез конференції уявляється не можливим надати повний обсяг проблеми, тому ми маємо намір зупинитися на окремих спільних недоліках законодавчих актів, процесу організаційно-правового забезпечення інформаційної безпеки в країні з акцентом на технологічно-правову складову окремих передбачених законодавцем заходів по їх реалізації з мінімальними коментарями.

Доволі ретельний та аргументований правовий аналіз Указу Президента про рішенням РНБО «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» було здійснено в публікаціях фахівця з міжнародного інформаційного права Андрія Пазюка [2].

Аналізуючи Указ і рішення РНБО в частині запровадження заборони Інтернет-провайдерам надання послуг з доступу користувачам мережі Інтернет до ресурсів/сервісів з метою оцінки їх відповідності законам і Конституції, а також міжнародно-правовим зобов'язанням України, стану дотримання законності при запровадженні санкцій і введенні їх в дію, допустимості, правомірність і адекватність обмежувальних заходів, їх впливу на реалізацію конституційних прав і свобод людини, вчений доходе висновку про їх невідповідність критеріям законності, обґрунтованості і пропорційності при обмеженні свободи інформації та необхідність їх скасування. В якості аргументів автор визначає невідповідність рішень РНБО, тобто й Указів Президента, положенням чинного законодавства, Конституції України (в частині принципів застосування обмежень прав людини) та нормам міжнародного права.

Підтримуючи повною мірою аргументи автора щодо такого висновку, зазначимо, що обраний законодавцем шлях створення організаційно-

правової платформи системи забезпечення інформаційної безпеки країни є безсистемним та мало ефективним.

Поряд з вказаними правовими "прогалинами" окремі положення вищезазначених, як саме й інших нормативних актів інформаційного законодавства, не враховують технологічної складової системи інформаційної безпеки країни, від якої на пряму залежать можливість та рівень ефективності передбачених ними заходів, їх реалізації, адекватність прийняття управлінських рішень щодо їх мети, реальність юридичної відповідальності за їх невиконання, а звідси й евентуальні соціально-економічні наслідки.

Так, передбачені Указом Президента «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» санкції в частині запровадження заборони Інтернет-провайдерам надання послуг з доступу користувачам мережі Інтернет до ресурсів/сервісів е відповідають не лише критеріям законності при обмеженні свободи інформації, а й технологічним можливостям.

Наприклад, доступ до популярних сервісів російського "Яндексу", відновився вже через два дні після технологічних заходів вітчизняних провайдерів, але не з того, що оператори перестали його блокувати. Це було пов’язано із технологічними маніпуляціями, організацією ряду антиблокувальних заходів у формі контр діянь – додатки Яндексу переїхали на іншу хмару і тепер живуть там (переходом із статичної на динамічну форму IP-адреси). Єдиним засобом протидії цьому і виконання вимог Закону є постійний моніторинг ситуації, що технологічно не можливо, але ж динамічна адреса міняти хоч кожний час. Фахівці Інтернет-асоціації (ИнАУ) відмічають, що "... просто через рік заблокуємо всі IP-адреси в Європі. Простіше вже відрізати Інтернет від країни. Ці догонялкі існують в усьому світі в усіх, хто підходить уводити, увести до ладу цій роботі безсистемно. Системно це теж неможливо заблокувати на 100%, але щоб воно було більш-менш ефективно, потрібно закуповувати дороге устаткування" [3].

Теж саме стосується соціальних мереж, таких як "ВКонтакте" та "Одноклассники". На жаль "революційна" спільнота не захищала своє право на інформацію, а аргументувала недоречність їх закриття в країні їх значенням як рекламної платформи та негативними наслідками для вітчизняного виробника. "Стежити за поширенням пропаганди на цьому сайті – це обов’язок СБУ або кіберпідрозділів (на які виділялися засоби з бюджету країни, з кишень платників податків), чому нездатність цих органів протистояти пропаганді в мережі повинне позначатися на звичайних людях?" – уточнюється в петиції підписаної в Україні лише 200 людьми [4].

В цьому контексті визиває подив доводи окремих "діячів"-юристів, і навіть на високому рівні. "В нашому законодавстві не передбачене обмеження доступу до сайтів без рішення суду. Тобто якщо є рішення, то доступ може бути обмежений. Іншої процедури не існує. Щодо юридичних

осіб можуть прийматися обмеження, але щодо блокування сайтів ... У нас таке поняття є, але тільки через суд. Тому мені буде цікаво подивитися, яким чином інтернет-провайдери будуть виконувати указ президента" – сказав уповноваженого Верховної Ради з прав людини Чаплига [5].

Зауважимо, що блокування інформаційних ресурсів (серверів та сайтів) в Україні легалізація за рішенням суду можлива лише згідно законодавства про інтелектуальну власність у справах про порушення авторських прав, а не як ні загалом.

Визиває подів і сумнів введення заборони на окремі російських ЗМІ в частині трансляції теле- радіо- мовлення, адже при бажанні громадяни можуть дивитися заборонені телеканали (і вони мають на це конституційне право) засобами супутникового телебачення, яке в України достатньо поширене і складає 22% від тих хто в загалі дивиться телебачення [6].

Але, треба визнати, що в цій ситуації багато провайдерів виконали (або як мінімум спробували виконати) припис РНБО, щоб не потрапити в опалу. Але, для того, щоб реальне заборонити доступ до іноземним сайтів, потрібне придбання устаткування для пакетного інспектування трафіку. Інакше елементарно залишається доступ через прокси-сервер.

Щодо пересічного споживача Інтернету, який не яким чином підпадає під санкції закону, та якого немає смислу контролювати до моменту скоєння ним інформаційного правопорушення, то справа простіше. Існує безліч технологій – спеціальних сервісів, через які можна підключатися до інших сайтів, що можуть бути заборонені й заблоковані. Тобто, ви можете переглядати будь-який потрібний вам сайт через сайт-посередник, не напряму. Звичайно, такі ресурси теж можна прикрити, але тоді це вже переросте в елементи неадекватної "кибервійни".

Наприклад, одним із самих популярних плагинов для більшості браузерів є Hola чи плагин Zenmate. Цей плагин безкоштовний, і дозволяє вибрати замість українського російський IP, а отже одержати доступ до будь-яких російських сайтів. Програма Tor, яка є анонімною віртуальною мережею, гарантує не тільки повну анонімність, але й доступ до санкційних ресурсів. У браузері Opera вбудований "турбо-режим", який також може дати доступ до "заборонених" сайтів. А одним з найпростіших розв’язків може бути використання перекладача Google. Якщо в запиті на переклад тексту вставити потрібний сайт, то відкриється шукана сторінка, пропущена через сервер у США.

Але, не зважаючи на різного плану петиції сумлінної громади та технологічну можливість, треба визнати, що обмеження кількості їх користувачів соцмереж і глядачів "ворожих" TV-каналів обумовлене не рішеннями РНБО України та, навіть, не особистим прикладом президента країни [7], а приватним рішенням користувача – свідомого громадянина, людини

з певним рівнем правової та інформаційної культури, в державі, яка прагне стати демократичною.

Окремої уваги заслуговує табу на використання спеціалізованого програмного забезпечення, виробники антивірусів "Лаборатория Касперского" та "Доктор Веб", а також бухгалтерської оболонки "1С".

Не зосереджуючи уваги на проблемах економічних втрат, які широко обговорюється а Інтернеті, лише зазначимо, що заміни цим досить популярним софтам вітчизняний ІТ ринок надати не годен. Питання заборони антивірусного програмного забезпечення адаптованого під пострадянський інформаційний простір напряму впливає на стан кіберзахисту країни. Теж саме стосується 1С-бухгалтерії, доля ринку якого в Україні становить до 80% та використовується близько 300 тисячами компаній [8].

Таким чином доцільності блокування російських Інтернет-ресурсів є сумнівною ініціативою як з юридичної, так і с правової точки зору. Співвідношення ефекту від того, що ми щось "недозаблокуємо", і з іншого боку, приєднання до "клубу" країн, які блокують Інтернет-ресурси – Росії, Північній Кореї й Китаю мабуть того не варто.

Заборона – це завжди найпростіший і самий неприємний варіант. Для країни прагнучої в Європу це неправильна тактика. Сприйняття цього світовим співтовариством однозначно стало негативним. Із пропагандою такі методи боротися не допоможуть. Із пропагандою взагалі важко боротися якісно, не скотившись на рівень агресора.

У нас є Міністерство інформаційної політики, яке похваляється тим, що не бере державних грошей. Але похвалятися потрібно не цим, а активною й ефективною політикою інформаційної контрпропаганди.

Ми впевнені, що однією з головних причин відсутності правового механізму, здатного ефективно регулювати суспільні відносини в інформаційній сфері в цілому та в секторі безпеки зокрема є брак легітимної державної інформаційної політики, як діяльності стратегічного рівня щодо внутрішніх та зовнішніх правостосунків і взаємодій, в який має бути комплексно визначені основні соціальні, організаційні, правові, методологічні, технологічні та інші засади позиції держави в процесі розвитку національної інформаційної сфери, шляхи формування та розбудови інформаційного суспільства в Україні, а також інтеграції в світовий інформаційний простір. Саме професійно формалізована державна інформаційна політика має замінити незчисленні концепції, програми, доктрини та стратегії, об’єднавши їх в єдиний законодавчий акт, і, нарешті, вирішити проблему термінологічно-поняттєвого апарату інформаційного законодавства.

**Література**

1. Указ Президента України від 15 травня 2017 року № 133/2017 "Про рішення Ради національної безпеки і оборони України «Про застосування персональних спеціа-

льних економічних та інших обмежувальних заходів (санкцій)» від 28 квітня 2017 року»" URL: http://www.president.gov.ua/documents/1332017-21850.

2. Інформаційний Інтернет-ресурс. Андрій Пазюк. Правовий аналіз Указу Президента щодо блокування доступу до ресурсів Інтернету URL: http://moe-pravo.com.ua/pravoviy-analiz-ukazu-prezidenta-shhodo-blokuvannya-dostupu-do-resursiv-internetu/.

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

4. STRANA.UA. Пользователи Вконтакте зарегистрировали петицию для Порошенко с просьбой оставить соцсеть в покое. 15:21, 16 мая 2017 URL: https://strana.ua/news/70992-polzovateli-vkontakte-zaregistrirovali-peticiyu-s-prosboj-ostavit-socset-v-pokoe.html.

5. 112.ua. В Украине можно заблокировать сайты только после решения суда, – офис омбудсмена. URL: https://112.ua/politika/v-ukraine-mozhno-zablokirovat-sayty-tolko-posle-resheniya-suda-chaplyga-390213.html.

6. ZN.UA. Без телевизора живут 3% украинцев. URL: https://zn.ua/UKRAINE/bez-televizora-zhivut-3-ukraincev-240682_.html.

7. STRANA.UA. Порошенко заявил о закрытии своей страницы "ВКонтакте". 15:48, 16 мая 2017. URL: https://strana.ua/news/71003-poroshenko-zayavil-o-zakrytii-svoej-stranicy-vkontakte.html.

8. STRANA.UA. Запретили ли на самом деле 1С в Украине. 16 мая 2017. URL: https://strana.ua/articles/analysis/71062-zapretili-li-na-samom-dele-1s-v-ukraine.html.

*УДК 342.95*

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

## УДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ АДМІНІСТРАТИВНО-ЮРИСДИКЦІЙНОЇ ДІЯЛЬНОСТІ ОРГАНІВ СБ УКРАЇНИ

Адміністративно-юрисдикційна діяльність органів СБ України представляє складну систему, що містить у собі різноманітні види суспільних відносин, пов’язаних із здійсненням безпосередніх заходів з реалізації повноважень щодо захисту державного суверенітету, конституційного ладу, територіальної цілісності, економічного, науково-технічного і оборонного потенціалу України, законних інтересів держави та прав громадян від роз-

відувально-підривної діяльності іноземних спеціальних служб, посягань з боку окремих організацій, груп та осіб, а також забезпечення охорони державної таємниці. Всі зазначені заходи потребують своєчасного, повного і достовірного інформаційного забезпечення.

В юридичній літературі під інформаційним забезпеченням, як правило, розуміється комплекс організаційних, правових, технічних і технологічних заходів, засобів та методів, котрі забезпечують у процесі управління і функціонування системи інформаційні зв'язки її елементів (суб'єктів та об'єктів) шляхом оптимальної організації інформаційних даних і знань [1, с. 531].

Інформаційне забезпечення адміністративно-юрисдикційної діяльності органів СБ України можна визначити як сукупність регламентованих чинним законодавством процесів збору, обробки, зберігання та надання інформації, необхідної для розгляду і вирішення адміністративно-правових спорів і застосування адміністративно-примусових заходів уповноваженими посадовими особами органів СБ України.

Закон України "Про інформацію" відповідно до галузевого призначення виділяє такі види інформації як: політична, економічна, духовна, науково-технічна, соціальна, екологічна, міжнародна [2]. Суб'єкти адміністративно-юрисдикційної діяльності використовують різні види інформаційного забезпечення комплексно або окремо. Головною ознакою якості службової інформації є її вірогідність і точність, кількість, цінність, повнота, корисність і своєчасність, вміння на її підставі ефективно здійснювати управлінський процес [3, с. 333]. Уповноважені посадові особи органів СБ України, здійснюючи адміністративно-юрисдикційну діяльність, використовують усі види інформації, тому що для вирішення поставлених завдань, їм потрібні різноманітні відомості.

Робота з інформацією має будуватися на певних принципах, основними з яких відповідно до ст. 2 Закону України «Про інформацію» є гарантованість права на інформацію; відкритість, доступність інформації, свобода обміну інформацією; достовірність і повнота інформації; свобода вираження поглядів і переконань; правомірність одержання, використання, поширення, зберігання та захисту інформації; захищеність особи від втручання в її особисте та сімейне життя [2].

Інформаційне забезпечення адміністративно-юрисдикційної діяльності здійснюється поетапно. До таких етапів належать: збір первинної інформації, її накопичення, розподіл між структурними підрозділами суб'єкта управління та їх працівниками, вивчення її з різних боків, обробка, виведення висновків, підсумків, формування управлінських рішень, доведення їх до виконавців, організація контролю за виконанням [3, с. 339].

В умовах модернізації всієї системи державної влади в Україні закономірно зростає потреба в удосконаленні оперативно-службової діяльнос-

ті органів СБ України, зокрема оптимізації професійної підготовки особового складу, здійсненні системних перетворень у правовому регулюванні, а також використанні іноземного досвіду інформаційного забезпечення адміністративно-юрисдикційної діяльності. Вивчаючи зазначений досвід, потрібно виділяти найбільш ефективні й сучасні способи забезпечення інформацією, які у свою чергу можуть бути використані підрозділами вітчизняних органів державної безпеки.

Вирішення завдань сучасного інформаційного забезпечення адміністративно-юрисдикційної діяльності органів СБ України має бути досягнуто за рахунок упровадження єдиної політики інформаційного забезпечення; створення органами державної влади спільних багатоцільових інформаційних систем; створення умов для ефективного функціонування інформаційних обліків, забезпечення їх повноти, актуальності та безпеки; переоснащення відповідних підрозділів сучасною електронно-обчислювальною технікою. Вважаємо за необхідне більш чітко регламентувати механізм надання інформації правоохоронним органам, а також адміністративну відповідальність за порушення права на одержання інформації.

**Література**

1. Плішкін В. М. Теорія управління органами внутрішніх справ : підруч. / Плішкін Валентин Михайлович. – К. : НАВСУ, 1999. – 701 с.

2. Закон України від 30 жовтня 1997 року № 2658-12 «Про інформацію» [Електронний ресурс]. - Режим доступу : http://zakon4.rada.gov.ua/. (дата звернення 26.02.2018).

3. Гусаров С. М. Адміністративно-юрисдикційна діяльність органів внутрішніх справ: дис... доктора юрид. наук: 12.00.07 / Гусаров Сергій Миколайович; Ін-т законодавства Верховної Ради України. – К., 2009. – 438 с.

*УДК 004.056.5:378.1(045)*

**Богуш В. М.**
кандидат технічних наук, доцент
Національна академія СБ України

## РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ ПІДХОДІВ ДО РЕАЛІЗАЦІЇ СТАНДАРТУ ВИЩОЇ ОСВІТИ ЗА СПЕЦІАЛЬНІСТЮ «КІБЕРБЕЗПЕКА» У СФЕРІ ПІДГОТОВКИ ФАХІВЦІВ ДЛЯ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ

У 2017 році Національне агентство із забезпечення якості вищої освіти погодило стандарт вищої освіти стосовно кібербезпеки, у якому випи-

сано, чому мають вчитися та що в результаті вміти випускники за цією спеціальністю після закінчення бакалаврату [2].

Вважаємо, що при реалізації даної версії стандарту можуть виникнути деякі проблеми у зв'язку вимогами закону України про основні засади забезпечення кібербезпеки України щодо створення національної системи кібербезпеки [1], а також узгодження змісту стандарту з основними положення типового навчального плану з кібербезпеки, розробленого робочою групою консорціуму «Партнерство заради миру» [3].

Для розв'язання цих проблем при розробці освітніх програм та навчальних планів слід прийняти до уваги, що за аналогією з класичним визначенням інформаційної безпеки під кібербезпекою фактично розуміють властивість захищеності активів від загроз конфіденційності, цілісності, доступності, але в деяких абстрактних рамках – кіберпросторі, який визначається як комплексне віртуальне середовище, сформоване в результаті дій людей, програм і сервісів в глобальній мережі за допомогою відповідних мережних і комунікаційних технологій [4].

Що стосується власне забезпечення кібербезпеки, то в якості пріоритету виділена координація взаємодії між організаціями, що формують кіберпростір, самостійні дії яких не забезпечують ефективний захист від кіберзагроз. Прикладна галузь кібербезпеки є інтегрованою з поняттями інформаційної безпеки, безпеки застосувань, мережної безпеки, безпеки глобальної мережі, а також безпеки критичної інформаційної інфраструктури. Безпека застосувань визначається в відношенні програмних засобів, а також інформаційно-програмних ресурсів і процесів, що беруть участь в їх життєвому циклі. Безпека мереж пов'язана з проектуванням, впровадженням і використанням мереж всередині організації, між організаціями, між організаціями і користувачами. Безпека в глобальній мережі стосується послуг мережі та відповідних систем інформаційно-комунікаційних технологій і мереж. Безпека критичної інформаційної інфраструктури характеризує захищеність від відповідних загроз, в тому числі загроз інформаційної безпеки.

Сам процес забезпечення кібербезпеки ґрунтується на ризик-орієнтованому підході, для чого визначаються активи кіберпростору і зацікавлені сторони, загрози, рекомендації і заходи з оброблення ризиків, причому як специфічна міра застосовуються вказівки щодо координації дій та обміну інформацією.

Для вирішення завдань раціонального поводження з ризиками організації, що мають вихід у кіберпростір, повинні впровадити у себе систему управління інформаційною безпекою, ключовим фактором у реалізації якої є забезпечення гарантій того, що в організації існує і функціонує система безперервної ідентифікації, оцінювання, обробки та моніторингу ризиків, пов'язаних з її діяльністю, включаючи безпосереднє надання послуг в глобальній мережі кінцевим користувачам або абонентам.

При створенні системи управління інформаційною безпекою в організації необхідно передбачити механізми відстеження і обробки інцидентів безпеки, а також координації заходів реагування на інциденти з підрозділами CIRT, CERT, або CSIRT в державі. Заходи реагування на інциденти повинні передбачати, крім усього іншого, моніторинг та оцінювання рівня безпеки сервісів організації, які використовується кінцевими користувачами, а також надання такої підтримки зацікавленим сторонам, яка буде підвищувати результативність їх власної реакції на прояви інцидентів безпеки.

У зв'язку з наведеним вище можна визначити, наприклад, відповідно до типового навчального плану з кібербезпеки [3] основні класи моделі професійних компетентностей у сфері підготовки фахівців для національної системи кібербезпеки.

До першого класу моделі професійних компетентностей слід віднести такі, що закладають основу наступних класів компетентностей, а також підкласів компетентностей щодо структурних компонентів кіберпростору, його основної архітектури та основ кібербезпеки та архітектури кібербезпеки. Причому компетентності щодо основ ідентифікації ризиків і управління ними повинні бути головним спільним, що зв'язує окремі компетентності і результати навчання.

У зв'язку з цим до другого класу моделі професійних компетентностей повинні входити компетентності щодо уразливостей, характерних для кіберпростору та способів і засобів для використання таких уразливостей за допомогою різних схем або векторів нападу. Розуміння даних уразливостей – невід'ємний компонент ризику і принципів зниження його рівня.

Третій клас професійних компетентностей складають компетентності щодо міжнародних організацій, політики та стандартів у сфері кібербезпеки. Вони полягають у змозі визначити роль організацій за міжнародними стандартами, аналізувати національну політику у сфері кібербезпеки в контексті міжнародних стандартів і рекомендованого досвіду, порівнювати їх з різними прикладами національних принципів, а також міжнародні правові режими кібербезпеки, що знаходяться на стадії розвитку.

До четвертого класу моделі професійних компетентностей можна віднести компетентності у сфері управління кібербезпекою на національному рівні. Це, насамперед, компетентності щодо розуміння методів управління кібербезпекою та рівнем національної готовності у сфері кібербезпеки з контекстом рамок ризику. Це можуть бути: компетентності щодо національних методів роботи, принципів дії та організації щодо кіберстійкості, планування в разі виникнення надзвичайних обставин і в процесі відновлення після кіберінцидентів, щоб звести до мінімуму пов'язану з цим дестабілізацію ситуації; компетентності щодо національних методів управління кібербезпекою, що включають заходи забезпечення кібербезпеки,

реагування на надзвичайні ситуації та мінімізацію ризику; компетентності щодо інструментів, методів і процедур у сфері кіберкриміналістики з метою збору, аналізу та інтерпретації даних з метою встановлення атрибуції і для спецслужб; компетентності щодо контролю і оцінки безпеки на національному рівні, та оцінки готовності в сфері національної кібербезпеки.

Засновуючись на наведених результатах дослідження підходів до реалізації стандарту вищої освіти за спеціальністю «кібербезпека» можна сформулювати основні компетентності та результати навчання у сфері підготовки фахівців для національної системи кібербезпеки.

Законом України про основні засади забезпечення кібербезпеки України поняття національної системи кібербезпеки трактується як організаційне об'єднання державних органів, а також сил та засобів кібербезпеки, що виконують свої функції на основі закону під контролем і захистом судової влади [1]. Основу національної системи кібербезпеки становлять Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи, особовий склад яких повинен бути підготовлений відповідно до моделей професійних компетентностей, що відповідають покладеним на них завданням.

Наприклад, для виконання завдань у системі національної системи кібербезпеки Службою безпеки України фахівці повинні бути підготовленими відповідно до таких основних професійних компетентностей: здатність описати широке коло методологічних, наукових та технічних основ побудови кіберпростору; здатність описати процеси протиборства у кіберпросторі; здатність аналізувати організацію протиборства у кіберпросторі провідних країн світу; здатність аналізувати спеціальні операції у кіберпросторі; здатність аналізувати методи та засоби розвідувальної та контррозвідувальної діяльності у кіберпросторі; здатність організовувати розвідувальну та контррозвідувальну діяльності у кіберпросторі; здатність здійснювати контррозвідувальні та оперативно-розшукові заходи у кіберпросторі.

Результати навчання повинні бути наступними: здатність до системного знання та викладення методологічних та теоретичних основ забезпечення безпеки особистості, суспільства та держави у кібернетичному просторі, що включає кібернетичну інфраструктуру, кібернетичні сервіси, соціологічні та психологічні сфери, пов'язані з діяльністю людей; володіння достатніми науковими знаннями щодо теоретичних та методологічних основ запобігання кібернетичній злочинності, кібернетичному тероризму, кібернетичним конфліктам і війнам на основі впровадження методів та експлуатації засобів забезпечення кібернетичної безпеки; здатність застосовувати стандарти, процедури та додатки для забезпечення конфіденційності, цілісності та доступності інформації та інформаційних систем; здатність використовувати системи та інструменти, необхідні для мінімізації

ризику у кібернетичному просторі; здатність здійснювати організаційно-технічні заходи щодо виявлення загроз й інцидентів, реагування на інциденти та запобігання інцидентам, а також відновлення після інциденту; здатність здійснювати розроблення концепцій, проектування та реалізацію системи управління кібербезпекою.

**Література**

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

2. Перший стандарт вищої освіти стосується кібербезпеки. Нацагентство із забезпечення якості вищої освіти погодило перший стандарт вищої освіти [Електронний ресурс]. – Режим доступу : https://ligazakon.net/lawnews/doc/-NZ173112-PERSHYY-STANDART-VYSHCHOYI-OSVITY-STOSUYETSYA-KIBERBEZPEKY?type=ep.

3. Cybersecurity: A Generic Reference Curriculum (RC). Dear Partners/NATO Members, 4500-1 (OSEM PED) October 2016. – 73 p.

4. ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity. – 50 p.

*УДК. 341.824*

**Бурий С. В.**
Науково-дослідний центр Військового інституту
Київського національного університету
імені Тараса Шевченка

## ЗНАЧЕННЯ ФОРМУВАННЯ ІНФОРМАЦІЙНОЇ КУЛЬТУРИ МАЙБУТНЬОГО ОФІЦЕРА В ПРОЦЕСІ НАВЧАННЯ ЯК ЧИННИКА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ

Постіндустріальний стан людської цивілізації правомірно пов’язують з розвитком інформаційного суспільства – суспільства, рівень якого у вирішальному ступені визначається кількістю і якістю накопиченої інформації, її свободою та доступністю. Виникнення інформаційного суспільства нерозривно пов’язане з усвідомленням фундаментальної ролі інформації у суспільному розвитку, розглядом в широкому соціокультурному контексті таких феноменів, як інформаційні ресурси, нові інформаційні технології, інформатизація. В сьогоденні в основі структури розвитку управління інформаційною безпекою держави лежить інформаційна культура. Для отримання, захисту інформації у ЗСУ величезне значення має інформаційна культура офіцера, яка повинна бути сформована в процесі навчання.

Інформаційна культура, на думку М.В. Руденка. є найбільш динамічною

складовою культури управління офіцера. Прийняття кожного важливого управлінського рішення вимагає від нього врахування великих обсягів різноманітної інформації та відповідної її обробки [4, с. 68].

Найбільш узагальнені критерії, що характеризують ефективність діяльності окремого військового фахівця щодо оволодіння військовою спеціальністю, визначає М. І. Нещадим [3]. Це такі критерії:

• ступінь сформованості інтелектуальних якостей (як результат включення особистості в цілеспрямовану навчальну та наукову діяльність);

• ступінь сформованості морально-психологічних і ділових якостей (як результат включення особистості у військово-педагогічний процес, її соціалізації, самовдосконалення внаслідок створення відповідної мотиваційної основи);

• рівень виконання військовослужбовцями обов'язків (як результат практичного застосування статутів ЗС України у повсякденній діяльності та адаптації до нових її умов).

На нашу думку, наведені критерії мають високий рівень узагальненості і для об'єктивного визначення формування інформаційної культури майбутніх офіцерів їх слід розкласти до простіших показників і відповідним чином систематизувати. А високий професійний рівень виконання військовим своїх професійних обов'язків особливо у військовий час без захисту інформації неможливий. Тому рівень виконання військовослужбовцями своїх професійних обов'язків залежить від управління інформаційними потоками.

Поняття "інформаційна культура" включає дуже багато складових:

• культуру пошуку нової інформації;

• культуру читання і сприйняття інформації;

• вміння переробляти великі масиви інформації з використанням як інформаційних (комп'ютерних) технологій, так і інтелектуальних нормалізованих методик (поаспектного аналізу текстів, контент-аналізу, класифікаційного і кластерного аналізу та ін.);

• розуміння важливості міжособистісного професійного спілкування в будь-якому виді діяльності;

• прагнення до підвищення рівня комунікаційної компетентності;

• виховання в собі терпимості до чужих точок зору і думок;

• вміння знаходити партнерів по спільній діяльності з використанням для цього телекомунікаційних каналів зв'язку;

• вміння чітко і доказово викладати результати власної діяльності, в тому числі, з урахуванням рівня підготовленості цільової аудиторії;

• знання норм, що регламентують використання інтелектуальної власності [1; 2].

Управлінська культура майбутнього офіцера являє собою міру і спосіб творчої самореалізації особистості управлінця в різноманітних видах управлінської діяльності, спрямованої на освоєння, передачу і створення

цінностей і технологій в управлінні військовим підрозділом. У такому випадку критеріями управлінської культури вважаємо: аксіологічний, технологічний, особистісний та мотиваційний.

Мотиваційно-аксіологічний критерій інформаційної культури майбутнього офіцера є сукупність інформаційної культури та управлінсько-педагогічних цінностей, що мають значення і сенс у формуванні значення інформаційної безпеки держави та особистого місця офіцера в цьому процесі. У процесі опанування інформаційною культурою майбутній офіцер засвоює нові теорії та концепції інформаційних технологій, основ управління, оволодіває вміннями і навичками і в залежності від ступеню їх застосування в практичній діяльності, щодо забезпечення управління інформацією. Сьогодні більшу значимість для ефективного управління інформаційною безпекою мають знання, ідеї, концепції, бо саме вони виступають основою інформаційного управління.

**Література**

1. [Електронний ресурс]: http://www.ifap.ru/projects/infolit.htm.

2. Інформаційна культура [Електронний ресурс]: http://www.fio.vrn.ru/2005/6/4.htm.

3. Нещадим І. М. Військова освіта України: історія, теорія, методологія, практика : моногр. / І.М.Нещадим. – К., 2003. – 766 с.

4. Руденко М.В. Культура управлінської діяльності офіцера Збройних Сил України / М.В. Руденко // Збірник наукових праць Київського гуманітарного інституту Національної академії оборони України. – 2003. – № 1(32). – С. 64–72.

*УДК 519.813.3: 519.854.6*

**Бутвін Б. Л.**
доктор технічних наук, професор
головний науковий співробітник ЦНДІ ЗСУ
**Гвоздь В.І.**
кандидат військових наук
старший науковий співробітник ЦНДІ ЗСУ
**Штифурак Ю.М.**
кандидат технічних наук
КПІ ім. Ігоря Сікорського

## МЕТОДИЧНИЙ ПІДХІД ДО ВИЗНАЧЕННЯ ІНТЕГРАЛЬНОГО РІВНЯ ЗОВНІШНІХ ЗАГРОЗ КІБЕРБЕЗПЕЦІ ДЕРЖАВИ НА ОСНОВІ НЕЛІНІЙНОГО, ПАРАМЕТРИЧНОГО МЕТОДУ ЇХ ОЦІНЮВАННЯ

Визначення рівня зовнішніх загроз кібербезпеці держави є одним з важливих завдань ведення сучасних кібервійн.

У залежності від цілей зовнішні загрози кібербезпеці держави можна розділити на наступні категорії:

1. Інформаційно-психологічний вплив на свідомість суспільства (частину суспільства) або окремих людей – найчастіше користувачів соціальних мереж (y1).

2. Вплив на комп'ютеризовані системи з метою виведення їх із ладу (y2).

3. Оволодіння ресурсами системи і несанкціоноване їх використання (y3).

4. Доступ до оброблюваної конфіденційної інформації (y4).

5. Спотворення або знищення оброблюваної інформації (y5).

Задача визначення інтегрального рівня загроз кібербезпеці держави у теперішній час вирішується здебільшого на основі адитивної, мультиплікативної або адитивно-мультиплікативної згорток окремих загроз.

Оцінювання адекватності цих згорток на основі статистичного показника детермінації, Кд, показало, що його величина змінюється від 0,3 до 0,5 та явно не відповідає сучасним вимогам.

Для подолання цього обмеження пропонується використовувати нелінійну, багатопараметричну згортку окремих загроз наступного виду:

$$Y_\Sigma = F\{y_1(z_1),...,y_5(z_1)\} \quad (1)$$

Для визначення функціоналу $F$ пропонується використовувати метод групового урахування аргументів у наступному виді:

$$Y_\Sigma = a_0 + \sum_{i=1}^{N} a_i y_i + \sum_{j=1}^{N}\sum_{i\le j} a_{ij} y_i y_j + \sum_{i=1}^{N}\sum_{j\le i}\sum_{k\le j} a_{ijk} y_i y_j y_k + ... \quad (2)$$

В основі методики, що реалізує розроблений методичний підхід, лежить метод нелінійної, ієрархічної декомпозиції з використанням методу групового урахування аргументів. Методику доведено до алгоритму та програмно реалізовано мовою Java. Завдяки цьому можливий її серверний варіант експлуатації на сучасних обчислювальних комплексах.

На рис. 1 наведено результати оцінювання статистичних показників якості (адекватності) визначеного аналітичного функціоналу, що характеризують ступінь адекватності визначення інтегрального показника загроз $Y_\Sigma$:

Міра похибки: По модулю — Вихідна змінна: У

| Результати заключної обробки | Навчання | Екзамен |
|---|---|---|
| Число спостережень | 17 | 4 |
| Макс. від'ємне відхилення | -0,0336728 | -0,771292 |
| Макс. додатне відхилення | 0,0282926 | 1,00952 |
| Середній модуль помилки (MAE) | 0,0122185 | 0,769955 |
| Середньоквадратичне відхилення (RMSE) | 0,0148477 | 0,784441 |
| Сума відхилень | -1,11022E-16 | 0,323675 |
| Стандартне відхилення залишків | 0,0148477 | 0,780256 |
| Коефіцієнт детермінації ($R^2$) | 0,999833 | 0,10495 |
| Кореляція | 0,999917 | 0,38431 |

Рис. 1. Результати оцінювання статистичних показників якості (адекватності) визначеного функціоналу інтегрального показника загроз $Y_\Sigma = F\{y_1(z_1),...,y_5(z_1)\}$

Нижче наведено фрагмент аналітичного функціоналу $Y_{\Sigma} = F\{y_1(z_1),...,y_5(z_1)\}$

$Y_{\Sigma}$ = 5.71023e-05 - N10*0.0476684 + N2*1.04765
N2 = -0.000608912 + N40*0.0120267 + N3*0.988189
N3 = -0.00135242 - N394^2*0.0011441 + N4*1.00407
N4 = -0.00109531 + N41*0.0214447 + N5*0.978943
N5 = 0.000833443 - N15*0.203097 + N6*1.2028
N6 = -0.00230041 + N266*0.00515691 + N7*0.995658
N7 = -0.00681348 - N394*N8*0.00175651 + N8*1.00793
N422 = 0.396517 + "y_1, cubert"*"y_2, cubert"*1.26691
N255 = -2.6778 + N390*2.42077 - N390^2*0.262177 + N412^2*0.118124
N412 = 1.33242 + N418^2*0.177727
N390 = 0.315258 + "y_2, cubert"*N401*0.654065
N401 = -0.899726 + "y_5, cubert"*2.78085

Аналіз наведених результатів дозволяє зробити висновок, що запропонований методичний підхід забезпечує адекватність за значенням показника детермінації на рівні 0.998. Це значно перевищує адекватність найбільш поширених методів визначення інтегрального рівня загроз кібербезпеці держави.

В подальшому на основі розрахованого інтегрального показника загроз вирішується оптимізаційна, богатопараметрична, нелінійна задача з застосуванням програми OPTQuest, що забезпечує визначення раціональних вхідних впливів для управління кібербезпекою держави відповідними посадовими особами.

**Література**

1. Штифурак Ю.М. Методичний підхід до оцінювання стабільності держави (регіону) на основі нечітких когнітивних моделей / Ю.М. Штифурак // Збірник наукових праць Інституту СЗР України. – 2013. – № 6 – С. 91-99.

2. Бутвін Б.Л. Аналітична методика оцінки стабільності держави (регіону) / Б.Л. Бутвін, Ю.М. Штифурак // Збірник наукових праць Інституту СЗР України. – 2012. – № 3 – С. 132-139.

3. Бочарников В.П. Fuzzy Technology: основы моделирования и решения экспертно-аналитических задач / Б.В. Почарников, С. В. Свешников. – К. : Эльга, Ника-Центр, 2003. – 296 с.

4. Силов В.Б. Принятие стратегических решений в нечеткой обстановке / В.Б. Силов. – М. : ИНПРО-РЕС, 1995. – 228 с.

5. OPTQuest [Електронний ресурс] – Режим доступу : http://www.opttek.com/products/optquest/ – Дата доступу : травень 2014. – Назва з екрану.

6. AnyLogic [Електронний ресурс] – Режим доступу : http://www.anylogic.ru/overview. – Дата доступу : серпень 2013. – Назва з екрану.

*УДК. 004.738.52*
**Буяло О.В.**
кандидат технічних наук, старший науковий співробітник
Воєнно-дипломатична академія імені Євгенія Березняка
**Пилипчук В.В.**
кандидат технічних наук
Воєнно-дипломатична академія імені Євгенія Березняка

# ОДИН ІЗ ШЛЯХІВ ВИРІШЕННЯ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ WEB-ДОДАТКІВ

Як тільки Web-додаток стає доступним в мережі, він робиться мішенню для кібератак. Виходячи з сучасних умов будь-який додаток незалежно від того, чи здійснюється атака цілеспрямовано зловмисниками, чи є результатом роботи автоматизованого шкідливого програмного забезпечення, буде постійно перевірятися на стійкість у відношенні безпеки [1-3]. Відповідно до цього, перед тим, як починати використовувати Web-додаток, необхідно забезпечити його захист. Одним зі шляхів вирішення проблеми забезпечення безпеки у Web- додатках є тестування. Відомо, що слабкими місцями, які зловмисники використовують для проникнення у Web- додатки є вразливості [2]. Причинами виникнення таких вразливостей може стати недостатньо добре написаний код, SQL-скрипт, або просто наявність вірусів на сервері.

Аналіз показав, що основними типами вразливостей веб-додатків є: міжсайтовий скриптінг (cross site scripting-XSS), маніпуляції з посиланнями (URL manipulation), SQL ін’єкції (SQL- injection), спуфінг (spoofing) [1-3].

В ході роботи розроблено рекомендації щодо забезпечення безпеки Web-додатків шляхом тестування на вразливості. Першим в списку можна виділити тестування паролів. Чим більш програмний продукт вимогливий до формату пароля, тим краще. У мережі достатні багато додатків для злому паролів, списків найбільш поширених паролів і імен користувачів. Неочевидним при тестуванні, але важливим елементом перевірки безпеки паролів є тестування cookies браузера. Загальна рекомендація – використовувати шифрування паролів cookies браузера. Та ж рекомендація стосується зберігання пароля в базі і при передачі пароля від клієнта до сервера. Навіть якщо за допомогою ін’єкції зловмисник дістане доступ до бази, існує можливість, що пароль він не розшифрує. Тестування паролів проводиться за допомогою перевірки тестувальником бази даних, шляхом складання запитів у відповідні таблиці, перегляд cookies браузера, і source коду сторінки. Це можна робити як простим пошуком, так і за допомогою спеціальних програм. URL маніпуляції найчастіше можливі там, де використовується метод GET HTTP-протоколу для передачі інформації між

клієнтом і сервером. Інформація передається в URL з елементами запиту в базу даних (це може бути user ID, група користувачів і ін.). Тестувальник, в такому разі, змінює ті дані в URL запиті, які відповідають запиту в базі. SQL ін'єкції досить поширений спосіб проникнення в додаток. Простим способом захисту від SQL ін'єкцій є заборона на спеціальні символи в полях введення даних, такі як ‘ =; * тобто всі ті символи, без яких неможливе виконання запиту. Разом з розробниками необхідно знайти місця в додатку, де є запити в базу з використанням призначених для користувача даних. Якщо призначені для користувача дані містять SQL запит для бази, навіть за наявності повідомлення про помилку, запит може бути виконаний, тому в цьому випадку необхідно не лише протестувати випадки SQL ін'єкцій, але і на рівні коду правильно на них реагувати. Для того щоб протестувати захист від XSS атак, необхідно переконатися що будь-які <script> елементи не приймаються додатком і не обробляються при відправленні запиту. Зловмисники мають можливість скористатися можливістю виконувати такого роду запити в полях додатка або в URL, шляхом впровадження в них скриптів. За допомогою таких скриптів існує можливість отримати доступ до інформації що зберігається в cookies.

Отже тестування безпеки у веб-додатках – це завжди тестування на злом. Метою тестування безпеки WEB-додатків повинно бути виявлення усіх можливих вразливостей. У доповіді розглянуто основні типи вразливостей та надано практичні рекомендації, щодо запобігання несанкціонованого доступу до Web-додатків.

**Література**

1. Питер Яворски Основы веб-хакинга // Lean publishing URL: http://leanpub.com/white-hat-hacking-ru.../ (звернення 27.01.2018).

2. Жуков Ю.В. Основи веб-хакинга: нападение и защита – Спб.: Питер.2011. – 176 с.

3. Веб-безпека, архів за січень, 2018// База даних Websecurity. URL: http://websecurity/com/ua...(дата звернення 10.01.2018).

*УДК 351.746.1:355.40*

**Ватраль А.В.**
кандидат юридичних наук,
докторант НА СБ України

## РОЛЬ КОНТРРОЗВІДУВАЛЬНОГО ПІЗНАННЯ У ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

В умовах зовнішньої агресії та гібридної війни проти України, особливо гостро відчувається потреба у захисті інтересів нашої держави у сфері інформаційної безпеки. Спецслужби іноземних держав активно викори-

стовують новітні інформаційні технології впливу на свідомість громадян, спрямовані на розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, насильницьку зміну конституційного ладу або порушення суверенітету і територіальної цілісності України.

Сучасна Доктрина інформаційної безпеки України визначає досить широкий перелік актуальних загроз національним інтересам та національній безпеці в інформаційній сфері, серед яких проведення спеціальних інформаційних операцій, направлених на підрив обороноздатності та деморалізацію особового складу військових формувань, провокування екстремістських проявів, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів; поширення закликів до радикальних дій, пропаганда автономістських концепцій співіснування регіонів в Україні тощо [1].

Основним інструментом забезпечення інформаційної безпеки є контррозвідувальна діяльність СБ України – одного із провідних суб'єктів реалізації державної політики України в інформаційній сфері. В свою чергу, ефективність контррозвідувальної діяльності безпосередньо залежить від результатів контррозвідувального пізнання – процесу формування достовірних знань про наявні та потенційні виклики і загрози державній безпеці (в тому числі в інформаційній сфері), умови та причини їх виникнення, а також масштаби можливих наслідків.

Аналіз особливостей контррозвідувального пізнання підтверджує, що вирішення широкого кола гносеологічних завдань дає можливість виявляти ознаки і факти розвідувально-підривної, терористичної, диверсійної та іншої протиправної діяльності спецслужб іноземних держав, а також організацій, окремих груп та осіб на шкоду безпеці держави і суспільства для їх своєчасного попередження і запобігання.

Відомо, що відправним пунктом отримання знань у будь-якій сфері суспільних відносин є інформація. Не є виключенням і контррозвідувальна діяльність. Застосовуючи спеціальні методи і засоби пізнання, контррозвідувальні підрозділи отримують і здобувають необхідну інформацію про явища і процеси, що становлять оперативну зацікавленість. В інформаційній сфері це стосується проявів обмеження свободи слова та доступу до публічної інформації, фактів поширення ЗМІ культу насильства, жорстокості, порнографії; комп'ютерної злочинності та комп'ютерного тероризму; фактів розголошення інформації з обмеженим доступом; намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації тощо.

На підставі отриманих відомостей, шляхом їх узагальнення, систематизації, аналізу та оцінки у контррозвідників формуються істинні знання, що можуть слугувати основою для створення умов та подальшої протидії внутрішнім та зовнішнім загрозам інформаційній безпеці. Такі знання

безпосередньо впливають на процес прийняття і реалізації уповноваженими суб'єктами обґрунтованих управлінських рішень у сфері забезпечення інформаційної безпеки України.

Пізнавальна діяльність в контррозвідці становить не лише систему накопичення, систематизації, аналізу і оцінки інформації для здійснення довгострокових прогнозів і планів протидії розвідувально-підривній діяльності, а і напрацювання на цій основі рекомендацій і пропозицій підвищення ефективності контррозвідувальної діяльності. Окрім цього, результати контррозвідувального пізнання утворюють можливість передбачення розвідувально-підривної діяльності не лише для її попередження і припинення, а і для перехоплення ініціативи, підпорядкування дій спецслужб іноземних держав, організацій та окремих осіб цілям і завданням контррозвідки.

Історія національних спецслужб свідчить про те, що на всіх етапах існування контррозвідувальної діяльності, пізнання як фундаментальна філософська категорія посідало важливе місце у системі забезпечення державної безпеки. Будучи складовою частиною контррозвідувальної діяльності воно відображувало процес формування знань про об'єкти контррозвідки для виявлення, попередження і припинення діяльності іноземних розвідок на шкоду інтересам України.

В сучасних умовах ведення проти України інформаційно-психологічної війни, зважаючи на уразливість державних інформаційних ресурсів до кібератак, недосконалість системи охорони державної таємниці та інші негативні фактори і чинники, пізнавальна діяльність контррозвідників як складний, безперервний, діалектичний процес формування істинних знань відіграє важливу роль у забезпеченні інформаційної безпеки. Результати контррозвідувального пізнання стають запорукою прийняття та реалізації правильних управлінських рішень щодо протидії загрозам безпеці держави в інформаційній сфері та недопущення використання інформаційного простору України в деструктивних цілях.

**Література**

1. Указ Президента України від 25.02.2017 р. №47/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України».

**Вацлавик О. М.**
Львівський державний університет безпеки життєдіяльності

## ПІДВИЩЕННЯ ОБІЗНАНОСТІ ПРО КІБЕРНЕТИЧНУ БЕЗПЕКУ

Напади на критичну інформаційну інфраструктуру стали частішими, та складнішими, оскільки злочинці впродовж останніх років були більш

професійними. Можливості своєчасного реагування та арешти злочинців є дуже обмеженими та вимогливими. Тенденція розвитку ІС для промислового використання, пов'язаного з Інтернетом, призводить до нових вразливостей цих систем. Досвід використання вірусом Stuxnet показує, що важливі промислові об'єкти не захищені від кібернетичних нападів. Кібернетична безпека залишається ключовою для підтримки функціонуючого держави в майбутньому.

Інвестиції в кібернетичну безпеку - це інвестиції в наше майбутнє та наше економічне зростання. Рівень кібернетичної безпеки складається з усіх заходів, як національних, так і міжнародних, прийнятих для захисту доступності ІКТ та цілісності, автентичності та конфіденційності даних в кіберпросторі. Кібернетична безпека повинна базуватися на складному підході, який вимагає обміну інформацією та координації дій. Під час створення системи кібернетичної безпеки необхідно забезпечити співробітництво між військовими та цивільними, громадськими та приватними, міжнародними та національними сферами. Тільки такий підхід забезпечує надійну роботу інфраструктури ІКТ у критичних областях, швидку та ефективну реакцію на кібернетичні напади та правовий захист у цифровому світі. Питання кібернетичної безпеки не може розглядатися як ізольована проблема окремих частин нашого суспільства. Це не тільки міжнародна, міжвідомча громадська або приватна сфера, а проблема всього суспільства. Тому забезпечення кібернетичної безпеки заслуговує на найвищий пріоритет.

Захист критично важливої інформаційної інфраструктури є одним з головних пріоритетів кібернетичної безпеки. Ця інфраструктура являє собою основну частину практично всіх частин критично важливої інфраструктури та стає дедалі важливішою. Як приватна, так і державна сфера мають створювати умови для тіснішої співпраці, що базується на обміні інформацією. Це буде належним чином оцінено там, де заходи безпеки будуть в повній мірі виконані, і де будуть надані додаткові повноваження у разі конкретних нападів та загроз.

Встановлення кібернетичної безпеки не може покладатися лише на технічні засоби. Належна увага повинна приділятися також кінцевим користувачам та адміністраторам систем ІКТ, працівникам з розробки, підрядникам державних контрактів, аудиторам та менеджерам. Недостатня інформація про безпеку систем ІКТ створює серйозні ризики. Відсутність кваліфікованого та обізнаного персоналу та подальша освіта підвищують вразливість та збитки.

Поінформованість громадян про кібернетичну безпеку повинна зростати через поширення відповідної інформації у співпраці з засобами масової інформації. Кібернетична безпека є частиною підготовки державних службовців, і її підтримають також у приватній сфері. Мета - досягти достатнього рівня знань для кожної позиції в галузі кібернетичної безпеки.

Співпраця, спрямована на створення навчальних програм, спрямованих на кібернетичну безпеку, розпочинається з академічної та приватної сфер. Необхідність кваліфікації в кібернетичній безпеці, можливості навчання та іншої освіти оцінюються на регулярній основі. Питання кібернетичної безпеки буде реалізовано на всіх рівнях освіти.

**Література**

1. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/96/2016

2. Шеломенцев В.П. Сутність організаційного забезпечення системи кібернетичної безпеки України та напрями його удосконалення [Електронний ресурс] – Режим доступу: http://nbuv.gov.ua/UJRN/boz_2012_2_36.

3. Дубов Д.В. Кібербезпека : світові тенденції та виклики для України [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/content/articles/files/kyber_bezpeka-aab17.pdf.

*УДК 351*

**Величко М. В.**
кандидат біологічних наук,
старший науковий співробітник,
професор спеціальної кафедри
Національна академія Служби безпеки України

## ІНФОРМАЦІЙНА БЕЗПЕКА БІОМЕДИЧНИХ ДОСЛІДЖЕНЬ: МІЖНАРОДНА ПОЛІТИКА

Наприкінці XX сторіччя вченим вдалося розробити ряд нових методів які дали можливість людині уже на рівні геному маніпулювати спадковістю живих організмів. Це відкрило додаткові можливості для біотехнології. Появились нові перспективні науки як генна інженерія, біоінформатика, синтетична біологія тощо. Одночасно людство зрозуміло, що наряду із новими преференціями у біотехнології воно отримало і нові загрози біологічного характеру. В числі перших серед міжнародних інституцій на новітні біозагрози відреагувала Всесвітня організація охорони здоров'я (ВООЗ). Стратегія біологічної безпеки та захисту ВООЗ щодо наукових досліджень в системі охорони здоров'я людини визначає на міжнародному рівні загальні рамки вимог, тобто доцільність та безпечність як для людини так і довкілля, яка схвалена і прийнята на 63-й сесії Всесвітньої асамблеї охорони здоров'я в резолюції WHA63.21 від 2010р.[1].Зазначене в першу чергу було пов'язане з тим фактом, що у XXI сторіччі, дослідни-

ки вийшли на істотно новий рівень коли із неорганічних хімічних речовин шляхом складного синтезу створили штучний білок, а потім і мікроорганізм в цілому. Розробили технології для передбачуваної генетичної модифікації або створення організмів із заданими ознаками або їх біологічних компонентів. Тобто, виникла нова наука – синтетична біологія. Хоча синтетична біологія спрямована переважно на корисні та законні цілі для людства, одночасно вона несе в собі і великі ризики в разі їх недооцінки не тільки здоров'ю та довкіллю, а і знищення всього живого (біоти) в цілому в разі злочинних намірів її застосування. Тобто, синтетичних біологічних технологій та технології редагування геномуCRISPR, «направленої людиною еволюції» та автоматизований біологічний дизайн тощо. У 2016 році директор Національної розвідки Джеймс Клеппер, в своїй щорічній доповіді Конгресу США стосовно оцінки викликів американській національній безпеці в розділі обговорення терористичних загроз від зброї масового знищення щодо біологічної - то пріоритет віддав новій біотехнології редагування геному CRISPR, зазначивши при цьому необхідність інформаційного обмеження доступу до неї (Clapper J.E., 2016) [2]. Одночасно у листопаді 2016 року у звіті Ради Радників з питань технології при Президентові США на тему: «Заходи, що необхідні для захисту США від біологічної атаки противника» (PCAST, 2016) [3] який, підготовлений консультативною групою JASON, потенційні ризики біотехнології CRISPR синтетичної біології також були визнані пріоритетними. Рівень сучасної американської біозахищенності, компетентність як урядових так і спеціальних служб і структур, технічна оснащеність, наукове та інформативне супроводження зазначеної проблематики, фінансування наразі є на порядок вищим від інших високо розвинутих країн. І їхнє бачення загроз від відкритості та доступності до результатів синтетичної біології, вже не кажучи від безпосередніх ризиків біологічного характеру таких біомедичних досліджень є авторитетним і заслуговує на увагу в тому числі і в Україні щодо покращення національної системи біобезпеки та біозахисту.

Незважаючи на те, що міжнародна Рада наукових редакторів (CSE), завданням якої є сприяння у впровадженні передового досвіду стосовно поширення наукової інформації результатів біомедичних досліджень, видала і опублікувала офіційний документ, який містить також розділ, де конкретно зазначається про відповідальність хоча б етичну перед світовою спільнотою в разі оприлюднення як відомих колу осіб, що мають до неї доступ так і нової з ознаками "подвійного використання" на думку американських фахівців на даний час є недостатнім. Так цей документ рекомендує редакторам "підвищувати професійний рівень безпекового характеру у членів редакції журналів, рецензентів та авторів; впроваджувати методи скринінгу для визначення досліджень потенційного "подвійного використання", що можуть становити загрозу в разі їх застосування із зло-

чинними намірами або ненавмисного вивільнення у довкілля в результаті надзвичайної події; залучати високого рівня фахівців не тільки по профілю наукової діяльності, але і щоб вони також були з досвідом експертів у питаннях біобезпеки та біозахисту, щоб отримувати високої якості та гарантованої безпечності рецензії наукових робіт; створювати та розширювати мережі постійного обміну досвідом і далі вдосконалювати систему управління ризиками від запланованих досліджень "подвійного використання", що можуть бути небезпечними для суспільства;і розробити рекомендації та процедури, що дозволяють проводити наукову оцінку, а також оцінку можливого ризику передачі інформації з потенціалом "подвійного використання" (Council of Science Editors (CSE), 2009) [4]. З появою новітніх біотехнологій по типу CRISPR, американці прийшли до висновку не тільки щодо необхідності вдосконалення міжнародної системи моніторингу та обмеження доступу до результатів біомедичних досліджень, які можуть містити ризики «подвійного використання», але і виокремлення нового напрямку міжнародного законодавства – біологічне законодавство з складовою кримінального переслідування за злочини у сфері біотехнологій в тому числі і за правопорушення інформаційного регулювання доступу до них.

Таким чином світова наукова спільнота акцентує увагу на те, що поряд з потенційними перевагами синтетичної біології, виникають і ряд питань, пов’язаних з біобезпекою і лабораторним біозахистом та можливими потенційними ризиками в разі біомедичних досліджень у сфері синтетичної біології, а також безліч етичних, соціальних і правових проблем з приводу наслідків досліджень для суспільства, громадського здоров’я та навколишнього середовища (The European Groupon Ethicsin Scienceand New Technologies to the European Commission, 2010) [5].

Отже, наведені випадки свідчать про наявність проблемних питань не тільки на національному рівні, але також як для ЄС, так і в цілому світової спільноти.

Підсумовуючи, вважаємо за доцільне звернути увагу міжнародних законодавців на необхідність розширення дії правового поля «Положення ЄС, щодо експортного регулювання технологій, матеріалів подвійного використання» включивши і контроль через національні комісії з питань біобезпеки та біозахисту за відкритими публікаціями наукових досягнень у сфері біологічних та хімічних наук (зважаючи на їх конвергенцію в останній час) з урахуванням синтетичної біології.

Щодо України, то вважається за доцільне, запозичивши зарубіжний досвід, враховуючи національні особливості, розробити алгоритм для оцінки стану наявної державної системи з біобезпеки та біозахисту, в тому числі і управління ризиками, пов’язаними з досягненнями світової синтетичної біології. Потім оцінити сучасний рівень біозагроз національній

безпеці України в умовах останніх наукових біотехнологічних досягнень та визначити сфери вразливості, а також окреслити пріоритети для вирішення цих проблем.

**Література**

1.Електронний ресурс-режим доступу: http://www.who.int/rpc/research_strategy /en/index.htm 1, accessedOctober 2010).

2. Clapper, J.E. 2016. WorldwideThreatAssessmentofthe U.S. IntelligenceCommunity. StatementfortheRecordbyJames R. Clapper, DirectorofNationalIntelligence. SenateArmedServiceCommittee, February 16, 2016. Availableat: https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf. AccessedonMay 19, 2017.

3. PCAST (President'sCouncilofAdvisorsonScienceandTechnology). 2016. ActionNeededtoProtectAgainstBiologicalAttack. November 2016. Availableat:

https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast _biodefense_letter_report_final.pdf. AccessedonMay 11, 2017.

4. Council of Science Editors (CSE). White paper on promoting integrity in scientific journal publications. March 2009.

5.TheEuropeanGrouponEthicsinScienceandNewTechnologiestotheEuropeanCommission. Ethics of synthetic biology. Opinion No 25, Brussels, 17 November 2009, Luxemburg, European Union, 2010.

*УДК 378.016:004.056.5*

**Воскобойніков С. О.**
кандидат педагогічних наук
Національна академія СБ України
**Кащук В.І.**
Національна академія СБ України

## ФОРМУВАННЯ ПРОФЕСІЙНОЇ КОМПЕТЕНТНОСТІ СУЧАСНОГО ФАХІВЦЯ З КІБЕРБЕЗПЕКИ ДЛЯ РЕАЛІЗАЦІЇ КОМПЕТЕНЦІЙ КОМП'ЮТЕРНОЇ КРИМІНАЛІСТИКИ

Кримінолого-криміналістична кваліфікація порушень у галузі комп'ютерних технологій є однією зі складових процесу формування фахової компетентності майбутніх фахівців з кібербезпеки.

У сучасному світі створення інформаційних ресурсів, обробка, систематизація та їх розподіл забезпечують ІТ-технології. Середовище обміну інформаційних потоків формують комп'ютерні мережі та телекомунікації. Їх застосування поширюється і на об'єкти критичної інфраструктури таких галузей, як енергетика, транспорт, банки і фінанси, інформаційні тех-

нології та телекомунікації, охорона здоров'я та інші, що є стратегічно важливим для функціонування і безпеки суспільства, держави та економіки, виведення з ладу або руйнування яких може мати вплив на національну безпеку і оборону та нанесення шкоди державі.

За визначенням американських науковців (Д. Айков, К. Сейгер та У. Фонсторх, 2007 р.) вимір трансакцій одного дня американської фінансової індустрії становить мільярди доларів.

У фокусі кримінолого-криміналістичного аспекту дослідження комп'ютерної злочинності знаходяться: цілі протиправної поведінки; важливі відомості про особу правопорушника; мотивація антисоціальної поведінки; типологія злочину; предмет і місце посягання; відомості про потерпілу сторону; та ін. елементи, що мають значення для виявлення, розслідування та запобігання загроз комп'ютерної криміналістики.

У фокусі виявлення загроз і боротьби зі злочинами у сфері використання комп'ютерних технологій перебувають особи, що мають доступ до комп'ютерної техніки за своїми функціональними обов'язками; особи, що не мають доступу до такої техніки. Порушення, які вони вчиняють, можуть полягати у несанкціонованому використанні комп'ютерів, розповсюдженні комп'ютерних вірусів та ін.

Для реалізації компетенцій комп'ютерної криміналістики майбутні фахівці кібербезпеки повинні виявляти і кваліфікувати правопорушення у галузі комп'ютерних технологій, незаконне використання комп'ютерів для моделювання, прогнозування своєї протиправної поведінки, комп'ютерного шантажу конкурентів, фальсифікації та містифікації інформації, комерційного шпигунства має на меті отримання матеріальної вигоди чи приховування інших правопорушень. Мотивовані порушники, не пов'язані трудовими відносинами з організацією, можуть бути найбільш професійно підготовленими в галузі ІТ, вчиняючи правопорушення, вони не тільки переслідують прямі матеріальні вигоди. Для них має значення насамперед нанесення шкоди інформаційним ресурсам, фізичне знищення або пошкодженням засобів комп'ютерної техніки,

До окремої категорії порушників відносять державні організації – юридичні особи, які займаються комп'ютерним шпигунством, розвідкою (державні розвідувальні та контррозвідувальні організації), метою яких є отримання важливої інформації, що становить державну таємницю чи комерційні секрети конкурента (супротивника) в економічній, політичній, науково-технічній та інших галузях суспільних відносин. Зазначені організації є суб'єктами міжнародного публічного і приватного права.

Проектування навчальних планів професійної підготовки майбутніх фахівців з кібербезпеки та модернізація навчальної програми з комп'ютерної криміналістики ґрунтується на впровадженні передового зарубіжного і вітчизняного досвіду викладання навчальної дисципліни у

вищих навчальних закладах, а також специфіці діяльності Служби безпеки України, вивченні досвіду своєчасного виявлення та запобігання інформаційним загрозам і кіберінцидентам, практичних аспектах прийняття фахових рішень, використанні інтерактивних методів, програмного і прогамно-апаратного забезпечення та поєднання ситуативного моделювання (Case Forensic) для реалізації фахових компетенцій з кібербезпеки у майбутній професійній діяльності.

Професіограма майбутніх фахівців з кібербезпеки поєднує інтегроване вивчення фахових навчальних дисциплін: «Технології програмування», «Інформаційні системи і технології», «Комп'ютерні мережі та комунікації», Безпека інформації в інформаційно-комунікаційних системах», «Теорія ризиків», «Аудит інформаційної та кібернетичної безпеки», «Комп'ютерні інциденти та методи їх дослідження», «Програмні засоби захисту інформації» та ін.

Модернізація змісту формування професійної компетентності майбутніх фахівців з кібербезпеки здійснюється з доповненням нових фахових дисциплін на засадах міжнародного співробітництва у галузі інформаційної безпеки та кібербезпеки: «OSINT» (Open source intelligence), «Архітектура та адміністрування сучасних операційних систем», «Methods of reverse engineering».

*УДК 351.746:007*

**Гавловський В.Д**.
кандидат юридичних наук,
старший науковий співробітник
Міжвідомчий науково-дослідний центр з проблем
боротьби з організованою злочинністю
при РНБО України

## ДО ПИТАННЯ НАЛАГОДЖЕННЯ МІЖВІДОМЧОГО ОБМІНУ ІНФОРМАЦІЄЮ

Одним із важливих напрямів підвищення ефективності діяльності СБ України щодо забезпечення інформаційної безпеки України є покращення забезпечення інформаційних потреб Служби за рахунок доступу до державних інформаційних ресурсів, зокрема до баз і банків даних МВС, митних і податкових органів та центральних органів виконавчої влади (ЦОВВ). Невирішеність зазначених питань негативно впливає на спроможність держави своєчасно виявляти та припиняти спеціальні інформаційні операції, акти розвідувальної та розвідувально-підривної діяльності, боротися з організованою злочинністю.

Наразі в автоматизованих базах і банках даних правоохоронних органів та ЦОВВ накопичені значні обсяги інформації. Проте залишається актуальним питання налагодження інформаційного обміну між суб'єктами, яке на сьогодні потребує відповідного нормативного регулювання як на державному, так і міжвідомчому рівнях.

Провідну роль в інформатизації правоохоронних органів України відіграє МВС України, більшість інформаційних ресурсів якого використовується всіма правоохоронними органами.

З метою поліпшення координації організаційних, оперативно-розшукових, правових та інформаційних заходів правоохоронних органів щодо боротьби із злочинністю, підвищення ефективності в цій сфері було прийнято низку нормативно-правових актів.

Так, у 2009 році відповідно до Указу Президента України від 31 січня 2006 року № 80 "Про Єдину комп'ютерну інформаційну систему правоохоронних органів з питань боротьби із злочинністю" КМУ прийняв постанову від 8 квітня 2009 року № 321 «Про затвердження Державної програми інформаційно-телекомунікаційного забезпечення правоохоронних органів, діяльність яких пов'язана з боротьбою із злочинністю».

Виконання цієї Програми дало б змогу створити систему, яка сприяла б істотному вдосконаленню інформаційної взаємодії правоохоронних та інших державних органів у сфері боротьби із злочинністю, поліпшенню координації їх діяльності, забезпеченню спільного формування та використання інформаційних ресурсів для ефективної боротьби із злочинністю.

Втрата чинності постановою у квітні 2013 року негативно вплинула на розвиток міжвідомчого інформаційного обміну.

14 червня 2016 року наказом МВС України № 511 затверджено Концепцію інформатизації МВС України та ЦОВВ, діяльність яких спрямовується та координується Кабінетом Міністрів України через МВС України, на 2016-2020 роки. Концепція спрямована на створення умов для ефективного інформаційного забезпечення діяльності системи МВС, НПУ, ДПС, ДМС, Державної служби з надзвичайних ситуацій.

Разом із тим, як зазначають у МВС, залишається невирішеним комплекс важливих питань, що ускладнюють виконання завдань, віднесених до сфер відповідальності МВС України, а також уповільнюють налагодження електронної взаємодії органів системи МВС з іншими органами державної влади та місцевого самоврядування.

На сьогодні кожний правоохоронний орган самостійно налагоджує доступ до окремих інформаційних ресурсів державних органів, зокрема шляхом укладання спільних нормативно-правових актів.

Правоохоронні органи заінтересовані також у прискоренні реалізації механізмів доступу до інформаційних ресурсів інших органів державної влади відповідно до Положення про електронну взаємодію державних електронних інформаційних ресурсів, затвердженого постановою Кабіне-

ту Міністрів України від 08 вересня 2016 року № 606, створення та впровадження якої в експлуатацію покладено на Державне агентство з питань електронного урядування України, яким на цей час підготовлено проект постанови Кабінету Міністрів України «Деякі питання організації електронної взаємодії державних електронних інформаційних ресурсів», у разі прийняття якої система має запрацювати в першому півріччі 2018 року.

Слід зазначити, що Службою безпеки України одним із важливих елементів забезпечення якісного аналізу кіберзагроз та організації дієвих заходів щодо їх протидії вважає оперативний обмін інформацією між основними суб'єктами забезпечення кібербезпеки держави в режимі реального часу про кібератаки, які мають ознаки злочинної діяльності, з боку міжнародних злочинних хакерських угруповань.

Питання налагодження міжвідомчого обміну інформацією та створення єдиної інтерактивної бази даних про кіберінциденти неодноразово порушувалися в рамках роботи Національного координаційного центру кібербезпеки при РНБО України, а також знайшло відображення в низці правозастосовних державних актів у сфері кібербезпеки, зокрема Указі Президента України від 30 серпня 2017 року № 254 «Про рішення РНБО України від 10 липня 2017 року «Про стан виконання рішення РНБО України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», уведеного в дію Указом Президента України від 13 лютого 2017 року № 32», де доручено «Адміністрації ДССЗЗІ України підготувати та внести в установленому порядку на розгляд Кабінету Міністрів України пропозиції щодо створення для потреб МО України, ДССЗЗІ України, СБУ, НПУ, НБУ, розвідувальних органів єдиної інтерактивної бази даних про кіберінциденти. Наразі Адміністрацією ДССЗЗІ України пропозицій на розгляд КМУ не внесено.

Висновок. Необхідно створити міжвідомчу робочу групу з розробки проекту нормативно-правового акту з метою регламентації налагодження міжвідомчого обміну інформацією. Результатом роботи цієї групи має стати узгодження проектів нормативно-правових актів про міжвідомчий обмін інформацією та міжвідомчий віддалений доступ до АІС (баз даних, реєстрів тощо) інших державних органів у режимі реального часу.

*УДК 342.7*
**Головко О.М.**
Навчально-науковий інститут права
і соціальних технологій ЧНТУ

## ЧЕТВЕРТЕ ПОКОЛІННЯ ПРАВ ЛЮДИНИ: БЕЗПЕКОВИЙ АСПЕКТ

Серед ключових складових human security в європейському співтоваристві виділяють особисту безпеку [1, с. 14]. Саме в її контексті пропону-

ємо розглядати інформаційну безпеку людини, оскільки вона часто розглядається як елемент національної інформаційної безпеки, про наявність якого лише згадується. Однак, концепція безпеки людини покликана утвердити думку про те, що «кінцевим бенефіціаром безпеки є швидше людина, а не держава; і що для людини насправді важливо бути захищеною у щоденному житті, мати засоби для існування та зберегти свою гідність» [2, с. 72].

Відповідно до ч. 1 ст. 5 Закону України «Про захист суспільної моралі», завданням державної політики є створення необхідних правових, економічних та організаційних умов, які сприяють реалізації права на інформаційний простір, вільний від матеріалів, що становлять загрозу фізичному, інтелектуальному, морально-психологічному стану населення. Таким чином, закон ставить під охорону три компоненти: фізичний, інтелектуальний та морально-психологічний стан населення, яким може бути завдана шкода в результаті наявності певних інформаційних небезпек, загроз чи впливів у сфері суспільної моралі. Вважаємо, що доречно застосовувати такий підхід й у інших сферах діяльності суспільства, виходячи з права людини на безпечний інформаційний простір загалом, а не лише в контексті недопущення пропаганди культу насильства, жорстокості та поширення порнографії. Вплив інтелектуально розвинених жорстоких індивідуумів (об'єднаних, наприклад, у терористичні мережі), а також неконтрольовані фінансові та інформаційні потоки роблять загрози і ризики безпеці більш складними й менш прогнозованими [3, с. 15].

Відповідно до ст. 2 Декларації прав людини і громадянина 1789 року, метою кожного політичного об'єднання є збереження природних і невід'ємних прав людини. Такими є свобода, власність, безпека і спротив пригнобленню. Таким чином, безпеку виділяють одним із об'єктів, котрий має бути поставлений під охорону держави в особі політичних сил. Зазначимо також, в змісті Загальної декларації прав людини 1948 року передбачено, що дотримання права на безпеку є підґрунтям для належної реалізації прав людини як невід'ємної складової загальних прав людини.

Резолюція A/RES/66/290, прийнята Генеральною Асамблеєю 10 вересня 2012 р. визначила, що безпека людини заснована на національній відповідальності. Оскільки політичні, економічні, соціальні та культурні умови безпеки людини істотно різняться на міжнародному та національному рівнях, безпеку людини зміцнює національні рішення, які сумісні з місцевими реаліями [4]. Таким чином, станом на момент прийняття даного документу було усвідомлено мінливість поняття «безпека людини» у світі в цілому. З урахуванням цього та ряду нових інформаційних загроз виокремлення безпеки людини в інформаційному просторі потребує особливої уваги. Більше того, загрози, що зароджуються у кіберпросторі, можуть матеріалізуватись – перенестись до реального життя і трансформуватись, наприклад, у збройні конфлікти [3, с. 43].

В цьому аспекті пропонуємо звернутися до теорії поколінь прав людини, котрі розвиваються відповідно до появи кардинально нового етапу розвитку людства. Так, зараз, в результаті колосального розвитку науки і техніки особливо в частині ІКТ, активно обговорюється питання становлення четвертого покоління прав людини. Так, до четвертого покоління прав зараховують лише інформаційні права та технології [5, с. 125]. Однак, деякі науковці вважають, що до прав четвертого покоління належать усі права, що виникли внаслідок наукового прогресу, розвитку моралі, а саме всі так звані «соматичні права», в тому числі інформаційні права [6, с. 215].

Безпека людини і права людини є тісно пов'язаними. Вона базується на забезпеченні прав людини, а також враховує права людини «третього покоління», в тому числі право на розвиток і право на мир [3, с. 17]. З огляду на це пропонуємо розглядати право на інформаційну безпеку людини як одне з прав так званого «четвертого покоління».

Отже, вважаємо, що визначення права людини на безпечне інформаційне середовище як одного з прав людини «четвертого покоління» має нагальну потребу в закріпленні на законодавчому рівні та її виокремлення з комплексу національної безпеки з метою їх подальшого нормативно-правового забезпечення.

**Література**

1. Alkire S. A Conceptual Framework for Human Security. CRISE Working Paper 2. London: University of Oxford, 2003. 52 p

2. Oberleitner G. The OSCE and human security. Security and Human Rights. Volume 19. 2008. Issue 1. P. 64-72.

3. Маляренко Т. Безпека людини у мінливому світі: монографія. Донецьк: ТОВ «Східний видавничий дім», 2013. 200 с.

4. Резолюции 66-й сессии (2011–2012 годы). URL: http://www.un.org/ru/ga/66/docs/66res3.shtml (дата звернення: 12.02.2018).

5. Головистикова А. Н. Права человека: учеб. / А. Н. Головистикова. – М.: Эксмо, 2008. – 327 с.

6. Барабаш О.О. Четверте покоління прав людини: загальнотеоретична характеристика / О.О.Барабаш // Вісник Національного університету «Львівська політехніка». Юридичні науки. – 2016. – № 837. – С. 213-217.

*УДК 351.74*
**Гордієнко С. Б.**
кандидат технічних наук, доцент
Національна академія СБ України
**Скубак О. М.**
кандидат технічних наук, доцент
Національна академія СБ України

# ЗАВДАННЯ АНАЛІЗУ ДОЦІЛЬНОСТІ РЕАЛІЗАЦІЇ ЗАХОДІВ ЩОДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Управління інформаційною безпекою, так само як і управління в багатьох інших сферах діяльності, передбачає періодичне прийняття різних управлінських рішень, які полягають, як правило, у виборі певних альтернатив або визначенні деяких параметрів окремих організаційних і/або технічних систем і підсистем [1]. Одним з можливих підходів до вибору альтернатив в ситуації прийняття управлінського рішення є т.зв. "Вольовий" підхід, коли рішення з тих чи інших причин приймається інтуїтивно і формально обґрунтований причинно-наслідковий взаємозв’язок між певними вихідними передумовами і конкретно прийнятим рішенням не може бути встановлений.

Очевидно, що альтернативою "вольовому" підходу стає прийняття рішень на підставі певних формальних процедурах і послідовному аналізі.

Основою такого аналізу і подальшого прийняття рішень є економічний аналіз, який передбачає вивчення всіх факторів, під впливом яких відбувається розвиток аналізованих систем, закономірностей їх поведінки, динаміки зміни, а також використання універсальної грошової оцінки.

Складність завдань економічного аналізу практично у всіх областях діяльності, як правило, обумовлюється тим, що багато ключових параметрів економічних моделей неможливо достовірно оцінити, і вони носять імовірнісний характер. Для забезпечення якомога більшої достовірності розрахунків в процесі проведення економічного аналізу і прийняття рішень необхідно організувати комплекс робіт зі збору вихідної інформації, розрахунку прогнозних значень, з опитуванням експертів в різних областях і обробці всіх даних.

Особлива складність економічного аналізу в такій сфері, як інформаційна безпека, обумовлюється такими специфічними факторами, як:

– швидкий розвиток інформаційних технологій і методик, що використовуються в цій сфері (як засобів і методів захисту, так і засобів і методів нападу);

– неможливість достовірно передбачити всі можливі сценарії нападу на інформаційні системи і моделі поведінки нападників;

– неможливість дати достовірну, досить точну оцінку вартості інформаційних ресурсів, а також оцінити наслідки різних порушень в грошовому вираженні [1].

Це вимагає додаткових зусиль по організації процесу економічного аналізу, а також часто призводить до того, що багато прийнятих рішень, які стосуються забезпечення інформаційної безпеки, можуть виявитися неадекватними.

У процесі поточної діяльності підприємствам постійно доводиться стикатися з тими чи іншими змінами: уточнюються бізнес-процеси, змінюється кон'юнктура ринків збуту і ринків споживаних матеріальних ресурсів і послуг, з'являються нові технології, змінюють свою поведінку конкуренти і контрагенти, змінюється законодавство і політика держави та ін.

Конкретні форми, в яких проявляється реакція керівників, можуть бути різними. Це може бути зміна маркетингової політики, реорганізація бізнес-процесів, зміна технологій, зміна продукту, що виробляється, злиття з конкурентами або їх поглинання і т.п. Таким чином, в ситуації, коли необхідно здійснити деякі нові організаційні або технічні заходи (реалізувати проект), основним завданням осіб, що відповідають за ефективну організацію інформаційної безпеки, є чітке співвіднесення витрат, які доведеться понести в зв'язку з реалізацією цього заходу, і додаткових (нових ) грошових потоків, які будуть отримані.

В якості основного показника, що відображає це співвідношення, в економічній практиці прийнято використовувати функцію віддачі від інвестицій – Return on Investment *(ROI)* [4].

І хоча з математичної точки зору всі розрахунки в описаній рамкової моделі оцінки *ROI* є гранично простими, визначення окремих параметрів (прогнозованих частоти порушень і розмірів втрат, а також передбачуваного терміну використання програмних і апаратних засобів і організаційних моделей) може викликати значні труднощі на практиці.

Причому, якщо оцінку ймовірностей атак, а також оцінку того, наскільки ці атаки можуть бути успішними, в переважній більшості можна довірити зовнішнім консультантам з інформаційної безпеки, то оцінку вартості інформації та економічних наслідків втрати контролю над інформаційними активами, швидше за все, доцільно здійснювати самим фахівцям, що працюють на підприємстві (економістам, маркетологам і т.п.), а також залучати для цього сторонніх фахівців з відповідних сфер діяльності (маркетингу, фінансів, торгівлі і т.п.) [3].

Незважаючи на всі труднощі процесу оцінки доцільності впровадження засобів захисту, запропонована методологія дозволяє менеджерам і фахівцям із захисту інформації отримувати обґрунтовані оцінки і робити формалізовані висновки щодо того, наскільки виправданими є вкладення в

певні засоби захисту інформації, а також визначити основні пріоритети витрачання коштів, передбачених у бюджеті на забезпечення інформаційної безпеки (якщо підприємство практикує виділення фіксованих сум на ці цілі).

**Література**

1. Анисимов А.А. Менеджмент в сфере информационной безопасности М.: БИНОМ, 2009.

2. Основи управления информационной безопасностью / А.П.Курило, Н.Г.Милославская, М. Ю.Сенаторов и др. – М.: Горячая линия-Телеком, 2012.

3. Петренко С.А. Управление информационными рисками. Экономически оправдання безопасность / С.А. Петренко, С.В. Симонов. – М.: Компания АйТи, ДМК-Пресс, 2004.

4. Артемов В.Ю. Основи менеджменту для інформаційних аналітиків: курс лекцій / В.Ю.Артемов. – К.: КНТ, 2007.

*УДК 004.56*

**Гулак Г.М.**
кандидат технічних наук, доцент
Національна академія СБ України
**Кащук В.І.**
Національна академія СБ України
**Складанний П.М.**
Київський університет ім. Б. Грінченко

## УТОЧНЕНА МОДЕЛЬ ПОРУШНИКА ТА МОДЕЛЬ РЕАЛІЗАЦІЇ КІБЕРАТАК В СИСТЕМАХ УПРАВЛІННЯ ТЕХНОЛОГІЧНИМИ ПРОЦЕСАМИ

Реалізація ефективного кіберзахисту (включаючи, криптографічний захисту інформації (КЗІ)), в системах управління технологічними процесами (СУТП) потребує побудови адекватної моделі загроз, що в умовах постійного вдосконалення методів та засобів нападу [1] вимагає постійного уточнення моделі потенційного порушника системи захисту [2].

Аналіз повідомлень про кібератаки дає змогу визначити мету його злочинних дій, а саме нанесення суттєвих збитків власнику системи, мінімізуючи при цьому власні фінансові, матеріальні та інші витрати. Для цього, по-перше, він має достатньо високу кваліфікацію та необхідний фінансовий ресурс, технічне і програмне оснащення, які дозволяють йому створювати складні програмні комплекси для реалізації кібератак.

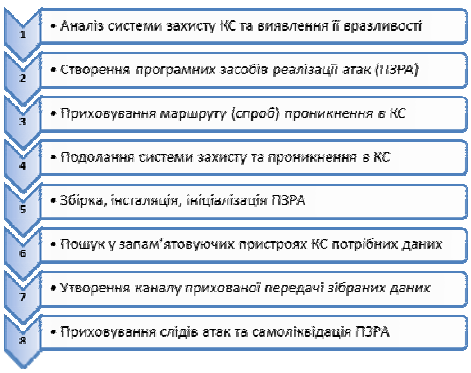
По-друге, згідно з принципом Керкхофса, він знає алгоритми функціонування засобів захисту, включаючи засоби КЗІ, але до початку атаки не знає діючих ключів. По-третє, для досягнення поставлених цілей порушник має можливість перехоплення будь якої інформації у транспортній мережі, модифікацію або створення неприпустимої команди за відносно невеликий час.

Виходячи з викладеного, можливо передбачити наступні варіанти його зловмисних дій (потенційних загроз) стосовно СУТП в цілому: 1) модифікація дійсної команди або реальної інформації про внутрішній стан системи; 2) формування та надсилання керованому об'єкту неприпустимої команди або фальшивих даних про внутрішній стан СУТП; 3) перехоплення в транспортній мережі окремих команд або частки інформації щодо внутрішніх станів задля їх вилучення; 4) крадіжка конфіденційної інформації щодо сервісів, які надаються; 5) модифікація або руйнування програмного коду СУТП.

Щодо програмних реалізацій засобів КЗІ, які використовуються в СУТП, можливо вважати, що метою дій порушника може бути: 1) зміна, знищення або крадіжка критичних параметрів CSP; 2) модифікація програмного коду (криптосхеми) засобу КЗІ.

На підставі аналізу наукових публікацій щодо реалізації кібератак у поєднанні з відомими методами криптоаналізу на основі побічних каналів [3] була сформована наступна модель кібератак в СУТП, яка включає вісім фаз активних дій порушника (рис.):

1. Розвідка. На першому етапі порушник, використовуючи всі доступні методи, здійснює приховане вивчення вразливостей комп'ютерної системи (КС), яка є технологічною базою функціонування СУТП, а також виявлення слабких місць наявної системи захисту [4].




2. Розробка. На цьому кроці, здійснюється вивчення отриманої інформації та розробка програмних засобів для реалізації атак (ПЗРА).

3. Маскування. Порушник здійснює заходи щодо усунення ознак, які пов'язують ПЗРА та спосіб його застосування з реальним розробником, та/або створює фіктивні ознаки, що ототожнюються з непричетними до кібератаки суб'єктами. Також він визначає тактику приховування реального маршруту (адрес проміжних вузлів глобальної мережі) спроб проникнення в КС.

4. Проникнення. Використовуючи створені засоби і технології, а також можливості інсайдерського впливу порушник забезпечує подолання системи захисту та проникнення ядра ПЗРА в програмне середовище КС.

5. Підготовка. Далі в автоматичному або автоматизованому режимі реалізується збирання ПЗРА з окремих модулів, його інсталяція та ініціалізація.

6. Реалізація. Ініціалізоване ПЗРА на основі певної апріорної інформації про підсистеми (елементи) КС, що виконують конкретні функції СУТП, а також про потрібні порушнику дані, зокрема, чутливі параметри безпеки криптографічних модулів SSP виявляє та ідентифікує зазначені об'єкти у запам'ятовуючих пристроях КС. У якості відповідної апріорної інформації можуть виступати розмір файлів, формати даних, певні ключові слова, програмні переривання/звернення до деяких ресурсів системи тощо. Залежно від цілей кібератаки виявлені ресурси можуть бути знищені, модифіковані або використані для розкриття конфіденційної інформації.

7. Витік. За необхідності, створюється канал прихованої передачі зібраних даних з використанням методів стеганографії, процедури стискання даних з наступним шифруванням, фізичного переносу під час підключення зовнішніх пристроїв тощо.

8. Самоліквідація. На завершальному етапі ПЗРА включає механізми самознищення та приховування слідів кібератаки. Цей етап реалізується автоматично, в разі настання в КС певних обставин (наприклад, визначеного часу), або автоматизовано на підставі отримання команди ззовні.

**Література**

1. Бурячок В.Л. Завдання форми та способи ведення воєн у кібернетичному просторі / В.Л.Бурячок, Г.М.Гулак, В.О.Хорошко // Науково-технічний журнал «Наука та оборона»,2011. – № 3. – С. 35-42.

2. Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації. Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20.07.2007 № 141, в редакції Наказу Адміністрації ДССЗЗІ від 14.12.2015 № 767.

3. J. Kelsey Side Channel Cryptanalysis of Product Ciphers / J. Kelsey, B. Schneier, D. Wagner, C. Hall // 5th European Symposium on Research in Computer Security Louvain-la-Neuve, Belgium September 16–18, 1998 Proceedings, Berlin, Springer, 1998, 97-111 pp.

4. Гулак Г.М. Забезпечення безпеки засобів КЗІ у кіберпросторі / Г.М.Гулак // Матеріали науково-технічної конференції «Сучасні інформаційно-телекомунікаційні технології» – Т. ІУ Сучасні технології інформаційної безпеки. – К., 2015. – С. 100-102.

*УДК 340*

**Гуцалюк М. В.**
кандидат юридичних наук, доцент,
старший науковий співробітник,
провідний науковий співробітник
Міжвідомчого науково-дослідного центру
з проблем боротьби з організованою злочинністю
при РНБО України

# АКТУАЛЬНІ ПИТАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

Сьогодні на другому місці за негативним впливом для світової спільноти після природних катаклізмів перебувають кібератаки (рік тому технологічні ризики разом із кіберзлочинністю займали третє місце). Це зазначено в щорічній доповіді експертів Всесвітнього економічного форуму в Давосі про глобальні ризики у світі під назвою "Global Risks Report 2018", яка опублікована в січні 2018 року [1]. Виходячи з концептів документу ризики кібербезпеки постійно зростають, як у їх поширеності, так і руйнівному потенціалі. Наприклад, кількість кібератак на підприємства у світі подвоїлася протягом п'яти останніх років, а інциденти, які колись розглядалися як надзвичайні, сьогодні стають все більш розповсюдженими.

Також зростають збитки від кіберзлочинів, які відповідно до звіту компанії McAfee і Центру стратегічних і міжнародних досліджень (CSIS) склали у 2017 році близько 600 млрд доларів [2].

Новою загрозою для кібербезпеки є створення кібервійськ, які здатні впливати на інфраструктуру «противників», що створюються багатьох країнах. Генеральний секретар ООН Антоніу Ґутерріша під час виступу в Лісабонському університеті 19 лютого 2018 року застеріг: «Наступна війна почнеться з масової кібератаки з метою знищення військового потенціалу і паралічу базової інфраструктури, такої як електричні мережі» [3]. Ґутерріш закликав світову спільноту до об'єднання з метою мінімізації впливу кібервоєн на життя цивільних громадян та запропонував створити в ООН платформу, на базі якої вчені, урядовці та інші особи могли б розробити правила «для забезпечення більш гуманного характеру» щодо вирішення будь-якого конфлікту, пов'язаного з інформаційними технологіями.

В Україні світові тенденції кіберзагроз посилюються внаслідок гібридної війни, під час якої об'єкти критичної інфраструктури стають мішенями, на яких випробовуються все нові технології кібератак, зокрема кібератаки Petya, NotPetya були зорієнтовані на українські підприємства.

Останнім часом для захисту вітчизняного кіберпростору були розроблені та прийняті ряд важливих нормативно-правових актів, серед яких слід

зазначити Стратегію кібербезпеки України, Рішення РНБО України «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», Закон України «Про основні засади кібербезпеки України» та інші документи у сфері кібербезпеки.

Водночас украй важливим є не тільки прийняття відповідних нормативно-правових актів, але й упровадження їх положень у практичну діяльність суб'єктів, задіяних у забезпеченні кібербезпеки. Зокрема конкретні заходи для усіх основних суб'єктів забезпечення кібербезпеки та терміни їх реалізації визначені в Плані заходів на 2017 рік з реалізації Стратегії кібербезпеки України, який затверджений розпорядженням Кабінету Міністрів України від 10 березня 2017 р. № 155-р.

Слід зазначити, що лише після потужних кібератак на критичні інфраструктури в грудні 2016 року та у 2017 році державними органами проведено значну роботу із зміцнення кібербезпеки. Але, на жаль, на початок 2018 року залишається невиконаною ще низка важливих заходів, особливо тих, що стосуються об'єктів критичної інфраструктури, зокрема:

– не визначений перелік об'єктів критичної інфраструктури України;

– не внесено до Верховної Ради України проект Закону України "Про критичну інфраструктуру та її захист"; не в повному обсязі імплементуються Директива 2008/114/ЕС [4] щодо захисту критичної інфраструктури, зокрема з питань кібербезпеки та кіберзахисту об'єктів критичної інфраструктури, Директива ЄС 2013/40/EU від 12 серпня 2013 року [5] щодо кібератак на інформаційні системи та Директива ЄС 2016/1148 від 6 липня 2016 року про заходи щодо забезпечення високого загального рівня безпеки мережевих та інформаційних систем [6].

Слід також вказати, що жодна країна не може самостійно протистояти проблемам кібербезпеки, а тому необхідна тісна співпраця на міжнародному рівні з європейськими та структурами країн НАТО. Поряд із цим слід підвищувати рівень державно-приватної взаємодії в галузі кібербезпеки, та, як це зазначено в Рекомендаціях Європейського центру протидії кіберзлочинності (European Cybercrime Centre - EC3 ) «Оцінка загроз організованої злочинності в Інтернеті», в зв'язку з тим, що сектори критичної інфраструктури є досить вразливими до руйнівних кібератак, необхідно забезпечити їх більш досвідченими та підготовленими співробітниками та відповідним обладнанням, щоб протидіяти кібератакам [7].

**Висновок:**

Виконання зазначених заходів сприятиме забезпеченню необхідного рівня кібербезпеки України та надасть можливість отримати значні переваги від впровадження інформаційних технологій в усі сфери суспільного життя.

**Література**

1. Global Risks Report 2018" < URL: http: www.weforum.org.

2. Збитки світової економіки від хакерів досягли $ 600 млрд < URL: https://ua.korrespondent.net/world/3943548-zbytky-svitovoi-ekonomiky-vid-khakeriv-dosiahly-600-mlrd

3. Генсекретар ООН закликав до глобальної боротьби проти кібервоєн < URL: https://www.radiosvoboda.org/a/news/29049044.html.

4. COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection < URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008L0114.

5. DIRECTIVE 2013/40/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA < URL: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32013L0040.

6. DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union < URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.194.01.0001.01.ENG.

7. Internet Organised Crime Threat Assessment (IOCTA) 2017 < URL: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017.

УДК 342 341.1/3 355/359

**Гущин О.О.**
кандидат юридичних наук
Військовий інститут КНУ ім. Тараса Шевченка

## ДО ПИТАННЯ ПРАВОВОГО РЕГУЛЮВАННЯ КІБЕРОПЕРАЦІЙ

19 лютого 2018 року Генеральний секретар Організації Об’єднаних Націй Антоніу Ґутерріш закликав до об’єднання світової спільноти з метою мінімізації впливу кібервоєн на життя цивільних громадян. “Наступна війна почнеться з масової кібератаки з метою знищення військового потенціалу і паралічу базової інфраструктури, такої як електричні мережі”, – сказав Ґутерріш під час виступу в Лісабонському університеті [1]. Він також зазначив, що “Епізоди кібернетичних бойових дій між державами вже мають місце. Але гіршим є те, що не існує регуляторної схеми для такого типу бойових дій та незрозуміло, як до них повинні застосовуватись Женевська конвенція чи міжнародне гуманітарне право” [2].

Дійсно, актуальність запровадження дієвого механізму правового регулювання кібероперацій не викликає жодного сумніву.

Так, у 2008 році Північноатлантичний Альянс для захисту від кібератак вирішив створити Об'єднаний центр передових технологій з кібероборони в місті Таллінн, Естонія. Як відомо, ініціатором його створення стала саме Естонія, що за рік до того постраждала від надпотужної кібератаки на державні органи, у якій звинувачено російських хакерів [3]. Тож цей заклад став багатонаціональним та міждисциплінарним центром експертизи в сфері кіберзахисту та зосереджується на технологіях, стратегіях, операціях та питаннях права [4].

Враховуючи новітні виклики, що постають перед країнами через кіберзагрози та надзвичайну актуальність належного правового регулювання реагування на них військовими методами, під егідою талліннського центру було скликано групу вчених-міжнародників, яка мала на меті знайти правові відповіді на ці питання. Як наслідок цього у 2013 році побачило світ "Талліннське Керівництво з міжнародного права щодо методів ведення кібернетичних бойових дій". В 2017 році вже вийшло друге видання цього Керівництва, яке змінило назву на "Талліннське Керівництво 2.0 з міжнародного права щодо методів ведення кібернетичних операцій" [5]. Навіть із зміни назви вбачається, що автори, попри сучасне почуття гумору, намагаються розширити сферу правового регулювання Права збройних конфліктів та Міжнародного права прав людини вже не тільки до "класичних" бойових дій із застосуванням кібернетичної складової, а взагалі до будь-якого виду кібернетичних операцій. Аналіз, що здійснено під час створення Талліннського керівництва 2.0, базується на розумінні того, що міжнародне право, яке створено до настання "кібер-епохи", застосовне й до кібероперацій, що проводяться державами і спрямовані проти держав. Це означає, що ці "кібер-події" не відбуваються в правовому вакуумі, і держави мають права та несуть зобов'язання за міжнародним правом [5]. На даний час Альянс намагається імплентувати висновки Талліннського керівництва вже у документи, що визначають процес прийняття рішень та бойового управління військами, а також під час створення відповідних структурних підрозділів.

На цьому тлі варто зазначити, що наша держава не залишилась осторонь цих новітніх процесів. Так, Указом Президента України від 15 березня 2016 року № 96/2016 затверджено рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" [6], а розпорядженням Кабінету Міністрів України від 10 березня 2017 року затверджено план заходів з її реалізації на 2017 рік. Ним, зокрема, передбачено питання удосконалення нормативно-правової бази шляхом впровадження норм міжнародних стандартів, стандартів ЄС та НАТО у сфері інформаційної безпеки та кіберзахисту [7].

Величезним позитивним моментом слід вважати прийняття 5 жовтня 2017 року Верховною Радою України Закону України “Про основні засади забезпечення кібербезпеки України”, яким, зокрема, вводяться такі поняття як “кібербезпека”, “кіберзахист”, “кібероборона”, “кібершпигунство” тощо. Згідно зі статтею 7 цього Закону одним з принципів забезпечення кібербезпеки є пропорційність та адекватність заходів кіберзахисту реальним та потенційним ризикам та реалізація невід’ємного права держави на самозахист відповідно до норм міжнародного права у разі вчинення агресивних дій у кіберпросторі.

З урахуванням зазначеного одним з пріоритетів у сфері нормотворчої діяльності складових сектору безпеки і оборони слід вважати розроблення та прийняття керівних документів із застосування норм Права збройних конфліктів та Міжнародного права прав людини.

## Література


1. Генсекретар ООН закликав до глобальної боротьби проти кібервоєн // Радіо Свобода. URL: https://www.radiosvoboda.org/a/news/29049044.html. (дата звернення 05.03.2018).
2. U.N. Chief urges global rules for cyber warfare // Reuters. URL: https://www.reuters.com/article/us-un-guterres-cyber/u-n-chief-urges-global-rules-for-cyber-warfare-idUSKCN1G31Q4. (дата звернення 05.03.2018).
3. NATO launches cyber defence centre in Estonia // CCDCOE. URL: http://www.spacewar.com/reports/NATO_launches_cyber_defence_centre_in_Estonia_999.html. (дата звернення 05.03.2018).
4. NATO Cooperative Cyber Defence Centre of Excellence // CCDCOE. URL: https://ccdcoe.org/ (дата звернення 05.03.2018).
5. Tallinn Manual. Research // CCDCOE. URL: https://ccdcoe.org/research.html. (дата звернення 05.03.2018).
6. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року “Про Стратегію кібербезпеки України” : Указ Президента України від 15 березня 2016 року № 96/2016 // Офіційне інтернет-представництво Президента України. URL: http://www.president.gov.ua/documents/962016-19836 (дата звернення 05.03.2018).
7. Про затвердження плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України : Розпорядження Кабінету Міністрів України від 10 березня 2017 року № 155-р // Урядовий портал. URL: https://www.kmu.gov.ua/ua/npas/249807504. (дата звернення 05.03.2018).
8. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 року № 2163-VIII // База даних “Законодавство України” / ВР України. URL: http://zakon5.rada.gov.ua/laws/show/2163-19 (дата звернення 05.03.2018).

*УДК 347.73.086*
**Дмитренко Е. С.**
доктор юридичних наук., професор,
завідувач кафедри фінансового права
ДВНЗ «Київський національний економічний
університет імені Вадима Гетьмана»

# АКТУАЛЬНІ ПИТАННЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СФЕРИ ПУБЛІЧНОЇ ФІНАНСОВОЇ ДІЯЛЬНОСТІ

Функціонування досконалого механізму забезпечення інформаційної безпеки є однією з ознак правової держави та громадянського суспільства. Такий механізм сприяє реалізації покладених на органи державної влади та місцевого самоврядування повноважень, в тому числі й у сфері публічної фінансової діяльності.

Незважаючи на важливість зазначеного, проблематика забезпечення інформаційної безпеки сфери публічної фінансової діяльності, окремо науковцями не розглядалася.

Розгляд зазначеного питання також актуалізується у зв'язку з прийняттям останнім часом відповідних норм у Податковому кодексі України від 02.12.2010 р. № 2755-VI (ПК України), Законах України «Про доступ до публічної інформації» від 13.01.2011 р. № 2939-VI, «Про відкритість використання публічних коштів» від 11.02. 2015 р. 183-VIII. У результаті ретельного вивчення змісту норм зазначеного законодавства та Закону України «Про інформацію» від 02.10. 1992 р. № 2657-XII, вважаємо, що сутністю діяльності із забезпечення інформаційної безпеки у аналізованій сфері є захист інформації, тобто сукупності відомостей і даних, що створені або отримані у процесі публічної фінансової діяльності її учасниками і необхідні для реалізації покладених на них завдань і функцій.

Результатом ефективної діяльності із забезпечення інформаційної безпеки сфери публічної фінансової діяльності, на нашу думку, має бути функціонування такого механізму, який спрямований на вільне одержання, використання, поширення, зберігання і захист інформації у цій сфері [1]. А тому основними напрямами зазначеної діяльності вважаємо забезпечення доступності інформації у сфері публічної фінансової діяльності та її захист.

Реалізація права на інформацію передбачає певний зв'язок між реальною її доступністю та режимом доступу до неї і, відповідно, доступність інформації обумовлена не лише її юридичним статусом, а й фактичними умовами її використання для різних суб'єктів [2] та специфікою сфери публічної фінансової діяльності. Так, відповідно до ст. 21 ПК України посадові особи контролюючих органів зобов'язані не допускати розголошення

інформації з обмеженим доступом, що одержується, використовується, зберігається під час реалізації функцій, покладених на такі органи, а також надавати органам державної влади та органам місцевого самоврядування на їх письмовий запит відкриту податкову інформацію в порядку, встановленому законом. Разом з тим, у ст. 5 Закону України «Про доступ до публічної інформації» визначено особливості використання публічної інформації з обмеженим доступом і виключний перелік інформації, до якої не може бути обмежено доступ і яка стосується: розпорядження бюджетними коштами; володіння, користування чи розпорядження державним, комунальним майном; умов отримання цих коштів чи майна тощо. Однак аналізована стаття містить застереження, що зазначені положення не поширюється на випадки, коли оприлюднення або надання такої інформації може завдати шкоди інтересам національної безпеки, оборони, розслідуванню чи запобіганню злочину.

Безперечно, надзвичайно важливим стало прийняття Закону України «Про відкритість використання публічних коштів», який визначив умови та порядок забезпечення доступу до інформації про використання публічних коштів розпорядниками та одержувачами коштів державного і місцевих бюджетів, суб'єктами господарювання державної і комунальної власності, фондами загальнообов'язкового державного соціального страхування. Відповідно до цього Закону зазначена інформація готується розпорядниками та одержувачами коштів Державного бюджету України, бюджету Автономної Республіки Крим і місцевих бюджетів, органами Пенсійного фонду, підприємствами, а також фондами загальнообов'язкового державного соціального страхування та подається ними для оприлюднення на єдиному веб-порталі використання публічних коштів.

Також особливого захисту потребує інформація даних про платників податків, відповідно контролюючі органи мають забезпечити достовірність таких даних в Єдиному банку даних про платників податків - юридичних осіб та Державному реєстрі фізичних осіб - платників податків, реєстрі платників податку на додану вартість, реєстрі неприбуткових організацій та інших реєстрах, що формуються та ведуться контролюючими органами згідно з ПК України, їх захист від несанкціонованого доступу, оновлення, архівування та відновлення даних.

З урахуванням зазначеного, основними проблемами забезпечення інформаційної безпеки сфери публічної фінансової діяльності вважаємо неузгодженість правових норм різних законів України щодо доступу до інформації у цій сфері, її захисту, а також відсутність норм, які б містили чіткі механізми реалізації таких норм, забезпечення права на доступ до інформації у сфері публічної фінансової діяльності, контроль за реалізацією цього права, притягнення до відповідальності посадових осіб за недотри-

мання чинного законодавства, що регулює відносини у сфері забезпечення доступу до такої інформації та її захисту.

Подальші дослідження доцільно спрямувати на теоретико-методологічне обґрунтування особливостей забезпечення інформаційної безпеки у окремих сферах публічної фінансової діяльності – бюджетній, податковій, банківській.

**Література**

1. Дмитренко Е.С. Місце інформаційного забезпечення у системі фінансової безпеки держави / Е. С. Дмитренко // Інформаційна безпека людини, суспільства, держави. – 2011. – №3 (7). – С. 13-17.

2. Дмитренко Е.С. Реалізація права на податкову інформацію у контексті Податкового кодексу України / Е. С. Дмитренко // Інформаційна безпека людини, суспільства, держави. – 2012. – № 2 (9). – С. 99-104.

*УДК 340.134::351*

**Дмитренко Ю. П.**
кандидат юридичних наук, професор
Національна академія СБ України

## СОЦІАЛЬНО-ПРАВОВІ ПРОБЛЕМИ КОМПЛЕКТУВАННЯ ПІДРОЗДІЛІВ СУБ'ЄКТІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ І КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ТА ШЛЯХИ ЇХ ВИРІШЕННЯ

В умовах глобалізації інформаційних процесів, їх інтеграції в різні сфери суспільного життя у багатьох державах приділяється значна увага створенню та удосконаленню ефективних систем захисту критичної інфраструктури від зовнішніх та внутрішніх загроз кібернетичного характеру.

У провідних країнах світу вже сформовані загальнодержавні системи кібернетичної безпеки – як найбільш оптимальні організаційно-функціональні структури, що здатні в короткий проміжок часу акумулювати сили та засоби різних державних органів і приватного сектору для протидії кіберзагрозам [1, с. 312]. В Україні також відбувається становлення системи забезпечення кібернетичної безпеки. Проте, вірус Petya, яким було вражено значну кількість інформаційних ресурсів органів державної влади України, показав недосконалість національної системи кібербезпеки, виявив суттєві недоліки в організації діяльності кадрового забезпечення її суб'єктів. Приклади кібератак зі спробами втручання в електронну виборчу систему, зокрема під час проведення виборів у різних країнах (навіть США та ін.) визначають надзвичайну актуальність цієї теми. В умовах ведення «гібридної війни» Російською Федерацією проти Украї-

ни, економічних та соціальних проблем необхідність у кваліфікованих кадрах у цій сфері постійно зростає. Від професіоналізму, компетентності, сумлінної праці, дисциплінованості та відповідальності кадрів, а зокрема керівників як суб'єктів управління, залежить успіх діяльності у будь-якій сфері. Особливо це стосується питань забезпечення інформаційної та кібернетичної безпеки.

СБ України також належить до суб'єктів забезпечення інформаційної та кібернетичної безпеки, де існує проблема якісного кадрового забезпечення. Метою кадрового забезпечення службової діяльності є своєчасне, ефективне комплектування підрозділів професіоналами, формування і збереження кадрового резерву, постійне підвищення професійного рівня співробітників, удосконалення механізму раціонального використання кадрового потенціалу СБ України, який відповідає покладеним на підрозділи органів і закладів завдань та забезпечує їх ефективне виконання.

На сьогодні існує проблема якісного комплектування і підрозділів СБ України у зазначеній галузі співробітниками-фахівцями, спроможними виконувати покладені чинним законодавством завдання з ефективного забезпечення державної безпеки в сучасних, зокрема в екстремальних умовах. Найбільшою проблемою залучення високопрофесійних фахівців до служби (роботи) в підрозділи суб'єктів забезпечення інформаційної та кібернетичної безпеки держави є недостатній рівень пропонованого грошового забезпечення за відповідними посадами. Як відомо співробітники ІТ сфери на сьогодні є одними з найбільш високооплачуваних фахівців у світі, тому питання їх мотивації при комплектуванні державних структур є далеко не останнім. На жаль, значна кількість фахівців ІТ сфери нині з України виїжджає на роботу за кордон.

На сьогодні критерії відбору до кандидатів на службу (роботу) в СБ України є досить високими. Так, під час роботи з кандидатами на службу (роботу, навчання) в СБ України керівниками підрозділів та органів СБУ повинна акцентуватися увага на: якісному відборі кадрів, з врахуванням професійно-ділових та особистих (зокрема, моральних) якостей кандидатів на службу (роботу, навчання); доведення об'єктивної інформації щодо питань фактичного соціального захисту співробітників, а в подальшому - у наданні практичної допомоги молодим співробітникам у період їх становлення та ін. Тому з метою вирішення цього питання важливе значення поряд із патріотичною складовою має встановлення високих соціальних гарантій для співробітників і, відповідно, створення конкурсу при комплектуванні підрозділів спецслужби та інших державних органів системи забезпечення інформаційної та кібернетичної безпеки.

У контексті інтеграції до європейського правового простору, в Україні здійснюється реформування і сфери соціального захисту. Однак під час

цього процесу, що характеризується руйнуванням існуючої системи захисту населення і відсутністю нових ефективних її форм, недостатністю бюджетного фінансування, окремі групи громадян, до яких з-поміж інших слід віднести і співробітників спецслужби та особливо пенсіонерів, які опинилися у не простому становищі.

Багато бажаючих кандидатів на службу (роботу) не відповідають за своїми професійними та особистими якостями встановленим вимогам. Складається ситуація: кому пропонують - не бажають служити, хто бажає служити – не завжди відповідає за станом здоров'я, особистими та професійними якостями встановленим вимогам.

Одним із виходів із ситуації, що склалася є підготовка кадрів для системи забезпечення інформаційної і кібернетичної безпеки. Проте, одночасно повинні бути створені і високі соціальні гарантії для професіоналів, інакше досвідчені працівники все одно, з часом, будуть звільнятись. Отже, вищевикладений аналіз ситуації, яка склалася на практиці з проблем комплектування підрозділів установ системи забезпечення інформаційної і кібернетичної безпеки, дає підстави зробити *висновки:* з метою підвищення рівня якісного складу кандидатів на службу (роботу) системи забезпечення інформаційної і кібернетичної безпеки необхідно підвищити рівень соціальних гарантій (повинен бути значно вищий ніж у інших співробітників військових формувань); встановити доплати досвідченим співробітникам підрозділів (наставникам), що відбирають кандидатів на службу (роботу), в подальшому навчають молодих співробітників (працівників); закріпити у нормативних актах обов'язкове відпрацювання (служби) випускників навчальних закладів (молодих спеціалістів) у підрозділах, які їх відбирали (не менше 3 роки). Зазначені заходи сприятимуть позитивній стабілізації питання укомплектованості відповідних підрозділів та підвищенню ефективності їх роботи.

**Література**

1. Шеломенцев В. П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення / В. П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2012. – Вип. 1. – С. 312-320.

2. Ліпкан В. А. Національна система кібербезпеки як складова системи забезпечення національної безпеки України / В. А. Ліпкан, І. В. Діордіца [Електронний ресурс]. – Режим доступу : http://goal-int.org/natsionalna-sistema-kiberbezpeki-yak-skladovoyi-sistemi-zabezpechennya-natsionalnoyi-bezpeki-ukrayini/.

*УДК 351.86 (477)*
**Довгань О.Д.**
доктор юридичних наук, с.н.с.
Науково-дослідний інститут інформатики і права
Національної академії правових наук України

# ЩОДО ДЕЯКИХ ПРАВОВИХ АСПЕКТІВ КУЛЬТУРИ КІБЕРБЕЗПЕКИ

Протягом усього періоду розвитку людської цивілізації життя людей постійно змінювалося, наповнюючись розвитком і широким використанням усе нових інформаційно-комунікаційних технологій. Перехід до інформаційного суспільства вимагало наявності таких його членів, які могли б ефективно жити і працювати в умовах, коли інформація, знання, інформаційно-комунікаційні технології стають важливим ресурсом та рушійною силою соціально-економічного, технологічного і культурного розвитку суспільства. Зазначене вказує на те, що кожна сучасна людина повинна мати відповідний рівень інформатичної компетентності й інформаційної культури. Тобто має бути готовою до освоєння нового способу життя на базі використання інформації, побудови нової (інформаційної) картини світу і визначення свого місця у ньому, при цьому вміти вибрати з величезного масиву інформації найбільш важливу і потрібну. Інформаційна культура, як частина загальної культури особистості, повинна засвоїти етику і естетику, ергономіку і питання інформаційної безпеки *(як у сенсі захисту інформації, так і в сенсі захисту людської психіки)*. Інформаційна культура, будучи пов'язаною з соціальною природою людини, є продуктом його різноманітних творчих здібностей і проявляється в таких аспектах: в конкретних навичках по використанню технічних пристроїв *(від телефону до персонального комп'ютера і комп'ютерних мереж)*; у здатності використовувати у своїй діяльності інформаційні технології; в умінні збирати інформацію з різних джерел: як з періодичної преси, так і з електронних комунікацій, представляти її в зрозумілому вигляді і вміти ефективно її використовувати; у володінні основами аналітичної переробки інформації; в умінні працювати з різною інформацією; у знанні особливостей інформаційних потоків у певній галузі діяльності.

Крім того, інформаційна культура, включаючи інформатичну компетентність людини, також передбачає: високий рівень культури міжособистісного спілкування; готовність толерантно сприймати іншу точку зору; вміння аргументовано вести дискусії, готовність визнати себе переможеним у цій дискусії; готовність не тільки отримувати нові знання, а й ділитися своїми; знання норм і правил, що регламентують використання інтелектуальної власності і готовність користуватися ними тощо.

Ряд прийнятих резолюцій Генеральної Асамблеї ООН стосувалися, зокрема й питань глобальної культури кібербезпеки. Так, у Резолюції Генеральної Асамблеї ООН A/RES/57/239 від 20 грудня 2002 року "Створення глобальної культури кібербезпеки (Creation of a global culture of cybersecurity), уперше було використано поняття кібербезпека. Розгляд теми кібербезпеки продовжився у Резолюціях A/RES/58/199 "Створення глобальної культури кібербезпеки та захист найважливіших інформаційних інфраструктур" 2003 року [1] та A/RES/64/211 "Створення глобальної культури кібербезпеки та оцінка національних зусиль по захисту найважливіших інформаційних інфраструктур" 2009 року [2]. У термінології, яку використовує ООН, мова йшла про глобальну культуру кібербезпеки, для визначення якої, було запропоновано дев'ять взаємопов'язаних елементів: *обізнаність* (тобто учасники повинні бути обізнані щодо необхідності безпеки інформаційних систем та мереж, а також про те, що вони можуть здійснити для підвищення безпеки); *відповідальність* (учасники відповідають за безпеку мереж відповідно до власної ролі); *реагування* (учасники мають вживати своєчасних та спільних заходів щодо попередження інцидентів, які стосуються безпеки, їх виявленню та реагуванню, у тому числі обмінюватись інформацією і вводити процедури, які передбачають оперативне та ефективне співробітництво з попередження, виявлення та реагування на такі інциденти); *етика* (врахування законних інтересів інших); *демократія* (безпека повинна забезпечуватись таким чином, щоб це відповідало демократичним цінностям, включаючи свободу обміну думками та ідеями, вільний потік інформації, конфіденційність інформації, належний захист приватної інформації; відкритість та гласність); *оцінка ризиків* (учасники повинні здійснювати періодичну оцінку ризиків з метою виявлення загроз та факторів уразливості, мати належні технології та інструменти контролю для цього, з урахуванням значущості інформації, яка захищається); *проектування та впровадження засобів забезпечення безпеки*; *переоцінка* (належні та своєчасні заходи з внесення змін у політику, практику забезпечення безпеки з урахуванням нових та зміни існуючих загроз) [3].

Враховуючи, те, що вирішення проблемних питань у сфері кібербезпеки є надзвичайно актуальними в контексті розвитку інформаційного суспільства, зростання кіберзлочинності, використання засобів кібертероризму у гібридних війнах та необхідності розбудови системи забезпечення кібернетичної безпеки України, дотримання культури кібербезпеки має велике значення.

Кожен з нас повинен мати необхідний рівень інформатичної компетентності й інформаційної культури, особливо при використанні засобів інформаційно-комунікаційних технологій. Основною вимогою сьогодення для кожного члена суспільства має стати підвищення рівня власної інформаційної культури та розвивати її протягом усього життя.

**Література**

1. Резолюция Генеральной Ассамблеи ООН 58/199, принятая на 78 пленарном заседании 58-й сессии. 23 декабря 2003 года URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N03/506/54/PDF/N0350654.pdf?OpenElement (дата звернення: 27.02.2018).

2. Резолюция Генеральной Ассамблеи ООН 64/211, принятая на 66 пленарном заседании 64-й сессии. 21 декабря 2009 года URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N09/474/51/PDF/N0947451.pdf?OpenElement (дата звернення: 28.02.2018).

3. Довгань О.Д. Розвиток законодавства у сфері кібербезпеки: інформаційно-правове дослідження / О.Д.Довгань, І.М.Доронін // Науковий часопис Національного педагогічного університету ім. М.П.Драгоманова. – Серія №18. Право: зб. наукових праць. – Вип. 32. – К., 2017. – С. 91-101.

*УДК 340.134::351.86 (477)+35.074 (477)*

**Доронін І.М.**
кандидат юридичних наук, доцент
НДІІ інформатики і права НАПрН України

## ПРАВОВІ ПРОБЛЕМИ ВИЗНАЧЕННЯ КОМПЕТЕНЦІЇ СУБ'ЄКТІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

Правові новації, пов'язані з ухваленням Закону України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року (набуває чинності 9 травня 2018 року), ще не стали предметом наукової дискусії. Попередні оцінки змісту законодавчого акту та досить жвава політична і фахова дискусія на етапі його ухвалення свідчили про існування проблем насамперед щодо повноважень державних (у першу чергу – правоохоронних) органів стосовно суб'єктів надання телекомунікаційних послуг. Водночас, система управління у цій сфері, яка має бути побудована на виконання вимог зазначеного спеціального законодавчого акту, серйозно не розглядались, хоча навіть побіжний аналіз законодавчих новацій дозволяє прийти до висновків про необхідність законодавчих узгоджень у майбутньому.

Найперше слід розглянути загальну систему державних органів, відповідальних за забезпечення кібербезпеки, так як вона визначена у самому законодавчому акті.

Закон по-різному розуміє значення термінів «кібербезпека» і «кіберзахист». Суттю першого терміну є поняття «захищеності» подібно до розуміння, що було закладено Законом України «Про основи національної

безпеки України» для поняття «національна безпека» у 2003 році. Суттю терміну «кіберзахист» є поняття «сукупність заходів», що характерне для роз'яснення поняття відповідної «діяльності» за аналогією із законодавчими визначеннями для оперативно-розшукової діяльності («система заходів» згідно ст. 2 Закону України «Про оперативно-розшукову діяльність» від 18.02.1992, що не змінювалась у подальшому), або контррозвідувальної діяльності (діяльність, що здійснюється з використанням «системи заходів» відповідно до визначеного у ст.1 Закону України «Про контррозвідувальну діяльність»). Термін «сукупність» відрізняється від терміну «система» і тому питання про те, чи мають становити заходи з кіберзахисту певну систему неодмінно виникне у подальшому під час реалізації положень Закону в практичній діяльності.

Заклавши термінологічний дуалізм у питанні кібербезпеки та кіберзахисту, законодавець визначив також і дві системи суб'єктів забезпечення. Мова йде про суб'єктів забезпечення кібербезпеки (ст. 5 Закону) та суб'єктів Національної системи кібербезпеки (ст. 8 Закону).

Суб'єктний склад щодо забезпечення кібербезпеки досить значний, але повноваження, що надані їм, обмежуватимуться визначеною для кожного суб'єкта спеціальним законодавством компетенцією. Отже, фактично суб'єктам кібербезпеки додаткових повноважень Законом України «Про основні засади забезпечення кібербезпеки України» порівняно із повноваженнями, визначеними для них спеціальними нормативно-правовими актами, не надано. Таким чином, мова у частині 5 статті 5 зазначеного Закону йде про завдання для цих суб'єктів, а не про їхні повноваження. До числа цих завдань належать:

1) здійснення заходів щодо запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях;

2) виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків;

3) інформаційний обмін щодо реалізованих та потенційних кіберзагроз;

4) розробка і реалізація запобіжних, організаційних, освітніх та інших заходів у сфері кібербезпеки, кібероборони та кіберзахисту;

5) забезпечення проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об'єктах та об'єктах, що належать до сфери їх управління.

Законом передбачено і здійснення інших необхідних заходів.

Слід зазначити, що завдання забезпечення кібербезпеки та кіберзахисту багато в чому повторюються, хоч заходи кіберзахисту містять у собі більш вагому технічну та організаційну складову.

Законом введено також новий термін – «Національна система кібербезпеки», яка згідно з наданими законодавчо дефініціями є одночасно су-

купністю суб'єктів та сукупністю заходів. Конкретні повноваження суб'єктів Національної системи визначатимуться з урахуванням приписів спеціального законодавства, яке визначає їх компетенцію. Суб'єктний склад Національної системи дещо інший порівняно з суб'єктами забезпечення кібербезпеки – її головним органом по суті визначено Державну службу спеціального зв'язку та захисту інформації України (ДССЗЗІ). Визначення цього державного органу зумовило виникнення низки питань, що складатимуть проблемне поле у правозастосуванні.

До числа них належать насамперед особливості статусу Державної служби спеціального зв'язку та технічного захисту інформації, що згідно з вимогами спеціального законодавчого акту про неї, є державним органом (до складу якого входить центральний орган виконавчої влади - Адміністрація), який формує та реалізує державну політику в певній сфері. Але згідно з вимогами ч. 1 ст. 1 Закону України «Про центральні органи виконавчої влади» формують державну політику тільки Міністерства, а згадана Державна служба не входить до складу жодного міністерства ані прямо, ані опосередковано.

Державний центр кіберзахисту (разом з Урядовою командою CERT) має діяти за умови забезпечення його функціонування з боку ДССЗЗІ, при цьому їх завдання хоча і визначені у тексті Закону (ст. 8 і 9), але окремі повноваження цім органам не надані, отже виконання завдань буде організовано з урахуванням повноважень, законодавчо наданих Державній службі спеціального зв'язку та технічного захисту інформації, правовий статус якої з формування державної політики не повністю відповідає вимогам чинного законодавства. Слід також зазначити, що ДССЗЗІ на сьогодні має контрольні, регуляторні, технічні та адміністративні повноваження, але не повноваження правоохоронного органу.

*УДК 351.86(477)*

**Дралюк І.М.**
кандидат юридичних наук
заступник начальника Головного управління «К»
СБ України

## ВНУТРІШНІ ЗАГРОЗИ БЕЗПЕЦІ ДЕРЖАВНОГО УПРАВЛІННЯ УКРАЇНИ

Шлях здобуття незалежності та становлення нашої держави виявився досить складним процесом. «Україна наприкінці XX ст. подолала тривалу внутрішню економічну кризу, але, майже через п'ять років, потрапила в

політичну кризу, яка супроводжувалася різними проблемними ситуаціями, пов'язаними з питаннями газу, бензину, цукру, інноваційних технологій і т.д., негативні наслідки якої для країни ще до кінця не з'ясовані. У зв'язку з цим виникає низка питань щодо якості управлінських рішень, які приймалися й приймаються на різних етапах керівниками різних рангів у різних органах існуючих гілок влади» [1].

Окремими авторами Національної академії СБ України ще у 2009-2011 роках було опубліковано низку проблемних матеріалів в галузі управління інформаційною безпекою[2-4]. Тоді велась мова здебільшого про внутрішні загрози, які залежали значною мірою від нас. Тепер же вони переросли переважно у зовнішні загрози, які нанесли збитки територіальній цілісності України і призвели до необхідності із зброєю в руках відстоювати незалежність держави. Сьогоднішня Сратегія національної безпеки [3] не поділяє загроз на внутрішні й зовнішні, а виділяє лише найбільш суттєві у цій сфері, де головною ланкою є державне управління. А тому ці загрози складають основу загроз державного управління, а їх поділ на зовнішні та внутрішні дасть можливість відстежити часову динаміку їхніх змін. Загрози державному управлінню можуть класифікуватися і за іншими ознаками: за часом – довготривалі, короткотривалі і тимчасові; за місцем поширення – місцеві, регіональні, загальнодержавні; за наслідками – локальні, маштабні, катастрофічні тощо.

Національною академією державного управління при Президентові України розроблено та запропоновано власне бачення дефініції *«управлінська безпека»,* згідно з якою під цим поняттям пропонується розуміти «стан внутрішніх і зовнішніх умов діяльності керівника в сфері державного управління, що нейтралізують або виключають можливість вироблення, прийняття й реалізації управлінських рішень, які можуть привести до негативних наслідків для держави й суспільства в різних сферах, у тому числі в зовнішньополітичній» [1].

Сьогодні перед Україною відкрито нові можливості для побудови системи державного управління національною безпекою, а також відносин між громадянином і державою, на що спрямована Стратегія національної безпеки України, оголошена Указом Президента України від 06.05.2015 «Про рішення Ради національної безпеки і оборони України». Стратегія визначає актуальні на сьогодні загрози національній безпеці України [5]. Серед внутрішніх загроз виділено:

*Неефективність системи забезпечення національної безпеки і оборони України*, а саме несформованість сектору безпеки і оборони України як цілісного функціонального об'єднання, керованого з центру; інституційна слабкість, непрофесійність, структурна незбалансованість органів сектору безпеки і оборони; недостатність ресурсного забезпечення та неефективне використання ресурсів у секторі безпеки і оборони; відсутність ефектив-

них зовнішніх гарантій безпеки України; діяльність незаконних збройних формувань, зростання злочинності, незаконне використання вогнепальної зброї.

*Корупція та неефективна система державного управління: поширення корупції*, її укорінення в усіх сферах державного управління; дисфункціональність, застаріла модель публічних інститутів, депрофесіоналізація та деградація державної служби; здійснення державними органами діяльності в корпоративних та особистих інтересах, що призводить до порушення прав, свобод і законних інтересів громадян та суб'єктів господарської діяльності.

*Економічна криза, виснаження фінансових ресурсів держави, зниження рівня життя населення*: монопольно-олігархічна, низькотехнологічна, ресурсовитратна економічна модель; відсутність чітко визначених стратегічних цілей, пріоритетних напрямів і завдань соціально-економічного, воєнно-економічного та науково-технічного розвитку України; високий рівень "тінізації" та криміналізації національної економіки, кримінально-кланова система розподілу суспільних ресурсів; деформоване державне регулювання і корупційний тиск на бізнес; надмірна залежність національної економіки від зовнішніх ринків; неефективне управління державним боргом; зростання рівня безробіття; активізація міграційних процесів унаслідок бойових дій; руйнування економіки та систем життєзабезпечення на тимчасово окупованих територіях, втрата їх людського потенціалу, незаконне вивезення виробничих фондів на територію Росії.

*Загрози енергетичній безпеці*: спотворення ринкових механізмів в енергетичному секторі; криміналізація та корумпованість енергетичної сфери; недієва політика енергоефективності та енергозабезпечення.

*Загрози 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.

*Загрози екологічній безпеці*: надмірний антропогенний вплив і високий рівень техногенного навантаження на територію України; негативні екологічні наслідки Чорнобильської катастрофи; незадовільний стан єдиної державної системи та сил цивільного захисту, системи моніторингу довкілля.

А також *загрози інформаційній безпеці*: ведення інформаційної війни проти України; відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства.

*Загрози 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.

Як бачимо, Стратегія хоча й не поділяє ризики на внутрішні та зовнішні, доволі повно рокриває їх зміст. В той же час вона не виділяє такого небезпечного і дуже поширеного в державі ризику, яким для України останнім часом є *екстремізм*, дослідженню стану протидії якому приділяється прискіплива увага з боку правоохоронних органів. В Україні сьогодні серйозну загрозу представляють кримінальний, політичний, молодіжний, релігійний та етнічний екстремізм. Основними рисами сучасного екстремізму є: нетерпимість до інших поглядів, переконань, вірувань тощо; застосування дій насильницького характеру; ірраціональність та емоційність; поляризація світосприйняття добро-зло. Сьогодні в Україні екстремізм – це діяльність фізичної чи юридичної особи або об'єднання громадян чи їхні публічні заклики або підбурювання, спрямоване на посягання на основи конституційного ладу та національної безпеки, порушення прав, свобод та законних інтересів людини і громадянина. Ми відносимо екстремізм одночасно до зовнішніх та внутрішніх загроз, оскільки він, як і тероризм та сепаратизм, часто формується, фінансується та спрямовується із зовнішніх джерел та в їхніх інтересах, а співучасниками злочинної діяльності є переважно громадяни України.

Узагальнюючи викладені позиції, можна дійти наступного висновку. Безпека державного управління – це стан гарантованого захисту механізму та апарату державного управління України від зовнішніх та внутрішніх загроз, які виходять від іноземних військових формувань, спецслужб, а також внутрішніх екстремістських об'єднань, злочинних співтовариств, груп і окремих осіб. Такий стан забезпечує своєчасне виявлення й нейтралізацію загроз у сфері державного управління як на рівні органів законодавчої, виконавчої і судової влади, так і в окремих регіонах, а також проведення кадрової політики в інтересах держави, уникаючи управлінських конфліктів, ризиків та викликів. Безпека державного управління в сьогоднішніх умовах є головною ланкою в системі національної безпеки, оскільки від її стану та надійної захищеності залежить доля і майбутнє незалежної держави, суспільства й кожного без винятку громадянина, як основних об'єктів національної безпеки. Надійна безпека державного управління дає змогу здійснити комплекс взаємопов'язаних, об'єднаних єдиним задумом, науково обґрунтованих заходів, які базуються на положеннях Конституції України, Стратегії національної безпеки України, законодавства в сфері державного управління.

**Література**

1. Мосов С.П. Концептуальний підхід до управлінської безпеки в системі державного управління в Україні / Н. Р. Нижник, С. П. Мосов // Університетські наукові записки. – 2012. – № 2 (42). – С. 44-50.

2. Стрельбицький М.П. Державне управління крізь призму інформаційної безпеки України / Стрельбицька Л.М., Стрельбицький М.П. // Інформаційна безпека людини, суспільства держави». – 2009. – № 2(2). – С. 53-56.

3. Стрельбицький М.П. Інформаційний тероризм та кіберзлочини: природа і наслідки / Стрельбицька Л.М., Стрельбицький М.П. // Інформаційна безпека людини, суспільства держави». – 2011. – № 2(6). – С. 90-95.

4. Стрельбицький М.П. Інформаційна безпека у сфері державного управління / Стрельбицька Л.М., Стрельбицький М.П. // Юридичний вісник України. – 11-17 вересня 2010. – № 37(793). – С. 6-7.

5. Указ Президента України Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України", № 287/2015, 26.05.2015.

*УДК 349, 323, 355/359*

**Єрменчук О.П.**
кандидат юридичних наук
Служба безпеки України

## ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНА СКЛАДОВА ДЕРЖАВНО-ПРИВАТНОГО ПАРТНЕРСТВА У ЗАХИСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЯК ВАЖЛИВИЙ ЕЛЕМЕНТ ЗАБЕЗПЕЧЕННЯ ДЕРЖАВНОЇ БЕЗПЕКИ

Захист критичної інфраструктури безпосередньо впливає на національну безпеку та реалізацію однієї із основних функцій держави, яка полягає у забезпеченні суверенності влади, оскільки формує здатність державного апарату ефективно та з урахуванням національних інтересів вирішувати внутрішні та зовнішні справи.

Безумовно, в цьому процесі належне місце має посісти і відповідна діяльність СБ України, як це передбачено її задачами визначеними ст. 2, 24 Закону України "Про СБ України". Важливо вказати, що Директивою Ради ЄС від 08.12.2008 № 2008/114/ЄС зобов'язано всіх членів ЄС на законодавчому рівні належно закріпити питання організації захисту критичної інфраструктури. Для України, яка визначила курс вступу до ЄС одним із пріоритетних, відповідність законодавства європейським стандартам теж є важливим аспектом.

Ефективний захист критичної інфраструктури можливий лише за умов досить глибокої інтегрованої взаємодії державного та приватного сектору, їх партнерства заснованого на двосторонній вигоді у забезпеченні безпеки та стійкості критичної інфраструктури [1]. У контексті цього, *"партнерство"* визначається як тісна співпраця між сторонами, які мають спільні інтереси у досягненні єдиної мети. Співпраця між державним та приватним секторами має ґрунтуватися на надійній взаємодії, де процеси

обміну інформацією мають позитивний вплив на діяльність об'єктів інфраструктури та організацію і спрощення відповідної роботи державного сектору, відбуваються відкрито і зрозуміло, захищаючи приватність та громадянські свободи.

Так, в Концепції основних заходів захисту критичної інфраструктури, розроблених німецьким Федеральним міністерством внутрішніх справ (Bundesministerium des Innern) для власників та керівників підприємств передбачено економічне обґрунтування по забезпеченню безпеки. У обґрунтуванні серед переваг для операторів критичної інфраструктури зазначена така вигода: збільшення доходів; спрощення обмежень; захист сегмента ринку; ризик-менеджмент; захист технологій та товарних знаків [2].

В процесі партнерства держава має бути гарантом внутрішньої безпеки та виступати в ролі посередника в інформаційних та комунікаційних процесах, при цьому приватний сектор володіє інформацією щодо актуальних ризиків та загроз їх функціонуванню, що при налагодженому процесі обміну дозволить державі застосовувати ефективні конкретні заходи із захисту.

Взаємодія між партнерами має відбуватися в рамках *національного плану* де мають бути передбачені спільні державно-приватні інтереси у забезпеченні безпеки та стійкості критичної інфраструктури.

Так, у США, згідно положень національного плану (NIPP – National Infrastructure Protection Plan) передбачено необхідність учасників-партнерів колективно визначати національні пріоритети та формулювати чіткі заходи задля пом'якшення ризиків, прогнозувати та аналізувати прогрес і вигоду та відслідковувати зворотній зв'язок [1]. В свою чергу, національний план є формою організації національних зусиль, він сприяє залученню широкого кола учасників-партнерів до розуміння важливості забезпечення безпеки і стійкості критично важливої інфраструктури. Крім того, сприяє підвищенню ефективності роботи органів державної влади, органів безпеки та приватного сектору пліч о пліч для досягнення соціально-економічного процвітання нації.

Як *висновки* можна зазначити, що саме інформаційно-комунікаційна складова у державно-приватному партнерстві під час захисту критичної інфраструктури має стати взаємовигідним фактором, що сприятиме взаємним інтеграційним процесам та забезпеченню державної безпеки.

На нашу думку, взаємна зацікавленість від партнерства держави та операторів критичної інфраструктури може полягати у наступному:

- державні органи можуть надавати доступ до наявної своєчасної, достовірної та найбільш повної інформації про загрози;
- державні органи можуть надавати дані операторам критичної інфраструктури щодо різних варіацій ризиків та тенденцій розвитку ситуації у певному сегменті внутрішнього чи зовнішнього ринку;
- державні органи можуть надавати детальну інформацію щодо ризиків чим забезпечують свій вклад у захист об'єктів КІ, що значиться на інвестиціях в безпеку та стійкість з боку операторів;

- оператори критичної інфраструктури можуть отримувати достовірну інформацію щодо об'єктів та суб'єктів інвестиційної зацікавленості для вжиття заходів з покращення інвестиційної діяльності;

- оператори критичної інфраструктури можуть впливати на дієвість та ефективність планів державних органів по забезпеченню безпеки та стійкості в їх сферах діяльності;

- оператори критичної інфраструктури, які займаються господарською діяльністю, за умов тісної взаємодії з державними органами у сфері захисту критичної інфраструктури, можуть якісно організувати роботу та підвищити прибуток. В свою чергу збільшення їх прибутку є прямо пропорційним вигоді держави із сплати ними податку з прибутку.

В свою чергу, СБ України виконуючи властиві їй, передбачені законодавством функції з інформаційно-аналітичного забезпечення в інтересах ефективної діяльності органів державної влади та управління, а також недопущення загроз державній безпеці, має стати об'єктивним та незалежним інструментом отримання інформації з об'єктів критичної інфраструктури та передачі її органам управління і навпаки, цим самим сприяючи забезпеченню захищеності критичної інфраструктури та державній безпеці.

**Література**

1. NIPP 2013 Partnering for Critical Infrastructure. Security and Resilience. [Електронний ресурс]. – Режим доступу: https://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience.

2. Защита критической инфраструктуры. Концепция основных мер защиты. Рекомендация для предприятий. – Bundesministerium des Innern, 2006. – [Електронний ресурс]. – Режим доступу: www.bmi.bund.de.

*УДК 007.51 (477)*

**Жиляєв І. Б.**
доктор економічних наук, старшій науковий співробітник
Науково-дослідний інститут інформатики і права
**Семенченко А. І.**
доктор наук з державного управління, професор
Національна академія державного управління
при Президентові України

## ОРГАНІЗАЦІЙНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ РОЗВИТКУ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ УКРАЇНИ: СТАН ТА ПЕРСПЕКТИВИ

1. Проблема формування сучасної національної системи кібербезпеки актуалізується: збільшується кількість, складність, масштабність та комплексність застосування кіберінцидентів, як на глобальному, регіонально-

му, національному рівнях, так й на рівні окремих бізнес-структур та інституцій громадянського суспільства, людини і громадянина. Стрімко нарощується масив як законодавчих актів, спрямованих на забезпечення кібербезпеки, накопичуються конкретні організаційні інструменти кіберстійкості.

2. В Україні почалося формування національної політики кібербезпеки, яка включає сукупність національних та міжнародних актів, насамперед: Конвенцію про кіберзлочинність, ратифікованої Законом України від 07.09.2005 р. № 2824-IV; Стратегією кібербезпеки України; Закон України «Про основні засади забезпечення кібербезпеки України»; Рішення Ради національної безпеки і оборони України від 29.12.2016 р. «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації»; Порядк формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави, затвердженим постановою Кабінету Міністрів України від 23.08.2016 р. № 563 тощо.

3. Однак, сформована національна політика кібербезпеки має певні суттєві розбіжності за спрямуванням та змістом з європейською політикою, у тому числі з оновленою версією Стратегії кібербезпеки ЄС 2013 р.

До основних недоліків чинного національного законодавчого розбудови національної системи кібербезпеки можна віднести:

проблему цільополагання: незважаючи на декларування захисту людини та громадянина, їх основних прав, свободи слова, персональних даних та конфіденційності цей розділ законодавства, насамперед зосереджений на захисті інтересів органів державної влади (фактично не вирішена проблема системності кіберзахисту всіх об'єктів національної системи кібербезпеки: людини/громадянина; бізнесу; органів публічної влади; в цілому держави, зокрема – в особливих сучасних умовах (війна / «гібридна війна») тощо;

значне «відставання» від світової практики законодавчого регулювання кібезбезпеки: так станом на 4 березня 2018 року на офіційному сайті європейського права http://eur-lex.europa.eu/ з цього питання було розміщено більш ніж 4 сотні юридичних документів, з них 31 – виданих у 2018 році. Проблема погіршується зволіканням з імплементацією – так, певна кількість норм Конвенції про кіберзлочинність за 12 років не була запроваджена. Цей правовий «цифровий розрив» збільшується як кількісно, але насамперед – якісно;

фрагментарність формування правової основи національної кібербезпеки – більша частина існуючих нормативно-правових актів (та тих, що розробляється) регулювання у сфері безпеки та інформаційних технологій навіть не згадують цю проблему (одним з прикладів є нещодавно схвалена урядова Концепція розвитку цифрової економіки та суспільства України на 2018-2020 роки, іншим – проект Закону про внесення змін до деяких законодавчих актів України щодо боротьби з тероризмом (реєстр. № 6438 від 12.05.2017, поданий Кабінетом Міністрів України), який пропонує внормовати діяльність з боротьби з актами ядерного тероризму без урахування загроз кібератак);

намаганні побудови ієрархічної організаційної структури управління кібезбезпекою країни, якій протидіють мережеві структури кіберзлочинців, перш за все – міжнародні та іноземні (протистояння за принципом «ієрархія проти мережі»);

опори на державні структури, які мають адміністративно-командно забезпечувати діяльність всіх суб'єктів кібербезпеки в країні (забувається, що об'єктів національної системи критичної інфраструктури є у приватній, а не у державній власності) – через директивні акти, а не шляхом рекомендаційних актів; не відбувається формування чіткої, відповідальної системи кібербезпеки рівноправних суб'єктів всіх форм власності; не сформованість системи державно-приватного партнерства у цій сфері;

відсутності централізованого фінансування комплексних проектів кібербезпеки, організації розробки та впровадження типових рішень (процедур і заходів) забезпечення кібербезпеки;

неекономічність – не беруться до уваги як економічні наслідки кіберінцидентів, так й ефективність пропонованих заходів (витрати – результати);

недостатню обґрунтованість – не передбачено включення (немає посилань на роль та місце) науки та інновацій, в той час як Стратегія кібербезпеки ЕС–2013 використовує Рамкову програму Європейського Союзу з досліджень та інновацій «Горизонт 2020», як невід'ємну частину;

відведення достатньо пасивної ролі бізнесу та інститутам громадянського суспільства, механізмам державно-приватного партнерства;

зосередженість на «злу волю» – дію зовнішніх кіберзлочинців, зовнішні кібератаки, а не на комплексний захист національного кіберпростору від всіх негативних впливів (зовнішніх та внутрішніх) тощо.

Потрібно терміново переглянути державну політику законодавчо-організаційного забезпечення інформаційної і кібернетичної безпеки України, залучивши до цього провідних українських та іноземних фахівців, грунтуючись на наявних передових практиках та прогнозах кіберстійкості.

*УДК 004.03:658.15*

**Заєць П.М.**
старший викладач КТЗІ
ННІ ІБ ННІ ІБ НА СБ України
**Іванова О.С.**
старший викладач КТЗІ, к.ф.-м.н.
ННІ ІБ ННІ ІБ НА СБ України

## ВИЗНАЧЕННЯ ПІДХОДІВ ЩОДО ВПРОВАДЖЕННЯ ЗАСОБІВ І СИСТЕМ АВТОМАТИЗАЦІЇ ПРОЦЕСІВ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ОРГАНІЗАЦІЇ

Ще недавно ринок пропонував велику кількість програмних продуктів, що дозволяють автоматизувати етапи життєвого циклу системи

управління інформаційною безпекою (СУІБ), всі вони роз'єднані, мають різні формати представлення, використовують різні методології управління ризиками, оцінки захищеності інформаційної системи, ієрархії і класифікації ресурсів, ґрунтуються на різних джерелах баз даних загроз і вразливостей і т. ін. У даному контексті впровадження єдиного автоматизованого засобу представляється найбільш перспективним для реалізації дійсно системного підходу до управління інформаційною безпекою (ІБ).

Для створення єдиного автоматизованого засобу СУІБ у першу чергу слід визначаються основні напрями автоматизації процесів управління інформаційною безпекою на усіх етапах циклу управління: планування, впровадження, перевірка, удосконалення відповідно до вимог стандартів серії ДСТУ ISO/IEC 27000 [1].

**Процес планування** повинен включати наступні етапи:

1. Визначення переліку інформаційних ресурсів компанії. Для цього автоматизований засіб допомагає зберігати дані про інформаційні ресурси і всі їх зміни, крім цього, він може спростити процес збору даних.
2. Оцінка критичності видів інформації. Тут автоматизований засіб може тільки зберігати дані, відомості анкетування.
3. Оцінка захищеності, тобто виявлення загроз і уразливостей інформаційних ресурсів. Інтеграція з базами вразливостей і вбудовані бази загроз допомагають оптимізувати даний процес і забезпечити його повноту. Крім того, можлива інтеграція з різними сканерами вразливостей.
4. Визначення інформаційних ризиків. Вбудований алгоритм розраховує інформаційні ризики на основі внесених (або зібраних автоматично) даних. Результат оформляється у вигляді звіту.
5. Вибір стратегії обробки ризиків, визначення заходів щодо зниження ризиків.

Автоматизований засіб дозволяє максимально гнучко і зручно моделювати різні варіанти впровадження засобів захисту, оцінити ефективність планованих засобів, вибрати найкращу стратегію захисту.

**Впровадження процедур СУІБ** засобів підвищення захищеності передбачає їх реалізацію в процесах діяльності організації. У даному процесі автоматизований засіб може акумулювати інформацію, здійснювати спілкування між фахівцями з ІБ, виконувати роль планувальника завдань.

На даному етапі основна роль автоматизованого засобу – зберігати документи СУІБ:

- регламентуючі документи (політики, регламенти, інструкції);
- записи, що підтверджують виконання існуючих процедур в організації.

Це дозволяє зберігати всю документацію СУІБ в одному централізованому місці і в разі необхідності без зволікання надавати її зацікавленим особам (наприклад, внутрішнім або зовнішнім аудиторам).

**Перевірка функціонування процедур** СУІБ необхідна для того, щоб гарантувати їх правильну і ефективну роботу або в разі виявлення будь-яких порушень визначити, які потрібні вдосконалення. На даному етапі автоматизований засіб може виконувати, наприклад, такі ролі:

**Ведення статистики та аналіз інцидентів**. Аналіз інцидентів є основним критерієм ефективності та достатності забезпечення інформаційної безпеки організації, а також ефективності всієї СУІБ в цілому. На основі інформації про інциденти визначаються заходи щодо вдосконалення засобів захисту.

Автоматизований засіб може надавати можливість структурованого зберігання даних про всі інциденти ІБ, збирати їх статистику за різними параметрами, позначати об'єкти, часто фіксуються в якості об'єктів інцидентів.

**Збір метрик оцінки ефективності ІБ**. Результати та частота інцидентів інформаційної безпеки – найбільш очевидна метрика оцінки її ефективності.

Крім того, автоматизований засіб може аналізувати, наприклад, такі дані: уразливості(знайдені, закриті), ефективність впроваджуваних контрзаходів, кількість проведених курсів по ІБ і т. ін.

На основі зібраних і проаналізованих метрик оцінки ефективності визначаються коригувальні дії та план їх впровадження. Як правило, коригувальні дії є або змінами в процедурах, документах, якими новими засобами захисту, тобто змінами в самій організації. Автоматизований засіб допомагає відображати результати, зберігати дані і вести контроль змін захищеності інформаційних ресурсів.

По завершенні останнього етапу весь процес заново переходить на етап планування і циклічно повторюється протягом всього життєвого циклу системи управління ІБ.

Підсистеми системи автоматизації процесів управління інформаційною безпекою можна класифікувати відповідно до вимог стандарту ДСТУ ISO/IEC 27001:2015 [2,3].

**Підсистема управління документами** ІБ автоматизує зберігання, узгодження, визначення актуальності документів щодо процесів управління ІБ.

**Підсистема управління класифікацією об'єктів** захисту автоматизує облік, класифікацію і визначення рівня критичності інформаційних активів організації.

**Підсистема управління ІБ при роботі з персона**лом автоматизує процедури доведення організаційно-розпорядчої документації щодо забезпечення ІБ для працівників організації, контроль знань працівників організації вимог щодо ІБ.

**Підсистема управління ризиками ІБ** автоматизує процедури ідентифікації, аналізу, оцінки і обробки ризиків.

**Підсистема управління інцидентами ІБ** автоматизує процедури реєстрації, оброблення інцидентів ІБ, оповіщення про них, зберігання статистики і результатів розслідування інцидентів ІБ.

**Підсистема управління відповідністю до вимог ІБ** автоматизує процедури самооцінки відповідності системи забезпечення інформаційної безпеки організації вимогам ІБ, визначених нормативно-правовими документами.

Система автоматизації процесів управління інформаційною безпекою інтегрується з комплексною СІБ та іншими системами такими, як:

- системи інвентаризації ІТ-активів;
- системи контролю використання інформаційних ресурсів;
- системи управління обліковими записами і ролями користувачів;
- системи контролю і аналізу захищеності;
- системи аналізу і кореляції подій ІБ.

Запропонована структура системи автоматизації процесів управління інформаційною безпекою може бути реалізована на довільній програмно-апаратній платформі.

**Література**

1. ДСТУ ISO/IEC 27000:2015 Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник (ISO/IEC 27000:2014, IDT).

2. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT).

3. Автоматизация процессов управления информационной безопасностью. Режим доступу: http://www.gaz-is.ru/reshenija/resheniya/avtomatizacija.html.

*УДК 004.621.3:519.816*

**Зибін С.В.**
кандидат технічних наук, доцент
Державний університет телекомунікацій

## ПІДТРИМКА ПРИЙНЯТТЯ РІШЕНЬ ПРИ ФОРМУВАННІ ПРОГРАМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ: РОЗПОДІЛЕННЯ РЕСУРСІВ

Підвищення якості і скорочення часу прийняття рішень при керуванні складними технічними та інформаційними системами різного призначення в теперішній час неможливо без інформаційно-аналітичної підтримки. Засоби інтелектуалізації процесів прийняття рішень являються найбільш важливими і практично необхідними в сфері інформаційної безпеки держави та інформаційних технологій.

Розробка і експлуатація складних систем виявили проблеми, які можна вирішити лише на підставі комплексної оцінки і обліку різних за своєю природою факторів, різнорідних зв'язків, зовнішніх умов та інших показників. Тому все більш важливим в сучасних умовах стає питання якісного та ефективного прийняття рішень [1, 2].

Комплексна програма забезпечення інформаційної безпеки держави (ПІБД) являє собою сукупність заходів, які об'єднані єдністю глобальної мети й загальними ресурсами. Основні задачі розробки складних ПІБД – це відбір програм, які являються частиною комплексної програми й розподіл між ними ресурсів. При цьому ПІБД, як правило, може плануватися на великі проміжки часу, тому необхідно оцінювати ефективність програм на заданому інтервалі часу.

При розробці ПІБД слід враховувати можливість виникнення загроз і ризиків, аналізувати їхній вплив і на цій основі передбачати заходи щодо протидії їм або усунення їх.

При формуванні ПІБД із урахуванням загроз і ризиків необхідно вирішувати наступні задачі:

- визначення кількісних характеристик впливу загроз і ризиків на ефективність ПІБД;
- визначення кількісних показників ефективності програм при наявності загроз і ризиків;
- розподіл ресурсів між засобами протидії загрозам і ризикам та програмами, що мають спрямованість на підвищення інформаційної безпеки держави.

Відомі методи рішення першої задачі передбачають ідентифікацію ризиків (якісний аналіз), а також оцінювання ймовірностей і розмірів можливого збитку (кількісний аналіз). Однак при цьому задача оцінки ефективності програм з урахуванням ризиків не вирішується й залишається на розсуд експерта – особи, що приймає рішення (ОПР). Більше того, визначення збитку в абсолютному вимірі часто неможливо для складних ПІБД.

Дана стаття являється продовженням робіт [1, 3] і присвячена викладанню запропонованого алгоритму розподілу ресурсів між засобами протидії загрозам і ризикам та програмами, що мають спрямованість на підвищення інформаційної безпеки [4]. Задача полягає у визначенні множини оптимальних ресурсів, таких, що максимізують ступінь досягнення мети. Задачу розподілу ресурсів можна сформулювати наступним чином.

Існує множина завдань забезпечення інформаційної безпеки $T = \{T_i\}, i = (\overline{1,m})$.

Для кожного завдання існує функція ступеню виконання в залежності від величини ресурсу $f(R_i / R_i^*), i = (1,m)$, де $R_i^*$ – необхідна кількість ресурсів, $\overline{R} = \{R_i\}$ – множина доступних ресурсів.

Обчислення ефективності відповідає вектору $\overline{R}$. $E(\overline{R}) = E(\overline{F})$, де $\overline{F}$ – ступінь досягнення поставленої мети.

Необхідно знайти вектор $R_x$, при якому $E(R_x) \to \max$, при обмеженні $\sum_{i=1}^{m} R_i \le R_{\max}$, де $R_{\max}$ – кількість ресурсів завдання.

Скористаємося методами оптимізації для вирішення задачі розподілу ресурсів при аналітичному завданні функції $E(\overline{R})$. В цьому випадку ефективність використання ресурсів: $E(\overline{R}) = \sum_{i=1}^{m} E(R_i)$. Необхідно знайти такий вектор $R_x$, при якому $E(R_x) \to \max$, при обмеженні $\sum_{i=1}^{m} S_i \le R_{\max}$.

При алгоритмічному завданні функції $E(\overline{R})$ розв'язок задачі невідомий, але для вирішення задачі можна скористатись генетичними алгоритмами. З цією метою необхідно обрахувати ефективність в кожній точці функції.

При оцінці ефективності можна використовувати критерій ризику інформаційної безпеки.

Найбільш поширена оцінка інформаційних ризиків має вигляд:

$R = pC$

де $R$ – інформаційний ризик;

$p$ – ймовірність порушення інформаційної безпеки;

$C$ – вартість інформаційних ресурсів.

При побудові системи захисту досить складно розрахувати загальне значення ймовірності порушення безпеки, але можливо знайти значення ймовірності реалізації окремих загроз.

**Література**

1. Зибін С.В. Підтримка прийняття рішень при формуванні програм інформаційної безпеки держави: моделі загроз і ризиків / С.В. Зибін, В. О. Хорошко // Інформатика та математичні методи в моделюванні. – Одеса. – ОНПУ, 2015. – Т. 5. – № 1. – С. 77-84.

2. Бідюк О. П. Комп'ютерні системи підтримки прийняття рішень : навч. посіб. / О. П. Бідюк, О. П. Гожий, Л. О. Коршевнюк. – Миколаїв : Вид-во ЧДУ ім. Петра Могили, 2012. – 380 с.

3. Зибін С.В. Підтримка прийняття рішень при формуванні програм інформаційної безпеки держави: оцінка ефективності програм / С.В. Зибін, В.О. Хорошко // Інформатика та математичні методи в моделюванні. – Одеса. – ОНПУ, 2015. – Т. 5. – № 2. – С. 122-129.

4. НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу".

*УДК 35:001.8:303.833*
**Золотухін Д.Ю.**
Міністерство інформаційної політики України

# БОРОТЬБА ІЗ «ФЕЙКОВИМИ НОВИНАМИ»: ДОСВІД УКРАЇНИ ТА РЕКОМЕНДАЦІЇ

“Фейкові новини” (“фейки”) є узагальненим терміном, який є продуктом медіапростору та ЗМІ, де існує необхідність надати певному явищу або феномену коротку назву для зручності у використанні. Використання цього словосполучення значно ускладнює роботу над науково-практичним та юридичним формулюванням конкретного визначення для цього феномену.

В широкому сенсі це словосполучення визначається як сукупність інструментів, що застосовується з метою маніпулювання суспільною свідомістю, і, частіше всього, виражається у інформаційному повідомленні (текст/фото/відео, чи їх комбінація), що містить неправдиву чи частково правдиву інформацію та поширюється традиційними засобами масової інформації, соціальними мережами чи іншими доступними шляхами розповсюдження інформації, і має на меті сформувати у свідомості споживачів (реципієнтів) певне відношення до явища чи об’єкту реального світу. Наприклад, сформувати ксенофобські настрої щодо якоїсь конкретної соціальної групи, через поширення негативної та емоційно зарядженої інформації про цю соціальну групу.

Через невизначеність підходів до розуміння цього явища, під категорію “фейкових новин” зазвичай потрапляють:

- навмисно створені інформаційні повідомлення, які мають на меті здійснення маніпулювання,
- інформаційні повідомлення, що є результатом непрофесійного та неетичного виконання своїх обов’язків співробітниками медіа.

Однак, в обох випадках на аудиторію здійснюється шкідливий вплив, що обумовлює важливість протидії обом типам “фейкових новин”.

Особливої уваги заслуговує той факт, що навмисно створені для маніпулювання аудиторією інформаційні повідомлення є різновидом т.зв. “активних заходів”, які є однією з форм роботи спецслужб та розвідувальних органів. Активні заходи (спеціальні заходи впливу, спеціальні інформаційні операції, інформаційно-психологічні спеціальні операції) використовуються спецслужбами з метою цілеспрямованої та спланованої зміни політичного дискурсу певної спільноти або суспільної думки.

Так, наприклад, “фейковою новиною” є інформація про, нібито, заклик Дмитра Яроша до лідера чеченських бойовиків Доку Умарова, яку 1-2 березня 2014 року розповсюдили провідні російські ЗМІ. В подальшо-

му ця новина була використана для легітимізації застосування Російською Федерацією своєї армії на території України. Це свідчитьпро спланований та підготовлений завчасно характер цієї інформаційної операції.

Практика планування та здійснення “активних заходів” з розповсюдження дезінформації включає в себе використання подій чи фактів, що дійсно відбулися в реальності, однак в інформаційному повідомленні їх подають в неповному або спотвореному вигляді, чи в контексті емоційного забарвлення.

Нерідко поширення фейкових новин пришвидшується завдяки реп лікуванню журналістами та редакторами онлайн-платформ гучних та скандальних новинних матеріалів (що є типовим для фейків). Тобто, фейк поширюється без належної перевірки фактів, з метою підвищення рейтингів чи відвідуваності інформаційних ресурсів. В цілому, гонитва окремих ЗМІ за увагою споживачів інформації істотно сприяє успішній реалізації “активних заходів” та здійсненню впливу на широку аудиторію.

Таким чином, ідентифікація та детекція “фейкової новини” за формальними ознаками є дуже ускладненою. Будь-які дії законодавчого, адміністративного чи експертного характеру щодо визначення, атрибуції та описання інформаційного повідомлення в якості “фейкової новини” неминуче призведуть до необхідності чітко регламентувати межі повноважень та компетенції суб’єкта, який здійснює таку діяльність.

Наприклад, чіткий та сталий перелік ознак “фейку” і жорстко регламентований підхід до визначення “фейкових новин” не дасть змогу ефективно протидіяти гнучким та поліморфним гібридним загрозам інформаційного простору, що будуть підлаштовуватися спецслужбами для обходу встановлених процедур. Характерною ознакою “фейкових новин” є постійне вдосконалення механізмів маніпуляції та її поширення, що нівелює спроби уніфікації їх визначення в рамках формальних ознак.

І навпаки, надто широке коло повноважень інституції, яка буде визначати “фейкові новини” на підставі суб’єктивних суджень (без жорсткої регламентації меж та чітких критеріїв і ознак) може призвести до виникнення ризиків для свободи слова.

Таким чином, реагування на “фейкові новини” шляхом їх ідентифікації і описання розцінюється як малоефективна з точки зору розвитку стратегічних комунікацій.

Крім вищеописаних труднощів адміністративно-правового підходу до протидії “фейковим новинам”, питання щодо ефективності викликає практика “розвінчування фейків”. З точки зору практики комунікації, цей процес є досить складним для сприйняття широкими аудиторіями і позитивно оцінюється тільки експертами або зацікавленими саме в такому контенті споживачами.

Враховуючи це, а також очевидний факт невідповідності ресурсів, які витрачаються Російською Федерацією на створення та поширення "фейкових новин" та ресурсів компетентних державних інституцій і недержавних організацій, що покликані протидіяти "фейковим новинам", реактивна протидія розповсюдженню "фейків" розцінюється багатьма експертами галузі як неефективна.

В той же час, представники державних інституцій різних країн Європейського Союзу (наприклад, країн Балтії) наголошують на тому, що вони "не протидіють фейкам, а просувають свій наратив". Тобто провідні державні і недержавні експерти відмовляються від реактивної протидії розповсюдженню "фейкових новин" на користь формуванню свого порядку денного в конкурентному інформаційному середовищі.

Одним з перших вітчизняних суб'єктів, хто почав просувати таку методику боротьби з "фейковими новинами", є Міністерство інформаційної політики України. Цей підхід не виключає необхідності реагування на "фейкові новини" шляхом перевірки, спростування брехливої інформації і надання об'єктивної інформації щодо конкретних питань. Однак проактивна діяльність державних інституцій стосовно конкурентного представлення своєї комунікаційної позиції в інформаційному середовищі була визначена пріоритетною.

Визнання проблематики "фейкових новин" та дезінформації на законодавчому рівні є необхідним кроком для організації подальшої системної протидії інформаційному впливу на суспільство. За відсутності законодавчого визнання проблеми інформаційної агресії, боротьба з дезінформацією залишатиметься неузгодженою системою локальних ініціатив неурядових інституцій та окремих дій органів державної влади, без створення системи превентивної протидії.

Україна, опинившись з 2014 року в умовах широкомасштабної дезінформаційної кампанії з боку РФ, більш двох років вибудовувала власне нормативно-правове забезпечення протидії фейкам. При цьому, в контексті європейської та євроатлантичної інтеграції України, така діяльність ретельно узгоджувалась з точкою зору закордонних партнерів, які постійно наголошували на необхідності пріоритету питань свободи слова над питаннями національної безпеки.

Водночас, саме завдяки ухваленню на початку 2017 року Доктрини інформаційної безпеки в Україні був чітко визначений механізм протидії інформаційній агресії, передбачено компетенції відповідальних органів влади у цій сфері та запроваджено підхід, який враховував пріоритети громадського суспільства та закордонних партнерів України.

Окрім вище зазначених нормативно-правових та адміністративних аспектів протидії "фейковим новинам", потребує визначення механізм притягнення до відповідальності суб'єктів поширення дезінформації.

Держава в особі органів державної влади є монополістом на застосування механізмів відповідальності та санкцій за невиконання обов'язків. Ці механізми реалізуються через уповноважені державні органи (суд, органи сектору безпеки та оборони, регуляторні органи тощо). Водночас, наділення органів державної влади повноваженнями щодо притягнення до відповідальності за поширення "фейкових новин" несе в собі ризик зловживання таким правом та навіть цензурування ЗМІ, що не відповідає принципам демократичного суспільства.

Крім того, суб'єктивний характер оцінювання "фейкових новин" обумовлює необхідність проведення експертиз (в т.ч. і неурядовими структурами) з метою уникнення безпідставного притягнення до відповідальності.

З огляду на вищезазначене, пріоритетна роль в системі притягнення до відповідальності за поширення "фейкових новин" має належати не державі, а профільним інституціям громадянського суспільства (ІГС).

Зважаючи на монополію держави на застосування примусу та необхідність дотримання принципів невтручання в діяльність ЗМІ, оптимальними видаються два механізми притягнення до відповідальності за поширення фейкових новин:

– змішаний, коли притягнення до відповідальності здійснюється уповноваженим Законом органом влади за висновком ІГС. При цьому, санкції матимуть адміністративний характер (попередження, позбавлення ліцензій, відкриття кримінального провадження тощо);

– недержавний, коли висновок ІГС є достатнім для відповідної реакції суспільства, публічного осуду, що тягне за собою публічну недовіру суб'єкту поширення дезінформації та нівелює його значущість у соціумі (відмова від акредитації на заходах, втрата аудиторії тощо).

Найбільш ефективним є недержавний механізм з наступних підстав. По-перше, втрата довіри до ЗМІ та його фактичне "забуття" має довготривалий ефект. По-друге, публічний осуд не може бути уникнено за допомогою адміністративних механізмів (наприклад, шляхом оскарження застосування санкції). По-третє, таке рішення засноване на колегіальній узгодженій позиції експертів, що виключає можливість впливу зацікавленої сторони на кінцеве рішення.

Втім, що найважливіше, такий спосіб заснований на принципах саморегуляції та невтручання держави в діяльність ЗМІ. А отже, виключається можливість владного впливу на сферу масової інформації.

Водночас, недержавний спосіб потребує існування ефективного та загальновизнаного в суспільстві органу саморегуляції ЗМІ, механізму прийняття рішення таким органом та застосування відповідного рішення.

Адже без належної підтримки суспільством такого рішення, його ефективність буде мінімальною та матиме скоріш декларативний ефект.

Саме тому, на період становлення відповідних громадянських інституцій, можливо тимчасове застосування змішаного механізму, який передбачатиме, по перше, систему стримувань і противаг (держава не може застосувати санкцію без рішення ІГС), а, по-друге, чітко передбачений Законом суб'єкт застосування санкції, механізм прийняття рішення, види санкцій тощо.

Основною проблемою застосування такого механізму є необхідність існування ініціативи від суб'єктів ІГС та підтримки такої ініціативи журналістською спільнотою.

Притягнення до відповідальності як спосіб реагування на дезінформацію є найбільш очевидним, втім не найефективнішим способом. Недоліком такого підходу є те, що притягнення до відповідальності – це реагування на вже здійснений факт. А фейки та інші т.зв. "активні заходи" зазвичай створюються так, щоб швидко поширюватись, фіксуватись у свідомості споживачів та гнучко підлаштовуватись під будь-які зміни, в тому числі нормативно-правового характеру. Будь-яке спростування, в тому числі публічне визнання компетентним органом фейкового характеру новини не зможе повністю нівелювати ефект від поширеної інформації.

Тому важливо враховувати інші способи протидії фейковим новинам, окрім тих, на яких було наголошено вище:

1. поширення власного наративу;
2. спростування і розвінчування фейків;
3. застосування механізмів суспільної відповідальності за поширення "фейкових новин" і розбудову саморегуляції та співрегуляції медіасередовища;

Одним із таких способів є підвищення медіаграмотності суспільства - комплекс превентивних заходів із вдосконалення здатності громадян самостійно виявляти фейки, опиратися маніпулятивному впливу, підлаштовуватися під зміни інформаційного середовища, розвивати власне критичне сприйняття інформації.

Таким чином, діяльність МІП в сфері протидії "фейковим новинам" сконцентрована на вищевикладених напрямках роботи та реалізовується в рамках проектних і програмних ініціатив по створенню системних спроможностей українського уряду і громадського суспільства нівелювати шкідливий маніпулятивний вплив, що створює загрози поступальному демократичному розвитку України на шляху інтеграції до Європейського Союзу та Північно-Атлантичного Альянсу.

*УДК 351:004.8*
**Карпенко О.В.**
доктор наук з державного управління,
завідувач кафедри інформаційної політики
та цифрових технологій Національної академії
державного управління при Президентові України
**Савченко Н.В.**
кандидат наук з державного управління,
старший науковий співробітник,
докторант кафедри інформаційної політики
та цифрових технологій Національної академії
державного управління при Президентові України

# ЦИФРОВІ ТЕХНОЛОГІЧНІ ТРЕНДИ СФЕРИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Цифрові технології повсякчас посилюють свій вплив на життєдіяльність суспільства. Зростає їх роль і в публічному врядуванні, зокрема особливої актуальності набувають цифрові трансформації у сфері вироблення державної політики щодо кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів, захисту інформації, телекомунікацій тощо. Одним зі значущих викликів сьогодення є створення належних умов та забезпечення побудови ефективних цифрових систем, платформ та інфраструктур із застосуванням вітчизняних стандартів та технологій, які мають бути використані у сфері інформаційної та кібербезпеки країни.

Цифровізація публічного врядування України повинна сприяти підвищенню рівня інформаційної безпеки органів публічної влади, кібербезпеки (як держави в цілому, так і кожного її громадянина), гарантування захисту персональних даних, забезпечення недоторканності особистого життя й прав користувачів цифрових технологій. Належний захист функціонування у кіберпросторі всіх суб'єктів інформаційних відносин є базовою умовою як цифрового розвитку, так і попередження, усунення та управління ризиками в процесі впровадження цифрових трансформацій.

Цифровізація публічного врядування є процесом реалізації цифрових трансформацій у публічній сфері (в контексті докорінного перетворення діяльності органів публічної влади), що призведе до стрибкоподібного переходу до цифрового врядування (цифрового управління) шляхом застосування цифрових технологій (інструментів цифрового робочого місця, штучного цифрового інтелекту прийняття типових управлінських

рішень, blockchain-, smart- (IoT), portal-, cloud-, network-сервісів тощо) [3, с. 8].

Блокчейн є сучасною технологією обліку та обміну правами власності на цифрові активи в одноранговій мережі, яка містить структуровані дані у вигляді розподіленого реєстру. Головною відмінністю блокчейну від класичних реєстрів є одночасне збереження даних, які розподілені серед певної кількості вузлів мережі без прив'язки до конкретної локації. Блокчейн-система є розподіленою базою здійснених транзакцій, у якій дані зберігаються у вигляді ланцюга блоків із відповідними записами. Зазначимо, що під час економічного форуму у Давосі (Швейцарія) було презентовано світову карту з чотирнадцятьма країнами-лідерами (США, Канада, Австралія, Ізраїль, Естонія, Велика Британія та ін.) у впровадженні блокчейн-технології, до яких увійшла й Україна [7]. Наприклад, в Україні цю технологію успішно впроваджено при створені Державного земельного кадастру [1] та Системи електронних торгів арештованим майном [6].

Однак, головною темою технологічних дискусій 2018 року продовжить залишатися штучний інтелект, а в його розробку будуть інвестувати значні кошти (в світовому вимірі). Вітчизняні науковці теж мають вагомі здобутки в галузі розробки та впровадження штучного інтелекту, зокрема у вивченні головного мозку. Про це свідчать результати фундаментальних досліджень, здійснених фахівцями Інститут проблем штучного інтелекту МОН України та НАН України, які вже застосовуються у медичній практиці [2].

Окремої уваги потребують смарт-технології та "Інтернет речей" (англ. Internet of Things, IoT). Технологічні здобутки 2017 року засвідчили про зростаючий потенціал розумних пристроїв "розумного міста", "розумного будинку", у тому числі за рахунок використання різноманітних мобільних гаджетів. Важливим аспектом сучасних гібридних воєн є технологія "Військовий інтернет речей" (Internet of Batlle Things, IoBT), яка набуває особливого значення в процесі здійснення як мережевих, так і військових операцій [4].

Серед інших, не менш популярних, технологій 2018 року відзначають "*доповнену реальність*", "*голосових асистентів"* (комплексні технологічні рішення Amazon, Google та ін.), поступовий перехід від хмарних (cloud computing) до *граничних обчислень* (edge computing) тощо.

Перераховані тренди не вичерпують переліку інновацій, які набуватимуть поширення у 2018 році. Однак, змушують замислитись над потребою реалізації на практиці механізмів цифрового розвитку та пошуку шляхів безпечного їх упровадження. Реалізація схваленої урядом Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки [5] потребує вибору оптимального інструментарію реалізації

державної політики «цифрового прориву», здатної забезпечити розвиток України у глобалізованому цифровому світі та гарантувати безпеку її громадян.

**Література**

1. Державний земельний кадастр відтепер використовує технологію Blockchain [Електронний ресурс]. – Режим доступу: http://dknii.gov.ua/content/derzhavnyy-zemelnyy-kadastr-vidteper-vykorystovuye-tehnologiyu-blockchain. – Назва з екрану.

2. Дослідження штучного інтелекту в Україні: здобутки та перспективи [Електронний ресурс]. – Режим доступу: http://www.nas.gov.ua/text/pdfNews/artificial_intelligence_Shevchenko_TV_interview.pdf. – Назва з екрану.

3. Куйбіда В.С. Цифрове врядування в Україні: базові дефініції понятійно-категоріального апарату / Куйбіда В.С., Карпенко О.В., Наместнік В.В. // Вісник Національної академії державного управління при президентові України. Серія "Державне управління". – К. : НАДУ, 2018. – № 1. – С. 5-11.

4. Левков О. Військовій інтернет речей та українські реалії [Електронний ресурс]. – Режим доступу: https://defence-ua.com/index.php/statti/4224-viyskoviy-internet-rechey-ta-ukrayinski-realiyi. – Назва з екрану.

5. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації: розпорядження Кабінету Міністрів України від 17 січ. 2018 р. № 67-р // Офіц. вісн. України. – 2018. – № 16.

6. СЕТАМ став першим у світі аукціоном на Blockchain та змінив назву на OPENMARKET [Електронний ресурс]. – Режим доступу: http://setam.gov.ua/article/setam-stav-pershim-u-sviti-auktsionom-na-blockchain-ta-zminiv-nazvu-na-openmarket. – Назва з екрану.

7. Україна ввійшла до рейтингу світових блокчейн-лідерів [Електронний ресурс]. – Режим доступу: https://www.ukrinform.ua/rubric-technology/2390185-ukraina-vvijsla-do-rejtingu-svitovih-blokcejnlideriv.html. – Назва з екрану.

*УДК 341.824:338.46*

**Касперський І.П.**
кандидат юридичних наук, доцент
Національна академія СБ України

## РОЗВИТОК МОЖЛИВОСТЕЙ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ СЕРВІСІВ ЕЛЕКТРОННОГО УРЯДУВАННЯ

Розвиток запроваджуваних в Україні систем електронного урядування потребує наявності у користувачів надійних засобів ідентифікації та автентифікації. Це дозволить забезпечити не тільки належне підтвердження

статусу користувача, а і підтримувати цілісність та достовірність вагомих масивів даних численних державних ресурсів.

З самого початку доступ громадян до електронних державних сервісів було організовано із використанням двох способів: дійсного електронного цифрового підпису та міжнародної системи ідентифікації клієнтів банків Bank ID.

Як бачимо, одразу до забезпечення можливостей користування громадянами адміністративними послугами в електронному вигляді було залучено суб'єкти приватного права – банки. Згодом до цього процесу підключили і операторів мобільного зв'язку, запроваджуючи реєстрацію користувачів у системі «Поліклініка без черг» за допомогою мобільних телефонів [1] та впровадженням системи Mobile ID [2]. За словами голови Держагентства електронного урядування Олександра Риженка впровадження мобільної ідентифікації громадян з використанням Mobile ID є одним із перших пунктів реалізації Концепції розвитку цифрової економіки та суспільства до 2020 року [3, 4]. По суті це та ж концепція електронного цифрового підпису, носієм ключів якого є модернізована SIM-карта, та яку заплановано спершу використовувати для отримання послуг двох державних ресурсів: Держгеокадастру та Онлайн будинку юстиції [2]. Основною перевагою такої системи ідентифікації менеджмент оператора зв'язку назвав низьку вартість SIM-карт як носіїв ключів [3].

З одного боку таке державно-приватне партнерство при наданні адміністративних послуг відповідає загальноприйнятій світовій практиці, так у Сенегалі та Уганді запроваджено проекти реєстрації новонароджених за допомогою мобільного телефону [5]. З іншого боку надмірна довіра громадян до приватних структур не завжди є виправданою, з огляду на постійні витоки персональних даних клієнтів, які допускають у тому числі і солідні компанії, такі як «Нова пошта» [6] чи «Міжнародні авіалінії України» [7]. Крім того, надійність використання терміналів мобільного зв'язку при ідентифікації користувачів навіть банківських послуг є сумнівною у зв'язку із поширенням шахрайських схем, що включають неконтрольований реальним власником перевипуск SIM-карти оператором, що дає зловмисникам несанкціонований доступ до рахунку. Подолання цієї вади шляхом запровадження обов'язкової реєстрації користувачів послугів мобільного зв'язку [8] викликає природній спротив громадянського суспільства [9].

Виходячи із викладеного, варто зауважити, що розвиток державою систем електронного урядування повинен відбуватися на принципах відповідального ставлення нею до власних обов'язків та прав громадян. У зв'язку із цим варто сформувати альтернативу можливість громадянам ідентифікувати себе як користувачів систем електронного урядування тими засобами, які б максимально не були б пов'язані із недержавними

структурами і надійність функціонування яких була б гарантована державою. Прикладом реалізації такої альтернативи є Естонія, яка попри традиційні способи ідентифікації користувачів адміністративних послуг ключами електронних цифрових підписів, що містяться на SIM-картках, спершу запровадила нанесення засобів електронного цифрового підпису на ID-карту громадянина, що випускається та обслуговується державою [10]. Поширення практики «державного носія ключів» в Україні підвищить надійність такого засобу ідентифікації і довіру громадян до систем електронного урядування.

**Література**


1. Інструкція користування системою «Поліклініка без черг» // [Електронний ресурс]. – Режим доступу: https://global.newmedicine.com.ua/assets/Інструкція%20для%20пацієнта.pdf.
2. Київстар запустив Mobile ID у дослідну експлуатацію // [Електронний ресурс]. – Режим доступу: https://kyivstar.ua/ru/mm/news-and-promotions/kievstar-zapustil-mobile-id-v-opytnuyu-ekspluataciyu.
3. За півроку Київстар планує підключити до Mobile ID близько 10 сервіс-провайдерів // [Електронний ресурс]. – Режим доступу: https://kyivstar.ua/uk/mm/news-and-promotions/za-pivroku-kyyivstar-planuye-pidklyuchyty-do-mobile-id-blyzko-10-servis.
4. Концепція розвитку цифрової економіки та суспільства України на 2018–2020 роки: затв. Розпорядженням Кабінету Міністрів України від 17.01.18 р. №67р // Офіційний вісник України від 23.02.2018. – 2018 р. – № 16.
5. Mobile Birth Registration in Sub-Saharan Africa. A case study of Orange Senegal and Uganda Telecom solutions // // [Електронний ресурс]. – Режим доступу: https://www.gsma.com/identity/wp-content/uploads/2013/05/Mobile-Birth-Registration-in-Sub-Saharan-Africa.pdf.
6. Карпусь В. Бывший сотрудник «Новой почты» осужден за продажу данных клиентов компании // [Електронний ресурс]. – Режим доступу: https://itc.ua/news/byivshiy-sotrudnik-novoy-pochtyi-osuzhden-za-prodazhu-dannyih-klientov-kompanii/.
7. Скрипин В. Уязвимости на сайте крупнейшего украинского авиаперевозчика МАУ позволяли без труда узнавать данные о его пассажирах // [Електронний ресурс]. – Режим доступу: https://itc.ua/news/uyazvimosti-na-sayte-krupneyshego-ukrainskogo-aviaperevozchika-mau-pozvolyali-bez-truda-uznavat-dannyie-o-ego-passazhirah-v-kompanii-ne-schitayut-poluchaemyie-dannyie-konfidentsialnyimi/.
8. Аналіз регуляторного впливу до проекту Закону України «Про внесення змін до Законів України «Про телекомунікації» і «Про радіочастотний ресурс України» щодо ідентифікації абонентів рухомого (мобільного) зв'язку та запровадження реєстрації кінцевого обладнання за міжнародним ідентифікатором» // [Електронний ресурс]. – Режим доступу: http://195.78.68.84/dsszzi/control/uk/publish/article?showHidden=1&art_id=278747&cat_id=38837&ctime=1500541975594.

9. Букатюк У. В Україні хочуть продавати SIM-карти за паспортом. Це тоталітаризм чи боротьба з шахраями?// [Електронний ресурс]. – Режим доступу: https://espreso.tv/article/2017/08/09/mobilnyy_zvyazok_za_pasportom_totalitaryzm_chy_cyvilizaciynyy_postup.
10. ID-card and Digi-ID // [Електронний ресурс]. – Режим доступу: https://www.id.ee/?lang=en&id=30500.

*УДК 006.034:658.562.4*

**Кожедуб Ю.В.**
кандидат технічних наук, доцент СК № 2
ІССЗЗІ НТУУ «КПІ ім. Ігоря Сікорського»
**Прокудо Р.М.**
ІССЗЗІ НТУУ «КПІ ім. Ігоря Сікорського»

# ДО ПИТАННЯ СТВОРЕННЯ КОМПЛЕКСУ ЗАХОДІВ ІЗ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ НА ОРГАНІЗАЦІЙНОМУ РІВНІ

Потреба захисту інформації є невіддільною від практичного застосування інформаційних технологій у повсякденному житті, з якими стикається кожна людина. Тому наявність систем захисту інформації для державних організацій та приватних підприємств є обов'язковою умовою успішного функціонування таких підприємств і організацій сучасного ринку. Зростає кількість спеціалізованих організацій чи підприємств, які пропонують послуги щодо захисту інформаційних ресурсів, інформаційних систем, загалом, інформації, зважаючи на зрослі темпи розвитку новітніх технологій та технічних застосунків, і відповідних рішень для забезпечення інформаційної безпеки. В Україні наразі є дві системи, що мають на меті зреалізувати прийнятні заходи для забезпечення інформаційної безпеки підприємств чи організацій насамперед сфери захисту інформації. Наголошуємо, що зазначені системи можуть бути упроваджені і для будь-яких інших підприємств чи організацій, щоб показати споживачам чи користувачам послуг, товарів, продукції зі світу інформаційних технологій, що вжито усіх необхідних й достатніх заходів задля убезпечення інформації.

Сучасні підприємства чи організації сфери захисту інформації пропонують створення систем, щоб поліпшити діяльність організації, зосередивши увагу на упровадженні різноманітних заходів і засобів із застосуванням сучасних технологічних рішень, технічних чи організаційних заходів з управління й контролю роботи персоналу, який має стосунок до інформаційних ресурсів. Функціонування зазначених систем не може повністю убезпечити організації і підприємства від загроз сучасних порушників інформаційної безпеки, проте створить відповідну основу для зниження ризиків інформаційної безпеки, спричинених людським фактором.

Застосування наукових принципів для практичного застосування змушує фахівців, теоретиків і практиків, більш ретельно зосередити увагу на практичних аспектах поставленої наукової проблеми. Проблема захисту інформації набуває нового значення після вдалих спроб порушників інформаційної безпеки, які зруйнували нібито «залізний» захист інформаційних систем державних установ і організацій. Постає питання використання новітніх інструментів технічного захисту інформації. Проте це є вартісним рішенням наболілого питання убезпечення інформації. Організаційні заходи є простим і дієвим бар'єром на шляху зловмисників. На сьогодні кожна організація, що має власні інформаційні бази даних, бази знань, потужні портали, успішні фірми декларують правила поводження з інформацією, називані Політикою інформаційної безпеки. Зазвичай декларативне означення правил поводження з інформацією, що циркулює в організації чи на підприємстві не є вирішальним чинником для забезпечення інформаційної безпеки, проте вона сприяє дисциплінованості й організованості персоналу і працівників зазначених організацій і підприємств. За точного виконання зазначених правил, за ретельного планування, постійного контролю, планового аудиту таких організацій і підприємств можна попередити виникнення подій інформаційної безпеки і попередити трапляння інцидентів інформаційної безпеки. Правильний менеджмент інформаційної безпеки, прогнозування подій і контролювання розвитку наслідків інцидентів інформаційної безпеки – є предметом роботи офіцерів з безпеки інформації. Сучасні підприємства сфери інформаційних технологій мають у своєму штатів подібний персонал, що його навчено зреагувати на такі ситуацій в світі інформації.

*УДК [001.8/.816/.817] + 001.92 + [371.315.5/.315.6/.335] +655.52*

**Козубцов І.М.**
кандидат технічних наук,
професор РАЕ, НЦЗІ ВІТІ
**Козубцова Л.М.**
кафедра №4 ВІТІ
**Куцаєв В.В.**
НЦЗІ ВІТІ
**Терещенко Т.П.**
НЦЗІ ВІТІ

## СТРАТЕГІЧНІ НАПРЯМКИ АНКЕТУВАННЯ СПЕЦІАЛІСТІВ ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ДЛЯ З'ЯСУВАННЯ РІВНЯ КІБЕРНЕТИЧНОЇ ЗАХИЩЕНОСТІ ОРГАНІЗАЦІЇ

Питання оцінки кібернетичної захищеності будь-якої організації є актуальним, проте і досі воно не вирішене. Наявні методики оцінки кіберне-

тичної захищеності побудовані на якісних показниках на разі не відповідають вимогам сучасності. Враховуючи вище викладене автори ставлять за мету розробити методику оцінки кібернетичної захищеності організації, що забезпечує перейти від якісних до кількісних показників в оцінці.

Методика оцінки рівня кіберзахищеності організації має забезпечувати можливість фахівці кібернетичної безпеки організації розрахувати рівень кіберзахищеності та надати числовий показник керівнику організації для того, щоб впевнитися у виконанні вимоги чинного законодавства України із забезпечення кіберзахисту установи.

Рішення цього завдання передбачає розробку підходу для визначення кількісного показника рівня кіберзахищеності і трансформація в кількісні значення якісного показника заданого рівня захищеності і проведення оцінки його отриманих результатів. Для отримання кількісної оцінки показника кіберзахищеності може бути використаний апарат теорії ймовірності, теорії прийняття рішень, теорії масового обслуговування і теорії надійності, що дозволить з достатньою точністю описувати (моделювати) процеси, які протікають в захищеній інформаційній системі.

Аналіз відкритих джерел в мережі Інтернет за ключовим словам «методика оцінки кібернетичної захищеності організації» не дав позитивного результату, що свідчить про недослідженість даного питання або напрямок за яким публікації становлять державну таємницю.

Методика побудована на процесі інтерв'ювання різних фахівців (керівників, системних адміністраторів, інших фахівців кібернетичної безпеки), що складається з опитувального листа, який, у свою чергу, розбитий на групи, що дозволяють оцінити рівень кіберзахищеності інформаційно-телекомунікаційної системи зв'язку організації: вимоги з організаційного захисту; вимоги з технічного захисту (витоки по технічних каналах; загрози несанкціонованого доступу); вимоги з програмного захисту; рівень захищеності (модель порушника; типи загрози; базові моделі загроз).

Запропонована методика оцінки кібернетичної захищеності організації складається з наступних етапів :

1 «Оцінка виконання вимоги з організації кібернетичного захисту»;

2 «Оцінка кібернетичної захищеності організації від загрози витоку інформації щодо керування правами доступу (адміністрування)»;

2.1 «Оцінка кібернетичної захищеності організації від загрози витоку акустичній інформації керування правами доступу»;

2.2 «Оцінка захищеності організації від загрози витоку візуальній інформації про права доступу»;

2.3 «Оцінка кіберзахищеності організації від загрози знищення, розкрадання апаратних засобів, матеріальних носіїв інформації шляхом фізичного несанкціонованого доступу»;

2.4 «Оцінка спроможності забезпечення кіберзахищеності організації

шляхом розмежування прав доступу»;

3 «Оцінка кіберзахищеності організації від загроз несанкціонованого доступу»;

3.1 «Оцінка кіберзахищеності організації від заходів розвідки кібернетичної інфраструктури»;

3.2 «Оцінка кіберзахищеності організації від заходів кібернетичного впливу на функціонування кібернетичної інфраструктури»;

3.3 «Оцінка спроможності забезпечення кіберзахищеності організації шляхом застосування системи кібернетичного захисту інфраструктуру»;

3.4 «Оцінка кіберзахищеності організації з виконанню вимог з програмного захисту»;

4 «Моделі внутрішнього і зовнішнього порушника»;

5 «Загальна оцінка рівня кіберзахищеності організації».

Кожен етап методики має включати перелік питань, за результатами опитування фахівців та відповідальних за інформаційну та кібернетичну безпеку на відповідність вимог інспектор визначає рівень забезпечення кібернетичної захищеності організації.

Таким чином, на даний час відсутня загальна методика оцінки кібернетичної захищеності організації. Поясненням цьому може бути те, що до складу методики можуть входити набагато більше складових - по мірі збільшення загроз, а наявні міждисциплінарні зв’язки ускладнюють їх вираховування на практиці; методика ґрунтується на процесі інтерв’ювання різних фахівців (керівників, системних адміністраторів, інших фахівців кібернетичної безпеки), що складається з опитувального листа; визначені питання у опитувальному листі не є догмою та можуть бути відкоректовані (уточнені) за потреби.

*УДК 004.056.5*

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

## ЗАХОДИ ПРОТИДІЇ ПРИХОВАНОЇ ПЕРЕДАЧІ ІНФОРМАЦІЇ В ЛОКАЛЬНИХ МЕРЕЖАХ

Однією з актуальних проблем функціонування інформаційно-телекомунікаційних систем на об’єктах критичної інфраструктури є можливість попадання інформації обмеженого доступу в локальні обчислювальні мережі (ЛОМ) організації, які мають доступ до ресурсів глобальної

мережі Інтернет, що автоматично призводить до появи ризиків, пов'язаних з можливістю витоку закритої інформації.

Численні дослідження, проведені в останні роки, показують, що більше 80% усіх інцидентів, пов'язаних з порушенням інформаційної безпеки, викликані внутрішніми загрозами. Причому витоки з використанням мереж, у тому числі Інтернету, складають більше 40% від усіх умисних інцидентів. Джерелами таких загроз, що спричиняють порушення конфіденційності інформації, є, як правило, інсайдери, тобто особи, що мають через свій службовий стан доступ до інформації обмеженого доступу.

Усе це вказує на те, що існує дуже актуальна проблема виявлення прихованої передачі закритої інформації по мережах.

Як правило, канал витоку інформації шляхом її прихованої передачі виявляється тільки після його тривалої експлуатації порушником. У випадках, коли об'єднання комп'ютерів в ЛОМ припускає підключення цієї мережі до зовнішніх мереж, виникає ряд можливостей утворення прихованих каналів витоку інформації обмеженого доступу, до яких слід віднести:

- несанкціоноване копіювання інформації обмеженого доступу на зовнішні носії з наступним їх винесенням за межі контрольованої зони;
- виведення на друк закритої інформації та її винесення на роздрукованих документах за межі контрольованої зони;
- несанкціонована передача інформації обмеженого доступу по мережі в зовнішні мережі за межі контрольованої зони;
- розкрадання носіїв закритої інформації.

Найбільшу небезпеку придбавають такі способи прихованої передачі інформації, як:

- використання порушниками анонімних https- та інших захищених проксі-серверів: тунелювання, що дозволяє порушникові, використовуючи дозволений протокол, передавати по ньому закриту інформацію, минувши міжмережевий екран;
- стеганографічні методи приховання інформації в різних файлах;
- шифрування порушником інформації обмеженого доступу перед її відправкою;
- перестановка мережевих пакетів певним чином (при цьому на основі заздалегідь обумовлених ознак передається послідовність біт);
- використання порушником троянських та інших шкідливих програм для реалізації прихованої передачі інформації.

Незалежний експерт з питань інформаційної безпеки Роберт Мерфі (США) представив програмний продукт VoodooNet. Для прихованої передачі інформації тут використовується протокол IPv6. Багато продуктів забезпечення безпеки не контролюють дані, передавані по цьому протоколу, тоді як цей стандарт підтримується програмним забезпеченням маршрутизаторів. Для вирішення проблеми прихованої передачі інформації цим

способом необхідно використовувати мережеві пристрої, контролюючі дані, що передаються по протоколу IPv6.

Для закриття таких каналів слід використовувати комплекс організаційно-технічних заходів, що включають:

- ізолювання ЛОМ для роботи з інформацією обмеженого доступу, тобто їх повне відключення від зовнішніх мереж;
- використання системи видаленого і локального моніторингу робочих станцій користувачів з боку адміністраторів;
- використання засобів криптографічного і антивірусного захисту інформації;
- застосування засобів контентного аналізу передаваних даних як в зовнішню мережу, так і із зовнішньої мережі в ЛОМ організації;
- застосування засобів контролю доступу до зовнішніх носіїв.

Таким чином, проблема витоку інформації обмеженого доступу тільки зростає. Це вимагає на об'єктах критичної інфраструктури пильної уваги адміністраторів безпеці. Крім того, потрібне впровадження організаційних методів (розробка регламентів забезпечення інформаційної і кібербезпеки з обов'язковим доведенням до усіх співробітників організації), перевірка встановлюваного програмного забезпечення на наявність недекларованих можливостей, екранування мережі, наявність грамотно налагодженої системи антивірусного захисту, а також постійний контроль користувачів по використанню засобів зберігання інформації (використання мобільних пристроїв).

*УДК 351.741*

**Комісаров О.Г.**
доктор юридичних наук, професор
Національна академія СБ України

## ПИТАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У МІСЦЯХ, ЯКИМИ ПЕРЕМІЩУЮТЬСЯ ОСОБИ

За усталеною практикою поняттям «інформаційна безпека» позначають певний стан захищеності систем *обробки і зберігання даних*, при якому забезпечено *конфіденційність, доступність і цілісність* інформації, а також унеможливлено несанкціонований доступ до такої інформації, у т.ч. з метою її використання у протиправних цілях. Поняття «інформаційна безпека держави», яке є похідним від поняття «інформаційна безпека», характеризується ступенем захищеності та стійкості основних сфер життєдіяльності по відношенню до небезпечних інформаційних впливів. Використання обох понять не може бути обмеженим лише сферою технічних

систем, формою надання (зберігання) даних тощо та стосується усіх аспектів безпеки людини та держави як творців/носіїв суспільно корисної інформації.

«Переміщення» особи є системою цілеспрямованих дій (поведінки) окремої людини працездатного віку, яка виходить за межі сімейних і трудових відносин та ними не обумовлюється. Будь-яку місцевість та територію на яких перебуває особа, а також будь-які системи *обробки і зберігання даних*, що «обслуговують» такі території можливо розділяти на категорії: «родина», «робота», «переміщення». Щодо останньої слід враховуючи тенденцію до збільшення відкритості інформації про можливість та безпечність переміщення територією із збільшенням масштабів її охорони. За таких умов, окрім зовнішніх меж «переміщення», слід розглядати також його внутрішню інформаційну систему, побудовану за принципом суспільного визнання та унормування окремих правил поведінки особи у цих місцях.

Виходячи із сутності інформаційного суспільства «переміщення» скеровує цілі низки взаємопов'язаних процесів: 1) процес перетворення інформації і знань на важливий ресурс та рушійну силу соціально-економічного розвитку людини; 2) процес приєднання людини до ринків інформації і знань, а також їх розгляду на одному рівні з ринками природних ресурсів, праці і капіталу щодо такої людини; 3) процес стрімкого зростання питомої ваги галузей, що забезпечують створення, передачу, обробку і використання інформації у життєдіяльності окремої людини; 4) процес розвитку інформаційної інфраструктури та її спільного із транспортною інфраструктурою перетворення на умову, що визначає національну та регіональну конкурентоспроможність, безпечність і комфортність проживання та життєдіяльності окремої людини.

«Фактичне переміщення» (вихід людини за межі місця проживання чи робочого місця) завжди зумовлене метою, яка не посягає на встановлений порядок і суспільну безпеку, цілком підтримується та пропагується суспільством як за допомогою морально-виховних й економічних засобів, так і засобів, що формалізовані у певному нормативно-правовому акті, який закріплює «доцільність» переміщення. Щодо останнього особа має розглядатися як користувач певної ділянки місцевості по якій вона здійснює «фактичне переміщення», системи *обробки і зберігання даних*, що «обслуговують» таку ділянку, та, відповідно, як споживач інформаційної продукції (інформаційної послуги) – результату інформаційної діяльності певної галузі господарства.

Здійснення особою будь-якого «фактичного переміщення» є можливим лише у межах Єдиної транспортної системи України із використанням окремих його об'єктів (транспорту загального користування (залізничний, морський, річковий, автомобільний і авіаційний, а також міського

електротранспорту, у тому числі метрополітену), відомчого транспорту) та шляхів сполучення загального користування. При цьому відповідне переміщення є можливим лише у визначеному у законі режимі, який, у свою чергу, є відображенням пануючих у суспільстві соціально-економічних відносин.

Окрім мети «переміщення», важливими є внутрішні кордони безпеки переміщення, в межах яких розробляються і діють правила поведінки. В цих кордонах накопичується та обробляється: 1) інформація щодо меж «родини» та «робочого місця», отримана під час правоохоронних заходів; 2) інформація щодо формулювання мети (напрямку) «переміщення», яке здійснювалося людиною відповідно до власної системи життєвих цінностей та з використанням відповідного «сленгу»; 3) відомості щодо внутрішніх кордонів безпеки, перетинання яких людина вважає доцільним під час «переміщення» у власній системі координат; 4) інформація щодо наявності загальновизнаних та затверджених нормативними актами правил поведінки у внутрішніх межах – публічних (громадських) місцях, які відвідує людина доведена до відома людини під час їх перетинання.

*УДК 004.056.5*

**Корченко О. Г.**
доктор технічних наук, професор
**Дрейс Ю. О.**
кандидат технічних наук, доцент
**Романенко О. О.**
Національний авіаційний університет

## КЛАСИФІКАЦІЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ

Автоматизація процесів надання послуг в усіх сферах забезпечення життєдіяльності людини, суспільства і держави призвела до посилення вимог до захисту інформації (ЗІ) в інформаційно-телекомунікаційних системах (ІТС) потенційно небезпечних об'єктів критичної інфраструктури (ОКІ). Відповідно до існуючого нормативно-правового забезпечення, пов'язаного з ОКІ, прослідковується неповнота щодо можливості їх коректної класифікації, також не сформований перелік ІТС таких об'єктів, відсутні критерії щодо оцінювання негативних наслідків від кібератак. Вирішення зазначених питань дозволить сформувати такий класифікатор об'єктів критичної інформаційної інфраструктури (ОКІІ), який дасть можливість створити умови для підвищення їх стійкості до кібератак. Відповідно до цього пропонується засіб класифікації ОКІІ держави. В основу його побудови закладена кортежна модель, складовими якої є упорядковані

ідентифікатори ОКІ, що відображають: сектор критичної інформаційної інфраструктури держави, форму власності власника / розпорядника ІТС, вид інформації, негативні наслідки кібератак на ІТС, тощо. За допомогою запропонованої моделі представлені приклади класифікації ОКІІ держави, а в подальшому вона дасть можливість сформувати перелік відповідних ІТС для забезпечення їх першочергового захисту від кібератак.

На основі проведеного аналізу відповідної нормативно-правової бази та інших публікацій [1-5] пропонується базова кортежна модель для класифікації ОКІІ держави, яка містить основні ідентифікатори об'єкта:

$$\mathbf{ID} = < \mathbf{ID}_1, \mathbf{ID}_2, ..., \mathbf{ID}_i, ..., \mathbf{ID}_n >, \quad (1)$$

де $\mathbf{ID}_i \subseteq \mathbf{ID}$ $(i = \overline{1,n})$ – компонент кортежу, що відображає *i*-й ідентифікатор об'єкта, *n* їх кількість, а для всіх членів **ID** характерна властивість порядку.

Наприклад, для формування переліку ІТС ОКІ держави відповідно до [2, 5], при $n = 8$ кортеж (1) визначимо як:

$$\mathbf{ID} = < \mathbf{ID}_1, \mathbf{ID}_2, \mathbf{ID}_3, \mathbf{ID}_4, \mathbf{ID}_5, \mathbf{ID}_6, \mathbf{ID}_7, \mathbf{ID}_8 > = < \mathbf{S}, \mathbf{U}, \mathbf{O}, \mathbf{N}, \mathbf{I}, \mathbf{R}, \mathbf{C}, \mathbf{M} >, \quad (2)$$

де $\mathbf{ID}_1 = \mathbf{S}$ (множина ідентифікаторів секторів (*Sectors*) КІІ); $\mathbf{ID}_2 = \mathbf{U}$ (множина ідентифікаторів адміністративно-територіальних одиниць (*Units*) України); $\mathbf{ID}_3 = \mathbf{O}$ (множина форм власності (*Ownership*) організацій-власників / розпорядників ІТС); $\mathbf{ID}_4 = \mathbf{N}$ (множина назв або/та унікальних ідентифікаційних номерів (*Number*) юридичної особи в Єдиному державному реєстрі підприємств та організацій України (ЄДРПОУ) організацій-власників / розпорядників ІТС як ОКІІ); $\mathbf{ID}_5 = \mathbf{I}$ (множина видів інформації (*Information*), що обробляється в ІТС); $\mathbf{ID}_6 = \mathbf{R}$ (множина реєстраційних номерів (*Registration*) документів, що засвідчують наявність атестованих/ліцензованих систем чи засобів захисту інформації (наприклад, атестатів відповідності на КСЗІ (КЗЗІ, СУІБ) або експертних висновків на технічні та програмні засоби, які реалізують функції ТЗІ та/або оцінки стану ЗІ чи на організаційно-технічне рішення на розгортання типової складової компоненти КСЗІ в ІТС); $\mathbf{ID}_7 = \mathbf{C}$ (множина ідентифікаторів негативних наслідків (*Consequences*) кібератак на ІТС); $\mathbf{ID}_8 = \mathbf{M}$ (множина ідентифікаторів геолокаційних ресурсів (*Maps*) за місцем знаходження ОКІІ).

В табл. 1 приведене умовне позначення семантики класифікатора ОКІІ держави, яке можна відобразити, як SS–UU–O–NN…N–RR…R–II–CC–MM.

Таблиця 1

Семантика класифікатора ОКІІ держави

| Елемент кортежу | **S** $(j = \overline{1,n_{1i}})$ | **U** | **O** | **N** | **R** | **I** | **C** | **M** |
|---|---|---|---|---|---|---|---|---|
| *i* | $\overline{1,5}$ | $\overline{1,27}$ | $\overline{1,3}$ | $\overline{1,n_4}$ | $\overline{1,n_5}$ | $\overline{1,3}$ | $\overline{1,10}$ | $\overline{1,3}$ |
| Елемент множини | *SS* | *UU* | *O* | *NN…N* | *RR…R* | *II* | *CC* | *M* |

Для прикладу розглянемо побудову семантичної структури класифікатора Державної фіскальної служби (ДФС) України як ОКІІ, що відображається у вигляді представленому в табл. 2.

Таблиця 2

Приклад класифікатора ОКІІ – ДФС України

| Елемент кортежу | **S** ($j = 7$) | **U** | **O** | **N** | **R** | **I** | **C** | **M** |
|---|---|---|---|---|---|---|---|---|
| *i* | 1 | 26 | 1 | 39292197 | 14273 | 2 | 8 | 1 |
| Елемент множини | 17 | 26 | 1 | 39292197 (ДФС – http://sfs.gov.ua) | 14273 | 03 | 08 | 1 |

Тобто, **17–26–1–39292197–14273–03–08–1**, де $\mathbf{S} \supseteq S_{17}$ = "17" – фінансовий сектор, $\mathbf{U} \supseteq U_{26}$ = "26" – місто Київ, $\mathbf{O} \supseteq O_1$ = "*Д*" = "1" – державна форма власності, $\mathbf{N} \supseteq N_1$ = 39292197 – універсальний ідентифікуючий номер ЄДРПОУ "ДФС" (http://sfs.gov.ua), $\mathbf{R} \supseteq R_1$ = 14273 – номер атестату відповідності на КСЗІ ІТС центру сертифікації ключів Інформаційно-довідкового департаменту ДФС, за реєстром Держспецзв'язку, $\mathbf{I} \supseteq I_2$ = "*CI*" = "03" – службова інформація, $\mathbf{C} \supseteq C_8$ = "08" – порушення сталого функціонування фінансової системи держави, $\mathbf{M} \supseteq M_1$ = "*GM*" = "1" – ресурс Google Maps.

На рис. 1 показано приклад відображення елементу множини **M**.

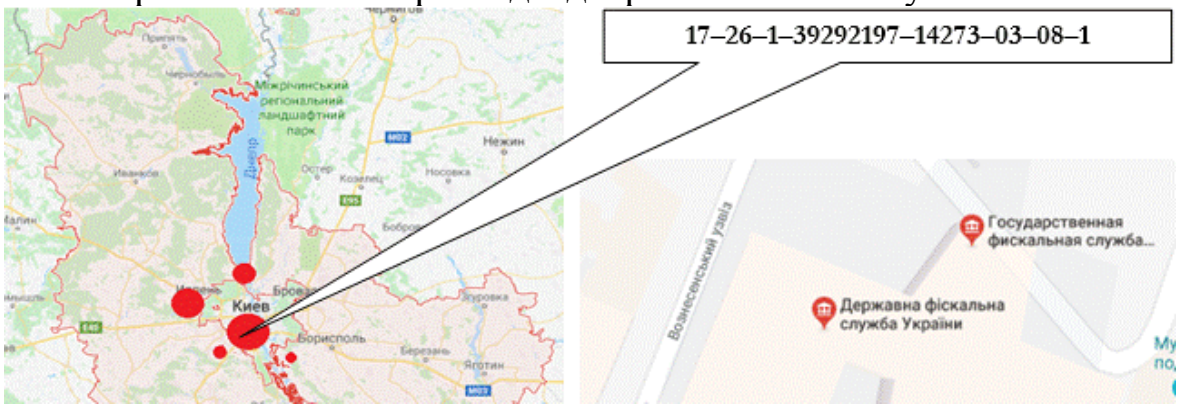



Рис. 1 – Приклад відображення $M_1$ = "*GM*" – зображення місця знаходження ДФС України

*Висновок.* Запропоновано базову кортежну модель класифікатора ОКІІ держави, яка за рахунок множин ідентифікаторів секторів, адміністративно-територіальних одиниць України, форм власності, назв організацій, видів інформації, реєстраційних номерів документів, ідентифікаторів негативних наслідків кібератак на ІТС, ідентифікаторів геолокаційних ресурсів за місцем знаходження КІІ, введених у кортеж дає змогу побудувати класифікатор та відобразити його у семантичному вигляді для подальшого створення практичного механізму формування переліку ІТС ОКІІ України.

**Література**

1. A. Korchenko, Y. Dreis, O. Romanenko, "Analysis problems in the field of state's critical infrastructure", Projekt interdyscyplinarny projektem XXI wieku: Monografia. Tom 1. – Akademia Techniczno-Humanistyczna w Bielsku-Bialej, 2017. – pp. 397-402.

2. О. Корченко, Ю. Дрейс, О. Романенко "Критична інформаційна інфраструктура України: терміни, сектори і наслідки", Захист інформації. – 2017. – Т. 19. – № 4. – С. 303-309.

3. Ю. Дрейс "Аналіз базової термінології і негативних наслідків кібератак на інформаційно-телекомунікаційні системи об'єктів критичної інфраструктури держави", Захист інформації. – 2017. – Т. 19. – № 3. – С. 214-222.

4. Ю. Дрейс, О. Романенко "Розширення базової термінології у сфері захисту критичної інформаційної інфраструктури держави", Автоматика та комп'ютерно-інтегровані технології у промисловості, телекомунікаціях, енергетиці та транспорті : матеріали Всеукраїнської науково-практичної інтернет-конференції, 16-17 листопада 2017. – Кропивницький : ЦНТУ, 2017. – С. 185.

5. О. Корченко, Ю. Дрейс, О. Романенко "Формування множини ідентифікаторів для класифікації об'єктів критичної інформаційної інфраструктури", Актуальні проблеми забезпечення кібербезпеки та захисту інформації: Тези доповідей учасників IV Міжнародної науково-практичної конференції, Закарпатська область, Міжгірський район, село Верхнє Студене, 21-24 лютого 2018 р. – К. : Вид-во Європейського університету, 2018. – С. 81-86.

*УДК 004.738.5:373.2-053.5(045)*

**Косик В.М.**
начальник відділу цифрової освіти та ІКТ
ДНУ «Інститут модернізації змісту освіти»
**Мельник О.М.**
кандидат педагогічних наук,
старший науковий співробітник
відділу цифрової освіти та ІКТ
ДНУ «Інститут модернізації змісту освіти»

## БЕЗПЕКА ДІТЕЙ В ІНТЕРНЕТ ЯК ЕЛЕМЕНТ ЦИФРОВОЇ ГРАМОТНОСТІ

З метою реалізації ініціатив "Цифрового порядку денного України 2020" (цифрова стратегія), створеного для усунення бар'єрів на шляху цифрової трансформації України у найбільш перспективних сферах, Кабінет Міністрів України схвалив Концепцію розвитку цифрової економіки та суспільства України на 2018-2020 роки (далі – Концепція) та затвердив план заходів щодо її реалізації.

Основними питаннями, на вирішення яких спрямовано Концепцію, є стимулювання економіки та залучення інвестицій, трансформація української економіки в конкурентоспроможну та ефективну за рахунок її «циф-

ровізації»; нівелювання «цифрового розриву», наближення цифрових технологій до громадян, у тому числі, шляхом забезпечення доступу до широкосмугового Інтернет, особливо у селищах та невеликих містах.

В наш час інформація стає провідним ресурсом економічного, соціального, політичного і культурного розвитку, а сучасні технології її обробки і поширення тільки посилюють цю тенденцію. Зростає темп життя, що у свою чергу вимагає підвищення рівня мобільності та адаптивності людей до умов, що постійно змінюються. Це стосується і сучасної дитини, яка вже народжується та живе у цифровому світі. З кожним роком діти все частіше починають використовувати мережу інтернет з раннього віку. Найчисельніші користувачі сучасних технологій сьогодні, різноманітних соцмереж, Інтернету тощо – це діти та підлітки, які знаходять там потрібну інформацію, грають в онлайн ігри, слухають музику, дивляться фільми, спілкуються, знайомляться, знаходять нових друзів та ін. Але нові можливості збільшують кількість ризиків. Крім позитивної сторони Інтернет-взаємодії, є небезпечна та негативна, тому учнів слід навчати, як зробити спілкування в Інтернет просторі безпечним, як максимально ефективно використати технології без надання шкоди іншим користувачам, тобто готувати їх до подальшого життя в цифровому суспільстві. Сьогодні правила інформаційної безпеки в онлайн-середовищі є своєрідними правилами дорожнього руху в мережі, від знання та дотримання яких часто залежить життя Інтернет-користувача. Тому однією з десяти ключових компетентностей, на формування яких спрямована Концепція реалізації державної політики у сфері реформування загальної середньої освіти «Нова українська школа» на період до 2029 року, є інформаційно-цифрова. Вона «передбачає впевнене, а водночас критичне застосування інформаційно-комунікаційних технологій для створення, пошуку, обробки, обміну інформацією на роботі, в публічному просторі та приватному спілкуванні» [1].

Тому змінюється і роль сучасного учителя – він повинен стати координатором інформаційних відомостей, володіти сучасними методиками і новими освітніми технологіями, щоб спілкуватися з учнями однією мовою, не відставати від прогресу, вчити дітей безпечній поведінці в Інтернет просторі, в тому числі на власному прикладі.

Навчання учнів критично ставитися до використання Інтернету включає в себе роз’яснення в чому полягає небезпека розміщення в мережі конфіденційної, особистої інформації та фото; як підібрати надійний пароль та реагувати належним чином на листи від незнайомців; як захистити свій пристрій від вірусів та активувати параметри безпеки від небажаного контенту, як правильно поводитися в онлайн просторі та перевіряти достовірність отриманої інформації тощо. На сайті ДНУ «Інститут модернізації змісту освіти» створено сторінку «Безпека в Інтернеті», на якій можна знайти багато корисної інформації з цього питання (https://imzo.gov.ua/diyalnist/bezpeka-v-interneti/).

Розуміючи актуальність питання інформаційної безпеки в онлайн-середовищі у вівторок другого тижня лютого кожен рік у світі відмічається День безпечнішого Інтернету, який було запроваджено у 2004 році. Цього року він пройшов під гаслом «Створюй, спілкуйся та поважай: кращий Інтернет починається з тобою». Але слід пам'ятати, що Інтернет має бути безпечним не лише один день на рік. Зробити це можна шляхом поєднання зусиль дітей, батьків, учителів та держави, бібліотек, вищих навчальних закладів, дитячих та молодіжних організацій, громадських організацій, закладів післядипломної педагогічної освіти та інших установ.

**Література**

1. Розпорядження КМУ № 988-р від 14.12.16 року «Про схвалення Концепції реалізації державної політики у сфері реформування загальної середньої освіти "Нова українська школа" на період до 2029 року». URL: https://osvita.ua/legislation/Ser_osv/54258/ (дата звернення 09.03.2018).

2. Розпорядження КМУ від 17 січня 2018 р. № 67-р «Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018—2020 роки та затвердження плану заходів щодо її реалізації» URL: http://zakon5.rada.gov.ua/laws/show/67-2018-%D1%80 (дата звернення 09.03.2018).

*УДК 354.42*

**Косогов О. М.**
кандидат військових наук,
старший науковий співробітник
**Сірик А. О.**
військова частина А1906

## ПІДХІД ДО МОДЕЛЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ДЕРЖАВНОЇ УСТАНОВИ

Ризик, пов'язаний з інформаційною безпекою державної установи, є багатовимірним складним поняттям, яке вміщує множину змінних. Основою моделювання ризику є його декомпозиція на логічні одиниці, що є дрібними складовими проблеми, такими, як наприклад, "безпека робочих станцій" або "безпека даних у системі резервного копіювання", які, у свою чергу, розподіляються на ще більш дрібні компоненти доти, поки оцінка елемента не зведеться до тривіального питання. Наступними кроками є оцінювання складових, отриманих під час декомпозиції, поширення інформації від нищого до вищого рівня ієрархії та розрахунок величини ризику.

Незважаючи на те, що традиційно ризик визначається як сукупність ймовірностей негативної події та потенційного збитку [1, 2], в інформа-

ційній безпеці (ІБ) сьогодні такий підхід застосовувати недоцільно, принаймні, якщо розглядати ймовірності в класичному трактуванні. Виникає багато проблем, які перешкоджають точному, кількісному оцінюванню, головною серед яких є брак даних – статистики відносно зламів і атак практично немає, особливо такої, яка б відповідала на запитання: наскільки інтенсивно інформація піддається небезпеці?

Проблема загострюється й тим, що потенційне джерело атак не є стохастичним генератором, який підлягає тільки випадковому розподілу, а найчастіше інтелектуальним агентом, тобто людиною, яка діє раціонально й насамперед, спрямовано. Таким чином, навіть маючи деяку частотну характеристику розподілу типу атак, використати лише її для оцінювання ризику ІБ недоцільно, тому що забезпечення захисту від атак, передусім, не гарантує безпеки даних.

Такі міркування наводять на те, що потрібно оцінювати не ймовірність потенційних подій, а їх реалізацію з урахуванням заходів протидії, іншими словами – рівень уразливості державної установи як об'єкта інформаційної безпеки. Таким чином, проблема з категорії "розрахунок імовірності" може бути переведена в категорію "агрегація даних". Критичним аспектом у вирішенні цього завдання є вибір математичного апарату, що забезпечив би достатній ступінь семантичної виразності, зокрема, давав би змогу враховувати не тільки ваги окремих компонентів ризику, а й взаємодію між ними.

Оператором агрегації пропонується використовувати інтеграл Шоке, який ґрунтується на поняттях нечіткої міри.

Семантичні можливості інтеграла Шоке дають змогу:

враховувати значимості компонентів, що агрегуються – операція визначення відносної ваги компонентів;

визначати характер агрегації (кон'юнктивну або диз'юнктивну спрямованість);

визначати ваги груп критеріїв;

визначати необхідні й достатні критерії.

Тобто для опису неадитивної нечіткої міри $\mu$ потрібно визначити $(2^n - 2)$ коефіцієнти, що істотно ускладнюють процес моделювання. Однак є декілька шляхів зменшення цієї кількості [3, 4]. Варто згадати, що кожний достатній або необхідний критерій зменшує кількість обумовлених коефіцієнтів у 2 рази [4].

Викладений підхід до моделювання ризиків ІБ порівнювався з імовірнісним підходом.

А тому агреговане значення, що розраховане за допомогою інтеграла Шоке, має більш позитивну оцінку, обмежену зверху значенням 0.5, а за допомогою ймовірнісного підходу – більше негативну, обмежену знизу значенням 0.5.

Причиною цього є різне семантичне трактування значень. Для теорії ймовірностей, 0.5 означає, що механізм забезпечення ІБ зупинить 50% атак. Така оцінка була б правильною за умови рівномірного частотного розподілу атак за якістю виконання й рівномірного ж розподілу вектора атаки. Іншими словами, кількість добре підготовлених експертних атак уважається рівною числу некваліфікованих спроб вторгнення, а спосіб атаки обирається випадково з імовірністю 1/3. Тому збільшення якості одного механізму із трьох веде до лінійного росту загальної захищеності установи. Для інтеграла Шоке, значення критерію виражає його якість. Тобто, 0.5 буде означати, що механізм здатний зупинити атаки певного рівня за шкалою [0,1].

Отже, можна з упевненістю заявити, що використання методики, заснованої на інтегралі Шоке має перевагу над імовірностним методом для моделювання в рамках досліджуваної проблеми.

**Література**

1. ISO/IEC Guide 73:2002 Risk management Vocabulary Guidelines for use in standards.

2. Managing Risk from Information Systems. An Organizational Perspective. SP-800-39. NIST Special Publication, 2007.

3. Sugeno M. Theory of fuzzy integrals and its applications. PhD thesis, Tokyo Institute of Technology, 1974.

4. Choquet G. // Annales de l'Institut Fourier, 1953. V. 5. P. 131.

*УДК 342.9*

**Костенко О.В.**
головний науковий співробітник
Інститут спеціальної техніки та судових експертиз
Служби безпеки України

## КОМПРОМЕТАЦІЯ ОСОБИСТОГО КЛЮЧА ЕЛЕКТРОННОГО ПІДПИСУ (ПРАВОВИЙ АСПЕКТ)

Розвиток телекомунікаційних технологій сприяв виникненню механізмів обміну між користувачами документами в електронній формі, які мають юридичну значимість. Потреба в використанні та обміні такими документами була настільки високою, що багато країн майже одночасно прийняли спеціальні закони, що регулювали основи електронної торгівлі та застосування електронних підписів. Це також посприяло виникненню нових суспільних відносин пов'язаних із обміном інформації у формі електронних (цифрових) документів між суб'єктами правовідносин під час:

електронного руху капіталу (Electronic Funds Transfer); електронної торгівлі (e-Trade); електронних грошей (e-cash); електронного маркетингу (e-market); електронного банкінгу (e-banking); електронної системи здоров'я (e-health); електроуного урядування (e-gov) тощо.

Надійність та цілісність інформації під час обміну інформацією у формі електронних (цифрових) документів між суб'єктами правовідносин забезпечується застосуванням алгоритмів електронного криптографічного захисту із використанням технології електронного підпису. Однак широке застосування цієї технології водночас виявило й правові проблеми, пов'язані із використанням особистого ключа електронного підпису, таку як, наприклад, правова невизначеність дефініції «Компрометація».

Аналіз іноземного і вітчизняного законодавства в галузі електронного підпису дозволяє констатувати, що на рівні національних та міжнародних нормативно-правових актів немає ні загальноприйнятого, ні однозначного визначення терміну «компрометація» [1-7]. А це означає, що відсутня не тільки сама дефініція «компрометація», а й фактично не має чіткого визначення та переліку подій або підстав, що дають можливість беззаперечно вважати їх компрометаційними, і, відповідно, бути базовими «маяками» для правознавців, які сьогодні оцінюють прецеденти порушення законодавства, пов'язані із використанням особистого ключа цифрового підпису. Також законодавство не надає правову оцінку діям або бездіяльність підписувача, які призвели до компрометації особистого ключа електронного підпису, а відсутність переліку базових ознак компрометації особистого ключа електронного підпису створює неоднозначність трактування правознавцями ознак злочинів, які вчиняються із використанням електронного підпису.

Цілком очевидно, що велика кількість визначень поняття «компрометація» призводить до необхідності формування загальноприйнятої дефініції терміну «компрометація» із обов'язковим урахуванням проблем, пов'язаних із складністю надання правознавцями оцінки юридичним наслідкам компрометації особистого ключа в період між реальним фактом компрометації та фактом її офіційного оголошення [8].

В умовах відсутності загальновизнаного визначення терміну «компрометація», зважаючи на наявну неврегульовану нормами права проблему суспільних відносин, пов'язану з використанням електронного підпису пропонуємо нову дефініцію:

«Компрометація особистого ключа електронного підпису як будь-яка явна або не явна подія та/або дія (втрата, розголошення, крадіжка, несанкціоноване копіювання тощо) з даними особистого ключа електронного підпису та засобами криптографічного захисту інформації, що призвела або може призвести до несанкціонованого розголошення, зміни, знищення, блокування, перехоплення, копіювання та використання особистого

ключа електронного підпису, а також інформації, яка обробляється та передається за його допомогою.

Явною компрометацією особистого ключа електронного підпису є втрата доступу до інформації особистого ключа, за участю або бездіяльністю підписувача або третіх осіб без застосування технічних засобів.

Неявною компрометацією особистого ключа електронного підпису є втрата доступу до інформації особистого ключа електронного підпису із застосуванням будь-яких технічних засобів без участі підписувача».

Дане визначення містить загальну норму компрометації та два деталізованих визначення явної та неявної компрометації. Такий підхід дозволить здійснювати більш якісну кваліфікацію суспільно небезпечних протиправних дій із використанням особистого ключа електронного підпису.

Дефініцію «компрометація особистого ключа» у пропонується внести до пункту 26 статті 1 Розділу І Закону України «Про електронні довірчі послуги».

**Література**

1. Типовой закон ЮНСИТРАЛ об электронных подписях. – Режим доступа : http://zakon0.rada.gov.ua/laws/show/995_937.

2. FIPS PUB 140-2. Security requirements for cryptographic modules [Електронний ресурс] // National Institute of Standards and Texchnology, May 25, 2001. – Режим доступу: https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402.pdf.

3. NIST SP 800-57 Part 3 Revision 1 Recommendation for Key Management [Електронний ресурс] // National Institute of Standards and Texchnology, January 2015. – Режим доступу: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57Pt3r1.pdf.

4. NIST SP 800-130 A Framework for Designing Cryptographic Key Management Systems [Електронний ресурс] // National Institute of Standards and Texchnology, August 2013. – Режим доступу: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-130.pdf.

5. Про довірчі послуги: Закон України від 05.10.2017 № 2155-VIII // Відомості Верховної Ради України. – 2017. – №45. – ст.400.

6. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-003-99, наказ ДСТСЗІ СБУ від 28.04.1999 № 22 [Електронний ресурс]. – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/doccatalog/list?currDir=41640.

7. Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту конфіденційної інформації та відкритої інформації з використанням електронного цифрового підпису: наказ ДССЗЗІ України від 20.07.2007 № 141: зареєстровано в Міністерстві юстиції України 30.07.2007 за № 862/14129 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/z0862-07.

8. Mike Just, Paul C. van Oorschot Addressing the Problem of Undetected Signature Key Compromise [Електронний ресурс] – Режим доступу: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.26.507&rep=rep1&type=pdf.

*УДК 351.865: 007.51: 004.02*
**Левченко О. В.**
кандидат військових наук, професор
Житомирський військовий інститут ім. С. П. Корольова

# МЕТОДОЛОГІЧНИЙ ІНСТРУМЕНТАРІЙ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Одним з ключових завдань системи забезпечення інформаційної безпеки (СЗІБ) є захист національних інтересів України у різних сферах. В умовах агресії, що триває проти України питання забезпечення її воєнної безпеки в інформаційній сфері стоїть особливо гостро [1]. Тому принципи побудови та основи функціонування СЗІБ у воєнній сфері в першу чергу повинні опиратися на дієвий та ефективний методологічний інструментарій (МІ).

На сьогодні розробленню та обґрунтуванню МІ оцінювання ефективності СЗІБ у воєнній сфері приділяється значна увага в фаховій науковій літературі. Більшість з цих та інших проаналізованих за темою наукових праць присвячені питанням удосконалення організаційної структури СЗІБ. У наукових працях, наприклад в [2, 3], розкриваються питання щодо підвищення ефективності функціонування СЗІБ в умовах дії різного роду небезпек та загроз. При цьому не завжди враховується те, що інформаційний чинник в сучасних умовах є не менш важливим, ніж воєнний. Таким чином, у результаті науково-технічного аналізу встановлено, що МІ оцінювання ефективності СЗІБ у воєнній сфері потребує подальшого розвитку. Зокрема обґрунтування та розроблення потребує система критеріїв та показників оцінювання ефективності СЗІБ, метод оцінювання ефективності СЗІБ та методика оцінювання ефективності СЗІБ. Нижче послідовно розкриємо сутність та зміст вирішення зазначених завдань.

Виходячи з основних положень теорії систем та розглядаючи СЗІБ як складну багатокомпонентну ієрархічну організаційно-технічну систему, а також додержуючись базових принципів П. Фішберна, можна стверджувати, що всі критерії оцінювання доцільно згрупувати за такими ознаками: перша група – функціональні ознаки; друга група – організаційно-технічні ознаки; третя група – цільові ознаки. Розкриємо фізичний зміст кожної із запропонованих груп розробленої *системи критеріїв*.

Перша група критеріїв описує функціональну ефективність СЗІБ відповідно до визначених цілей та завдань. Основними критеріями для даної групи пропонується обрати: продуктивність; захищеність, керованість; ресурсоспоживання та функціональність.

Друга група критеріїв характеризує ефективність СЗІБ, яка обумовлена організаційно-технічними аспектами функціонування системи. До неї пропонується включити такі критерії: структурної відповідності СЗІБ покладеним на неї функціям і завданням; здатності її підсистем до виконання завдань за призначенням; рівня забезпеченості СЗІБ технічними, програмними і спеціальними засобами; рівня забезпечення фінансовими ресурсами; наявності й досконалості національного законодавства та відомчої нормативно-правової бази; наявності взаємодії з державними та відомчими інституціями щодо забезпечення інформаційної безпеки.

Третя група критеріїв описує цільову ефективність функціонування СЗІБ. Основними її критеріями визначимо: готовність до реагування на інформаційні загрози (ІЗ); оперативність реагування на ІЗ; повнота виконання завдань реагування на ІЗ; безперервність виконання завдань за призначенням.

Описані вище групи критеріїв виступають підґрунтям для створення відповідного *методу оцінювання ефективності СЗІБ*. Розроблений графоаналітичний метод оцінювання ефективності СЗІБ полягає в обчисленні наведених вище показників шляхом розрахунку площ геометричних фігур – багатокутників, які вони утворюють у результаті побудови секторних діаграм. Кількість багатокутників дорівнює кількості груп у запропонованій системі критеріїв, а кількість вершин у кожному багатокутнику визначається кількістю показників у даній групі. Враховуючи те, що для кожної групи багатокутник має свою кількість вершин, а значить і площу, то для подальшого коректного і достовірного обчислення ефективності функціонування СЗІБ у методі передбачено здійснення нормувальних процедур. Отже, числове значення оцінювання ефективності функціонування СЗІБ визначається площею багатокутника, утвореного відповідно до системи критеріїв, яка згідно з розробленою спеціально для цього фундаментальною нормованою оберненою шкалою оцінок узгоджується з якісною (лінгвістичною) оцінкою.

Описаний вище метод є основою *методики оцінювання ефективності СЗІБ*. На першому етапі методики шляхом розрахунків або експертним методом визначається множина вхідних даних для оцінювання ефективності функціонування СЗІБ. На другому етапі методики проводиться оцінювання частинної ефективності функціонування СЗІБ за кожною з обраних груп системи критеріїв. На третьому, заключному етапі, – оцінюванню підлягає ефективність функціонування СЗІБ у цілому. На основі одержаних кількісних і якісних оцінок розробляються практичні рекомендацій з підвищення ефективності функціонування СЗІБ та уживаються заходи з їх впровадження.

Отже, розроблений МІ оцінювання ефективності СЗІБ виступає підґрунтям для прийняття своєчасних та обґрунтованих управлінських рі-

шень. У перспективі на основі розробленого МІ планується створити програмний продукт, який автоматизуватиме процедури оцінювання ефективності СЗІБ.

**Література**

1. Левченко О. В. Еволюція гібридної війни Російської Федерації проти України / О. В. Левченко // Наука і оборона. – 2017. – № 2. – С. 16–19.

2. Богданович В. Ю. Теоретико-методологічні основи забезпечення національної безпеки України : монографія : у 7 т. – Т.4. Воєнна безпека держави і шляхи її забезпечення / В. Ю. Богданович, І. Ю. Свида, Є. Д. Скулиш; за заг. ред. Є. Д. Скулиша. – К. : Наук.-вид. відділ НА СБ України, 2012. – 464 с.

3. Грищук Р. В. Основи кібернетичної безпеки : монографія / Р. В. Грищук, Ю. Г. Даник ; під заг. ред. Ю. Г. Даника. – Житомир : ЖНАЕУ, 2016. – 636 с.

*УДК 331.107.5 : 65.012.8*

**Лісовська О.Л.**
кандидат економічних наук, доцент
**Ничитайло І.М.**
кандидат юридичних наук, доцент
Національна академія СБ України

## ДЕРЖАВНО-ПРИВАТНЕ ПАРТНЕРСТВО У СФЕРІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Одними з перших нормативно-правових документів, що регламентують запровадження державно-приватного партнерства у забезпеченні національної безпеки, стали документи, що регламентують забезпечення кібербезпеки України. Так, у Стратегії кібербезпеки України мова йде про те, що забезпечення кібербезпеки нашої держави має ґрунтуватися, зокрема на принципах «державно-приватного партнерства, широкої співпраці з громадянським суспільством у сфері забезпечення кібербезпеки та кіберзахисту» [4]. У Законі України «Про основні засади забезпечення кібербезпеки України» зазначений принцип, визначений вже як «державно-приватна взаємодія», уточнює – «шляхом обміну інформацією про інциденти кібербезпеки, реалізації спільних наукових та дослідницьких проектів, навчання та підвищення кваліфікації кадрів у цій сфері» [1].

Загалом, відповідно до Закону України «Про державно-приватне партнерство», співробітництво між державним та приватним партнерами уособлює собою державно-приватне партнерство, що здійснюється на договірній основі. До державного партнера відноситься держава, територіальні громади в особі державних органів та органів місцевого самоврядування, а

під приватним партнером розуміють юридичні особи, крім державних та комунальних підприємств, або фізичні особи – підприємці. Законодавцем зазначається, що у рамках державно-приватного партнерства можуть укладатися договори про концесію, спільну діяльність, управління майном, змішаний договір та інші договори.

Серед основних ознак механізму державно-приватного партнерства, що обумовлюють його ефективність при залученні приватного бізнесу, перед усім, є: надання прав управління (користування, експлуатації) об'єктом партнерства або придбання, створення (будівництво, реконструкція, модернізація) об'єкта державно-приватного партнерства з подальшим управлінням (користуванням, експлуатацією), за умови прийняття та виконання приватним партнером інвестиційних зобов'язань відповідно до договору, укладеного в рамках державно-приватного партнерства; фіксація у договірних відносинах «державного інтересу"; довгостроковість відносин (від 5 до 50 років); передача приватному партнеру частини ризиків у процесі здійснення державно-приватного партнерства; внесення приватним партнером інвестицій в об'єкти партнерства із джерел, не заборонених законодавством [2].

Зазначимо, що станом на 1 січня 2018 року на засадах державно-приватного партнерства було укладено 191 договір, що реалізується у наступних сферах господарської діяльності: оброблення відходів; збір, очищення та розподілення води; будівництво та/або експлуатація автострад, доріг, залізниць, злітно-посадкових смуг на аеродромах, мостів, шляхових естакад, тунелів і метрополітенів, морських і річкових портів та їх інфраструктури; виробництво, транспортування і постачання тепла; виробництво, розподілення та постачання електричної енергії; управління нерухомістю; пошук, розвідка родовищ корисних копалин та їх видобування та інші. На жаль, на сьогодні, зокрема інформаційно-комунікаційні технології та інформаційні ресурси, не є предметом зацікавленості зі сторони суб'єктів державно-приватного партнерства.

Разом з тим механізми, що пропонуються державно-приватним партнерством у ракурсі функціонування національної системи кібербезпеки, дадуть змогу створити відповідні умови для залучення підприємств та організацій всіх форм власності, що проводять діяльність у сфері електронних комунікацій та захисту інформації, а також є власниками або розпорядниками об'єктів критичної інфраструктури, до забезпечення кібербезпеки України. Фінансові та людські ресурси, об'єднані у межах державно-приватного партнерства, безумовно створять синергетичний ефект у розробці дієвих механізмів запобігання кіберзагрозам, реагування на кібератаки й кіберінциденти, та, у подальшому, усунення їх наслідків. Зазначимо, що визначений державою шлях функціонування національної системи кібербезпеки, а саме «формування конкурентного середовища у сфері еле-

ктронних комунікацій, надання послуг із захисту інформації та кіберзахисту» [1], на сьогоднішньому етапі найбільш ефективним буде саме за рахунок впровадження елементів державно-приватного партнерства.

На жаль, Доктриною інформаційної безпеки України не підіймається питання залучення державно-приватного партнерства до реалізації національних інтересів України в інформаційній сфері, хоча, на нашу думку, «розвиток та захист національної інформаційної інфраструктури», «розвиток інформаційного суспільства, зокрема його технологічної інфраструктури», «забезпечення розвитку інформаційно-комунікаційних технологій та інформаційних ресурсів України» [3], цілком є можливим у найближчий перспективі у тому числі завдяки державно-приватному партнерству.

**Література**

1. Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163 – VIII [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/2163-19.

2. Сутність державно-приватного партнерства [Електронний ресурс]. – Режим доступу: http://www.me.gov.ua/Documents/List?lang=uk-UA&id=311dfbfa -b31a-425f-8cff-428f450c7a0f&tag=SutnistDerzhavnoprivatnogoPartnerstva.

3. Указ Президента України № 47/2017 від 25 лютого 2017 року Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/47/2017.

4. Указ Президента України № 96/2016 від 15 березня 2016 року Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/96/2016.

*УДК 355*

**Марічев В.Є.**
кандидат юридичних наук,
доцент, професор
Національна академія СБ України

## ЗАБЕЗПЕЧЕННЯ СБ УКРАЇНИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СИСТЕМІ ТЕРИТОРІАЛЬНОЇ ОБОРОНИ УКРАЇНИ

Організація службової діяльності СБ України, її органів та підрозділів складається з напрямів відповідно до функціональних завдань, визначених чинним законодавством України [1, ст. 24].

Сучасні зміни у зовнішній та внутрішній політичній, військовій, соціальній та оперативній обстановці в Україні засвідчили, що найбільш акту-

альними загрозами для неї сьогодні є: збройна агресія з боку Російської Федерації; порушення російськими військами територіальної цілісності і державного суверенітету нашої країни; формування спецслужбами РФ злочинних озброєних формувань, нових військових з'єднань і частин на тимчасово окупованих територіях Донецької і Луганської областей; розгортання тактичної ядерної зброї в анексованій АР Крим; постачання сепаратистським силам на сході важкої бойової техніки, стрілецької зброї і засобів МТЗ; активізація спецслужбами РФ розвідувально-підривної діяльності проти України з метою дестабілізації соціально-політичної обстановки, створення умов для ліквідації України.

Саме тому сьогодні до основних завдань сектору безпеки і оборони України відносяться оборона від зовнішньої агресії, одним з елементів якої є територіальна оборона України (ТрО), становлення та розгортання якої було завершено лише на початку двадцять першого століття. Сьогодні вона набула настільки серйозних правових, методологічних, організаційних, технологічних і функціональних змін, що почала вимагати змістовного перегляду наукових поглядів на призначення, структуру, механізми функціонування і управління, забезпечення її органами та підрозділами СБ України [1, 2, 3].

ТрО відповідно до Тимчасової настанови з територіальної оборони України – це система загальнодержавних воєнних і спеціальних заходів, що здійснюються в особливий період на тилових територіях країни або в окремих місцевостях крім зон/районів ведення бойових дій [4, п. 2.1]. Її організаційні основи визначаються Положенням про територіальну оборону України, Тимчасовою настановою з територіальної оборони, Стратегією національної безпеки України, на основі яких формуються концептуальні засади її побудови, суб'єкти, їх компетенція, правове регулювання службової діяльності [4, п. 2; 5, р. 1].

До завдань СБУ як суб'єкту ТрО відносяться: проведення контррозвідувальних заходів з виявлення, розкриття і припинення будь-яких форм розвідувально-підривної діяльності проти України; забезпечення виконання інших завдань в інтересах ТрО за заявками Збройних Сил [5, п. 16].

Стратегія нацбезпеки України розкриває актуальні загрози і заходи у сфері інформаційної безпеки [6, п. 3.6], кібербезпеки і безпеки інформаційних ресурсів [135, п. 3.7], засвідчує застарілість системи охорони державної таємниці, інформації з обмеженим доступом [6, п.3.8]. З урахуванням зазначених загроз рівень обороноздатності нашої держави з точки зору державної безпеки України запропоновано зміцнити таким чином: реформувати СБУ шляхом створення динамічної, укомплектованої високопрофесійними фахівцями, забезпеченої сучасними матеріальними і технічними засобами спецслужби, здатної ефективно захищати державний су-

веренітет, конституційний лад і територіальну цілісність України з концентрацією зусиль на забезпеченням інформаційної безпеки шляхом:

- посилення наступальності заходів інформаційної безпеки на основі асиметричних дій проти всіх форм і проявів інформаційної агресії;
- створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них;
- протидії інформаційним операціям проти України, маніпуляціям суспільною свідомістю і поширенню спотвореної інформації;
- виявлення суб'єктів українського інформаційного простору, створених та/або використаних РФ для ведення інформаційної війни проти України, унеможливлення їхньої підривної діяльності [6, п. 4.11];
- створення системи забезпечення кібербезпеки, розвитку мережі реагування на комп'ютерні надзвичайні події (CERT);
- моніторингу кіберпростору з метою своєчасного виявлення, запобігання кіберзагрозам та їх нейтралізації, розвитком спроможностей правоохоронних органів щодо розслідування кіберзлочинів;
- забезпечення захищеності об'єктів критичної інфраструктури, державних інформаційних ресурсів від кібератак;
- створення системи підготовки кадрів у сфері кібербезпеки для потреб сектору безпеки і оборони [6, п. 4.12];
- реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом, захисту державних інформаційних ресурсів з урахуванням практики держав - членів НАТО та ЄС [6, п. 4.12];
- розвитку міжнародного співробітництва у сфері забезпечення кібербезпеки, інтенсифікацією співпраці України та НАТО для посилення спроможностей України у сфері кібербезпеки [6, п. 4.12].

Виходячи з викладеного автор вважає, що назріла необхідність із змістовного поглиблення чинної відомчої нормативно-правової бази СБУ для детального визначення мети, завдань і основ функціонування її органів та підрозділів у ТрО, насамперед щодо забезпечення інформаційної безпеки. Для цього на основі Інструкції про організацію в СБУ заходів з підготовки та ведення територіальної оборони розробити методичні рекомендації органам та підрозділам СБ України щодо організації виконання поставлених у цій сфері завдань.

**Література**

1. Закон України «Про Службу безпеки України.
2. Марічев В.Є. Погребицький М.Л. Трансформація поглядів на сучасну систему територіальної оборони України : наукова стаття. – Південноукраїнський правничий часопис. – Одеса, 2015. – № 2. – С. 151-161. – інв. 2250.
3. Матеріали оперативного навчання ГШ ЗС України з ТрО України 12.07.2015 року. – С. 123-140.

4. Тимчасова настанова з територіальної оборони: у 2-х ч. Ч. 1, затверджена наказом Генерального штабу Збройних Сил України від 1 березня 2017 року № 04.

5. Положення про територіальну оборону України, затверджене указом Президента України від 23 вересня 2016 року № 406/2016. – для службового користування.

6. Указ Президента України Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України».

*УДК 342.951*

**Мельник Д.С.**
кандидат юридичних наук
Національна академія СБ України

# ЩОДО АКТУАЛЬНИХ ПОТРЕБ ЗАХИСТУ НАЦІОНАЛЬНОЇ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

Переваги сучасного цифрового світу та розвиток інформаційних технологій зумовили виникнення нових загроз національній безпеці в інформаційній сфері. Сучасні інформаційно-комунікаційні технології можуть використовуватися для здійснення терористичних актів, зокрема шляхом порушення штатних режимів роботи автоматизованих систем керування технологічними процесами на об’єктах критичної інфраструктури. Дедалі частіше об’єктами кібератак та кіберзлочинів, кількість та потужність яких постійно зростає, стають інформаційні ресурси фінансових установ, підприємств транспорту та енергозабезпечення, державних органів, які гарантують безпеку, оборону, захист від надзвичайних ситуацій.

В умовах збройної агресії РФ та ведення нею гібридної війни проти нашої держави вказані загрози набувають принципово нового значення та мають тенденції до посилення їх негативного впливу на стан національної безпеки в різних її сферах. Україна стала полігоном для хакерських експериментів спецслужб РФ, численних диверсій та терактів проти об’єктів критичної інфраструктури та їх співробітників. Шкідливі вірусні програми («Black Energy», «WannaCry», «Petya», «Locky», «Bad Rabbit» тощо) спершу апробуються в Україні, а потім використовувалися вже у країнах Заходу.

Зокрема, протягом 2014-2017 років Україна зазнала безпрецедентної кількості диверсій та кібератак на об’єкти критичної інфраструктури – підприємства життєзабезпечення, енергетичної, транспортної сфери, державні фінансові установи тощо. Безпосереднього шкідливого впливу від деструктивних дій зазнали інформаційні системи та мережі на таких об’єктах.

Перша зареєстрована успішна кібератака на енергетичну систему України з виведенням її із ладу сталася 23.12.2015 р., коли російським хакерам із використанням троянської програми «BlackEnergy» вдалося успішно атакувати комп'ютерні системи управління низки енергопостачальних компаній. Найбільше від першої кібератаки постраждали споживачі «Прикарпаття-обленерго», оскільки було вимкнено близько 30 підстанцій, біля 230 тисяч мешканців залишались без світла протягом однієї-чотирьох годин. Наступна менш масштабна за наслідками, кібератака сталась вночі з 16 на 17.12.2016 року. На понад одну годину була виведена з ладу підстанція «Північна» енергокомпанії «Укренерго», без струму залишились споживачі північної частини правого берега м. Києва та прилеглих районів області.

У грудні 2016 року жертвами кібернападів з використанням модифікації вірусу «BlackEnergy» стали НБУ та низка державних банків разом з Мінфіном, Держказначейством та Пенсійним фондом України. Протягом травня – липня 2017 року комп'ютерні системи низки державних фінустанов та багатьох комерційних структур в Україні зазнали масованої атаки вірусу «WannaCry» та мережевого черв'яка «Petya», розробники яких вимагали значні суми коштів за відновлення доступу до інформації. У жовтні 2017 року комп'ютерні системи і мережі знову були атаковані з використанням вірусів «Locky» та «Bad Rabbit». Збитків зазнали «Київський метрополітен» та аеропорт «Одеса», а також інформресурси ДФС України та сайт держзакупівель «ProZorro».

Вказані загрози прискорили процеси формування національної системи кібербезпеки та зумовили прийняття в державі низки законодавчих та підзаконних нормативно-правових актів, насамперед Стратегії кібербезпеки України, затвердженої Указом Президента України від 15.03.2016 № 96/2016, та Закону України «Про основні засади забезпечення кібербезпеки України».

Відповідно до ст. 1 цього Закону, критичну інформаційну інфраструктуру утворює сукупність її об'єктів - комунікаційні або технологічні системи об'єктів критичної інфраструктури, кібератака на які безпосередньо вплине на їх стале функціонування. При цьому саме такі об'єкти є *об'єктами кіберзахисту*. Решта об'єктів критичної інфраструктури - підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей, відповідно до ст. 4 Закону є *об'єктами кібербезпеки*.

Відповідно до ст. 2 Закону та Порядку формування переліку інформаційно-телекомунікаційних систем (ІТС) об'єктів критичної інфраструктури держави[1], формування переліку здійснюється Адміністрацією ДССЗЗІ України на підставі отриманих від заінтересованих органів пропозицій, погоджених з СБУ. Перелік ІТС об'єктів критичної інфраструктури держави затверджується КМ України, а в банківській системі України - НБУ.

Включені до переліку ІТС об'єктів критичної інфраструктури, є *критичною інформаційною інфраструктурою держави*, що підлягає пріоритетному захисту від кібератак. Захист ІТС об'єктів критичної інфраструктури держави від кібератак покладається законодавством на власника (розпорядника) таких систем.

Національна система кібербезпеки - сукупність суб'єктів її забезпечення та взаємопов'язаних заходів захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури. Закон у ст. 5 визначає широкий перелік суб'єктів забезпечення кібербезпеки - Президент України, КМ України, РНБО України, яка через свій робочий орган Національний координаційний центр кібербезпеки здійснює координацію та контроль за діяльністю інших суб'єктів, а також низку державних та недержавних суб'єктів, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки. Відповідно до ст. 8 Закону та Стратегії кібербезпеки України, основу національної системи кібербезпеки становлять ДССЗЗІ, СБУ, НПУ, Міноборони та Генштаб ЗСУ, Нацбанк України, розвідувальні органи, на які покладені відповідні завдання.

У рамках реалізації Угоди між СБУ та Румунською службою інформації від 23.07.2015 в Україні створено Трастовий фонд «Україна – НАТО» з питань кібербезпеки, спрямований на надання Україні необхідної підтримки виключно для розвитку оборонних технічних можливостей (CSIRT), у т.ч. впровадження на об'єктах критичної інфраструктури передових технічних рішень та систем кібербезпеки, які забезпечуватимуть належний рівень безпеки, а також лабораторій для розслідування інцидентів у кібернетичній сфері.

Разом з тим, в умовах збройної агресії РФ та ведення нею гібридної війни проти нашої держави наявна в країні ситуація вимагає перегляду засад діяльності всієї системи забезпечення національної безпеки України, спрямованої на захист її критичної інформаційної інфраструктури.

Враховуючи викладене, для *удосконалення захисту національної критичної інформаційної інфраструктури* – необхідно вжити таких заходів:

---

[1] Порядок формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави, затверджений постановою КМ України від 23.08.2016 № 563. [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/563-2016-п.

1) *законодавчих* – остаточно унормувати визначення національної *критичної інфраструктури* та *системи її захисту* шляхом прийняття Стратегії захисту критичної інфраструктури України та Закону України «Про національну критичну інфраструктуру України»;

2) *організаційних* – створити ефективну *загальнодержавну систему захисту критичної інфраструктури України*, *координації та управління силами і засобами забезпечення її безпеки*. Виконанню цього завдання сприятиме реалізація положень Концепції створення державної системи захисту критичної інфраструктури та плану заходів з її реалізації, схваленої розпорядженням КМ України від 06.12.2017 №1009-р., а також Закону України «Про основні засади забезпечення кібербезпеки України» та Стратегії кібербезпеки України;

3) *режимних, розвідувальних, контррозвідувальних та оперативно-розшукових,* спрямованих на зниження рівня вразливості об'єктів критичної інформаційної інфраструктури.

Реалізація вказаних заходів в рамках загального процесу становлення національної системи захисту критичної інфраструктури сприятиме посиленню захисту її інформаційної складової відповідно до існуючих світових стандартів.

*УДК 004.056.53*

**Мельник С.В.**
кандидат технічних наук, доцент
Національна академія Служби безпеки України

## ФОРМУВАННЯ КУЛЬТУРИ КІБЕРБЕЗПЕКИ: ОСОБИСТІСНИЙ, КОРПОРАТИВНИЙ, ДЕРЖАВНИЙ ТА ГЛОБАЛЬНИЙ ВИМІР

Сучасні реалії створення та удосконалення систем кібернетичного захисту на рівні людини, організації, держави та міжнародної спільноти, що обумовлені особливостями кіберпростору як транснаціонального утворення з притаманними йому загрозами, охоплюють технічні, правові, організаційні, соціальні та етичні аспекти кіберзахисту. При цьому кіберзахист розглядається в контексті управління кіберінцидентами, що включають заходи попередження (у тому числі і з технічних, правових та етичних позицій управління мотивацією потенційних порушників), виявлення та реагування (у тому числі і з позиції управління наслідками кіберінцидентів).

Відповідно, зрозуміло, що ефективне забезпечення кібербезпеки можливе лише при системному вирішенні технічних, правових та соціальних складових проблеми протидії кіберзагрозам, а людина як і технічні засоби є об'єктом захисту. Потрібно також враховувати, що людина – це пересіч-

ний користувач мережі Інтернет, громадський діяч регіонального, національного чи світового рівня, або ж співробітник компанії, державної установи чи міжнародної організації. І в кожному випадку це різні наслідки від реалізації загроз кібербезпеки як для особи (громадянина), так і для її справи в індивідуальному та колективному вимірі. Звісно, у загальному випадку, основними зацікавленими сторонами у забезпеченні кібербезпеки особи є установа (корпорація), держава, громадськість і міжнародне товариство – структурні компоненти міжнародної системи кібербезпеки.

У цьому контексті актуалізується питання культури кібербезпеки в контексті її складових, принципів та заходів формування. Однак на сьогодні відсутнє чітке розуміння поняття культури кібербезпеки, і цей факт пояснюється широтою та різноманітністю складових цього типу та виду культури, наявною дискусією щодо співвідношення понять інформаційної та кібернетичної безпеки. Крім того, виходячи із ретроспективи діяльності із забезпечення інформаційної та кібернетичної безпеки найбільш поширеними дефініціями є корпоративна та глобальна культура кібербезпеки.

В загальному випадку, основними суб'єктами формування культури кібербезпеки є структури, що опікуються питаннями:

– захисту інформації з обмеженим доступом, безпеки бізнесу та національної безпеки – проблема корпоративної культури кібербезпеки;

– протидії кіберзлочинності, захисту права людини на недоторканість приватного життя, впровадження технологій електронної комерції та електронного урядування – проблема глобальної культури кібербезпеки.

Формування корпоративної культури у сфері кібербезпеки є одним із завдань управління інформаційною (кібернетичною) безпекою організації, регламенти якого встановлені багатьма відомчими, національними та міжнародними стандартами та полягають у визначенні компетенцій та контролів у виробничих та адміністративних процесах організації. Корпоративна культура кібербезпеки є частиною загальної корпоративної культури організації, яка спрямована на забезпечення безпеки бізнес-процесів та забезпечення конкурентоздатності організації. Так, Стів Мартіно, провідний фахівець компанії Cisco порівняв сутність поняття корпоративної культури кібербезпеки з огородженням магістралі, що не заважає руху (діяльності організації та її співробітників), а захищає тих, хто рухається цією магістраллю. Поняття корпоративної культури кібербезпеки стосується і державних установ, у тому числі, і правоохоронних органів в контексті забезпечення безпеки діяльності на всіх критичних ланках, пов'язаних з обігом службової та особистої інформації співробітників.

Формування глобальної культури кібербезпеки почалось з рекомендацій Організації економічної співпраці та розвитку (Organisation for Economic Cooperation and Development) 2002 року «Керівні принципи з безпеки інформаційних систем і мереж: На шляху до культури безпеки»,

які лягли в основу Резолюції Генеральної Асамблеї ООН «Створення глобальної культури кібербезпеки», прийнятої у 2003 році.

У 2012 році робочою групою Організації економічної співпраці та розвитку по безпеці і конфіденційності цифрової економіки (Working Party on Security and Privacy in the Digital Economy) була започаткована робота з перегляду Керівних Принципів та у 2015 році був прийнятий новий документ. У якості основних Принципів визначено: поінформованість, навички та розширення прав і можливостей; відповідальність; права людини і основні цінності.

Основними складовими культури кібербезпеки можна вважати правила, норми і стандарти безпечного використання комп'ютерних та мережевих технологій з метою попередження кіберінцидентів, що стосуються забезпечення конфіденційності, цілісності та доступності інформаційних ресурсів, а також інформаційно-психологічної безпеки у кіберпросторі. Водночас, до основних завдань заходів формування культури кібербезпеки, що підлягають оцінюванню, можна віднести доступність освітніх послуг з питань забезпечення кібербезпеки, доступність засобів та систем кіберзахисту, а також достатність профілактичних заходів із попередження кіберзлочинності на національному та міжнародному рівнях.

Більшість успішних інформаційно-просвітницьких та пропагандистських кампаній по формуванню корпоративної і глобальної культури кібербезпеки розвинутих країн світу реалізовані, перш за все, у сфері освіти із залученням ініціатив IT бізнесу. Загалом, національні та міжнародні ініціативи направлено, насамперед, на роботу з дітьми та студентами, громадськістю, персоналом приватних та державних установ шляхом надання освітніх послуг та розповсюдженням тематичних інформаційних матеріалів.

Звісно тематика формування корпоративної та глобальної культури кібербезпеки є актуальною і для України, потребує всебічного вивчення та наукового опрацювання з метою визначення та реалізації пріоритетних заходів у рамках стратегії кібербезпеки України. Державна політика у сфері кібербезпеки повинна бути спрямована на створення умов для ефективної співпраці приватного та державного сектору Національної системи кібербезпеки з урахуванням інтересів особи, бізнесу, суспільства, держави та міжнародної спільноти.

*УДК 343.983.25*
**Нізовцев Ю.Ю.**
заступник начальника відділу
комп'ютерно-технічних і телекомунікаційних експертиз
Центру судових і спеціальних експертиз Українського
науково-дослідного інституту спеціальної техніки
та судових експертиз Служби безпеки України

# ЩОДО ОКРЕМИХ ПРОБЛЕМ УНІФІКАЦІЇ ПОНЯТІЙНО-ТЕРМІНОЛОГІЧНОГО АПАРАТУ КІБЕРБЕЗПЕКИ

Будь-яка важлива для функціонування держави сфера життєдіяльності потребує ефективного регулювання та захисту з боку держави. Особливо це стосується безпеки інформаційного простору (кіберпростору) України, що знаходиться під дією негативних чинників, які впливають як на стан кібербезпеки держави в цілому, так і на кібербезпеку та кіберзахист її окремих об'єктів. Зазвичай протидія таким загрозам потребує злагодженої роботи багатьох державних інститутів, і, в свою чергу, ефективність цієї роботи значною мірою залежить від якості нормативної регламентації.

В Україні нормативно-правову основу функціонування інформаційно-телекомунікаційних систем, технічного захисту оброблюваної в них інформації та кримінальної відповідальності за несанкціоноване втручання в їх роботу становлять Конституція України, закони України, акти Президента України та Кабінету Міністрів України, нормативно-правові акти Служби безпеки України, Державної служби спеціального зв'язку та захисту інформації України, інших державних органів, міжнародні договори України, згода на обов'язковість яких надана Верховною Радою України. Саме цією нормативною базою керуються правоохоронні органи України під час протидії несанкціонованим втручанням в роботу інформаційно-телекомунікаційних систем. Для судових експертів особливу актуальність має закріплений у зазначених нормативно-правових актах понятійний апарат, який використовується під час проведення комп'ютерно-технічних та телекомунікаційних експертних досліджень ознак несанкціонованих втручань в роботу інформаційно-телекомунікаційних систем.

На думку автора, частина положень зазначених вище нормативних документів неузгоджені між собою. Це, зокрема, ускладнює судово-експертне дослідження як шкідливих програмних засобів, так і ознак несанкціонованих втручань в роботу інформаційно-телекомунікаційних систем, вчинених за допомогою зазначених програм.

Так, декілька ключових законодавчих актів, які мають безпосереднє відношення до захисту інформації та протидії кіберзлочинності, містять дещо різні терміни, під якими розуміються технічні засоби обробки та передачі інформації, а саме:

- електронно-обчислювальні машини (комп'ютери), автоматизовані системи, комп'ютерні мережі та мережі електрозв'язку (ст. 361 КК України [1]);
- інформаційна (автоматизована), телекомунікаційна та інформаційно-телекомунікаційна системи (Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [2]);
- технологічна та комунікаційна системи (Закон України «Про основні засади забезпечення кібербезпеки України» [3]).

Проаналізувавши зазначені терміни та їх визначення, автор дійшов висновку, що найбільш універсальним є термін «інформаційно-телекомунікаційні системи». Він охоплює усі, зазначені вище: інформаційні/автоматизовані та технологічні системи, електронно-обчислювальні машини (комп'ютери) та комп'ютерні мережі, мережі електрозв'язку, телекомунікаційні та комунікаційні системи. Враховуючи розглянуте вище розмаїття фактично рівнозначних понять, на думку автора, доцільним є перегляд та уніфікація чинного законодавства із застосуванням єдиного терміну «інформаційно-телекомунікаційні системи».

Наступна низка споріднених термінів, які потребують уніфікації, є наступні:
- несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361 КК України [1]);
- втручання у дані (ст. 4 Конвенції про кіберзлочинність [4]);
- втручання у систему (ст. 5 Конвенції про кіберзлочинність [4]);
- атака (НД ТЗІ 1.1-003-99 [5]);
- кібератака (ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» [3]).

Розглянувши та проаналізувавши визначення наведених термінів, автор вважає, що найбільш повним за змістом та точним терміном є «кібератака». Вбачається необхідним уніфікувати розглянуті вище терміни у різних нормативних актах, застосувавши найоптимальніший з них – «кібератака».

Також, на думку автора, слід уніфікувати терміни «виток» та «витік», що закріплені, відповідно, у Законі України «Про захист інформації в інформаційно-телекомунікаційних системах» [2] та ДСТУ 3396.2-97 [6].

Підсумовуючи вищевикладене, можна констатувати, що частина нормативних документів, які мають відношення до забезпечення кібербезпеки в Україні, мають неузгоджений понятійний апарат. Приведення у відповідність цього апарату дозволить уникнути неоднозначностей у тлумаченні тих чи інших термінів та спростить розуміння різних нормативних актів, що стосуються однієї спільної або кількох суміжних сфер регулювання.

**Література**

1. Кримінальний кодекс України : закон України від 05.04.2001 № 2341-III // База даних «Законодавство України» / Верховна Рада України. URL: http://zakon3.rada.gov.ua/laws/show/2341-14 (дата звернення: 28.02.2018).

2. Про захист інформації в інформаційно-телекомунікаційних системах : закон України від 05.07.1994 № 80/94-ВР // База даних «Законодавство України» / ВР України. URL: http://zakon2.rada.gov.ua/laws/show/80/94-вр (дата звернення: 28.02.2018).

3. Про основні засади забезпечення кібербезпеки України : закон України від 05.10.2017 № 2163-VIII // База даних «Законодавство України» / ВР України. URL: http://zakon2.rada.gov.ua/laws/main/2163-19 (дата звернення: 28.02.2018).

4. Конвенція про кіберзлочинність, ратифікована із застереженнями і заявами Законом України від 07.09.2005 № 2824-IV // База даних «Законодавство України» / ВР України. URL: http://zakon4.rada.gov.ua/laws/show/994_575 (дата звернення: 28.02.2018).

5. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28.04.1999 р. – № 22. – Київ, 1999. – 30 с.

6. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. – Київ, 1998 р. – 15 с.

*УДК 334.7*

**Ожеван М.А**.
д.ф.н., професор,
Заслужений діяч науки і техніки України
Національний інститут стратегічних
досліджень при Президентові України

## ПУБЛІЧНО-ПРИВАТНЕ ПАРТНЕРСТВО У КІБЕРБЕЗПЕКОВІЙ СФЕРІ ЯК МОДЕРНІЗАЦІЙНИЙ ВИКЛИК

Сутністю «публічно-приватного партнерства» (надалі - ППП) є співпраця органів державного управління й місцевого самоврядування («публічної сфери») з приватними організаціями у сфері надання публічних послуг або «суспільних благ». До числа цих «благ» можуть бути віднесені найрізноманітніші речі й послуги, які неможливо виключити зі споживання пересічного громадянина і які водночас не є в споживанні конкурентоспроможними, призначеними для персонального збагачення тощо.

Існує дві необхідні й достатні передумови адекватного розуміння «суспільного блага», які стосуються як постачальників, так і споживачів цих благ. По-перше, доброчесний постачальник не повинен правовим чи неправовим чином перешкоджати постачанню й використанню такого блага

іншими постачальниками. По-друге, споживання «суспільного блага» однією людиною не має виключати можливості й іншим людям споживати те ж саме благо. Тобто без будь-яких негативних наслідків для соціуму в цілому чимало людей можуть водночас споживати одне й те ж саме «суспільне благо».

У недемократичній державі «суспільні блага» (у колишньому СРСР – «фонди суспільного споживання») є благодіяннями держави та її диктатора, але не недержавних суб'єктів, що принципово унеможливлює ППП або ставить його в рамки штучних рестрикцій. Натомість, у демократичній державі «суспільні блага» є результатом спільної дії громадян. Одні й ті ж самі послуги можуть бути віднесені демократичним соціумом до публічної або приватної сфери, або ж до тієї й іншої водночас, залежно від волі й особистого вибору громадян.

Одним зі способів отримання «суспільних благ» є «публічні (державні) послуги», які жодним чином не можуть бути монополізовані державою. Тобто такі послуги держава може надавати як безпосередньо, так і опосередковано, звертаючись до приватних структур й фінансуючи від імені суспільства подібну діяльність з бюджетних засобів. Тут передусім важливо щоб надавці відповідних благ із публічного (державного) чи не публічного (недержавного) сектору не намагалися заробляти на них «додаткову ренту».

Варто виокремити наступні визначальні ознаки ППП:

- співпраця публічного (державного) сектору з сектором приватним;
- цивільно-правовий характер подібної співпраці;
- конкретна мета подібної співпраці: побудова інфраструктурних об'єктів, надання певних послуг, що традиційно виконувалося публічним (державним) сектором;
- оптимальний поділ завдань між обома секторами;
- поділ ризиків між обома секторами;
- взаємна користь [1].

З правової точки зору, виокремлюють наступні форми ППП :

1. Спільне підприємство (Joint Venture) - спільне використання ресурсів та поділ ризиків між урядом та приватним сектором включно з використанням спеціальних інструментальних засобів (Special Purpose Vehicle (SPV).

2. Сервісний договір (Service Contract): уряд наймає з метою надання певних послуг приватну компанію на певний період (зазвичай 1-3 роки).

3. Управлінський договір (Management Contract): «фундаментальні» видатки бере на себе уряд, приватна компанія забезпечує оборотний капітал для реалізації проекту.

4. Договір оренди (Lease contract) - приватний сектор бере на себе повністю реалізацію контракту терміном до 10-20 років включно з фінансуванням, експлуатацією, управлінням якістю та ризиками.

5. Концесії (Concessions) – концесіонер (приватна компанія) - підприємство повного обслуговування контракту включно з капітальними вкладеннями, експлуатацією, управлінням та обслуговуванням. Зазвичай діє схема: «побудова об'єкту – його експлуатація – передача його державі» (Build-Operate-Transfer (BOT), хоча можливі варіації. Сутність концесії гарно передає поняття британського права – «приватна фінансова ініціатива» (PFI – Private Finance Initiative) [2].

Дискусії довкола сутності ППП стосуються передусім можливості його ототожнення/розрізнення з «концесійною діяльністю» (концесіями). Тут зустрічаються дві крайніх позиції: ототожнення цих форм взаємодії державного (публічного) й приватного партнерів та їх строге розрізнення. Найоптимальнішим уявляється погляд, відповідно дол. якого ППП – більше широке поняття, а концесія – лише один з різновидів ППП, який стосується переважно реалізації інфраструктурних об'єктів за кошти приватного інвестора з наступною їх передачею державному (публічному) власнику. Водночас існує підхід, відповідно до якого ППП й концесії є нетотожними.

Четверта промислова революція поставила «руба» питання ППП в кібербезпековій сфері, оскільки число комп'ютерних інцидентів зростатиме, на думку фахівців, пропорційно числу пристроїв, підключених до різних «хмар», сховищ «великих даних» тощо. За оцінкою відомої компанії The Gartner, видатки на цілі кібербезпеки вже наприкінці 2020-х рр. складатимуть до третини всіх інвестицій «передових компаній» [3]. Враховуючи, що ППП істотно здешевлює ці видатки і що сама природа кіберпоростору побудована на засадах «мультистейкхолдеризму» («multistakeholderism»), як державні установи так і приватні компанії просто «приречені» на розвиток ППП. Разом з тим, сферу кібербезпеки важко відокремити від сфери кібервійн, яка поки що залишається доменом держави.

Наразі кібербезпека як і національна безпека в цілому є головно функцією держави, яка спрямовує зусилля на підтримання громадського порядку та захист національної безпеки (включно з кіберпростором). Наслідком такого стану справ є різні обмеження вільноринкових свобод. Відтак, конкуренція у безпекових сферах діяльності є досить незначною (за винятком участі компаній у державних закупівлях). Така тенденція досі була більшою мірою притаманна ЄС і меншою –США та «просунутим» країнам Азії.

Нині ситуація повільно, але впевнено міняється на користь ППП. Більше того, міжнародні ініціативи в сфері кібербезпеки виходять нині від приватного сектору навіть частіше й настирніше, аніж від держав. Йдеться зокрема про діяльність таких чотирьох організацій.

1. *Міжнародна організація із стандартизації* (International Organization for Standardization (ISO): розробила два стандарти в сфері кі-

бербезпеки (інформаційної безпеки): ISO 27001 (раніше - 2005,3) й ISO 270024. Приватні структури можуть добровільно перевірити своє обладнання на відповідність стандартам ISO/IEC [4].

2. *Форум з інформаційної безпеки* (The Information Security Forum's (ISF): пропонує бізнес-структурам «Стандарт гарної практики з інформаційної безпеки» (Standard of Good Practice for Information Security (SoGP або Standard).

Остання редакція Standard пропонує наразі рішення у таких предметних безпекових сферах як:

- Загроза шпигунства (Threat Intelligence);
- Захист від кібератак (Cyber Attack Protection);
- Промислові контрольні системи (Industrial Control Systems);
- Оцінка інформаційних ризиків (Information Risk Assessment);
- Архітектура безпеки (Security Architecture);
- Менеджмент підприємницької мобільності (Enterprise Mobility Management) [5].

3. *Модель запевнення зрілості програмного забезпечення* (The Software Assurance Maturity Model (SAMM) [6].

4. *Альянс хмарної безпеки (Cloud Security Alliance (CSA)*, у поле зору якого потрапляють безпека «Інтернету речей» та блокчейнових технологій [7].

З огляду на критично низький стан кібербезпекової складової вітчизняного сегменту кіберпростору, що навіть спонукало українську владу звернутися за підтримкою до американських партнерів, бажано якомога швидше провести його об'єктивне незалежне оцінювання на рівні як державних, так і недержавних інституцій під егідою недавно створеного Національного координаційного центру кібербезпеки при РНБО України й однієї з авторитетних міжнародних кібербезпекових організацій (імовірно, - європейського підрозділу Business Software Alliance (BSA) [8] за наступними критеріями:

- правові підстав функціонування даного фрагменту кіберпростору;
- організаційні інституції та механізми забезпечення кібербезпеки;
- стан державно-приватного (публічно-приватного) партнерства;
- секторальна кібербезпека;
- кібербезпекове просвітництво.

Пріоритетними завданнями ППП•у кібербезпековій сфері уявляються наступні:

- розвиток публічно-приватного діалогу у сфері підготовки законопроектів, покликаних посприяти створенню ефективних правил та процедур діяльності у сфері кібербезпеки;
- підписання відповідних угод у сфері цілей та завдань кібербезпеки через налагодження діалогу на теоретичному та практичному рівнях;
- просування українських рішень та продуктів у сфері кібербезпеки (стартапів) на національному та міжнародному рівнях;

•ефективна співпраця та державна підтримка у сфері кібербезпеки для приватних операторів компонентів інфраструктури критичних систем управління з використанням телеінформаційних систем і операторів та провайдерів телеінформаційних послуг;

•залучення представників державного, приватного та державного секторів, громадян до процесу безперервної освіти та підвищення рівня обізнаності щодо загроз в галузі кібербезпеки.

**Література**

1. Partnerstwo Publiczno-Prywatne (PPP) // Instytut Partnerstwa Publiczno-Prywatnego. [Електронний ресурс]. – Режим доступу: www.paih.gov.pl/files/?id_plik=16912.

2. Surya Kiran Sharma. Public-Private-Partnership in Cyber Security // Centre for Land Warfare Studies (CLAWS). [Електронний ресурс]. – Режим доступу: http://www.claws.in/1278/public-private-partnership-in-cyber-security-surya-kiran-sharma.html.

3. Special Report: Cybersecurity at the Speed of Digital Business - [Електронний ресурс]. – Режим доступу: https://www.gartner.com/doc/3426427?srcId=1-3132930191&cm_sp=gi-_-cysec-_-srpage.

4. ISO/IEC JTC 1 – об'єднаний технічний комітет Міжнародної організації із стандартизації (ISO) й міжнародної електротехнічної комісії (International Electrotechnical Commission (IEC). [Електронний ресурс]. – Режим доступу:https://en.wikipedia.org/wiki/ISO/IEC_JTC_1.

5. The ISF Standard of Good Practice for Information Security. [Електронний ресурс]. – Режим доступу: https://www.securityforum.org/tool/the-isf-standardrmation-security/.

6. Software Assurance Maturity Model. [Електронний ресурс]. – Режим доступу: http://www.opensamm.org/news/.

7. Cloud Security Alliance. [Електронний ресурс]. – Режим доступу: https://cloudsecurityalliance.org/.

8. BSA | The Software Alliance. [Електронний ресурс]. – Режим доступу: www.bsa.org/.

*УДК 342.951:351*

**Пальчик М.Л.**
кандидат юридичних наук
Національна академія СБ України

## ПРАВОВИЙ РЕЖИМ ІНФОРМАЦІЇ ПРО ОБ'ЄКТИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Масштабні та неочікувані комп'ютерні атаки на об'єкти критичної інфраструктури (далі – КІ), що відбулись тільки за минулий рік, вкотре актуалізували питання вироблення ефективних організаційних та право-

вих механізмів попередження загроз критичній інфраструктурі та її захисту в цілому. Окремим вектором діяльності при формуванні системи правових засобів захисту критичної інфраструктури, на наш погляд, є розроблення правових механізмів захисту інформації, пов'язаної з функціонуванням КІ. Захист інформації, у свою чергу, безпосередньо пов'язаний з правовим режимом вказаної інформації. Фактично, правовий режим є визначальним при виробленні необхідних заходів, що забезпечать цілісність та збереження інформації, належний порядок доступу до неї.

Варто зауважити, що правовий режим інформації визначається науковцями за порядком доступу до неї. При цьому, відповідно до статті 20 Закону України «Про інформацію» за порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом. Відповідно, будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом. Інформацією з обмеженим доступом відповідно до статті 21 Закону України «Про інформацію» та статті 6 Закону України «Про доступ до публічної інформації» є конфіденційна, таємна та службова інформація [1, 2].

Правовий режим інформації з обмеженим доступом, у свою чергу, полягає в тому, щоб охороняти відомості, вільний обіг яких може порушити права та інтереси держави, суспільства та окремої особи, забезпечити інформаційну незалежність суб'єктів приватного права у відносинах із державою і між собою, узгодити публічну потребу у свободі інформації та право кожного на збереження таємниці [3, с. 13].

Для визначення правового режиму, який може бути застосований до інформації про об'єкти критичної інфраструктури, стан їх захищеності, а також про заходи щодо забезпечення їх стійкого функціонування, варто звернутись до положень одного з основних нормативних документів, прийнятих Європейським співтовариством за визначеним напрямом, а саме Директиви 2008/114/ЄК.

Аналіз положень вказаного нормативного акту є актуальним ще й тому, що здійснення заходів з імплементації правових норм ЄС у сфері захисту критичної інфраструктури, зокрема Директиви 2008/114/ЄК, передбачено національними річними планами з реалізації Стратегії кібербезпеки України [4, 5].

Відповідно до положень Директиви інформація, що пов'язана з присвоєнням статусу «європейської критичної інфраструктури» конкретній інфраструктурі, має бути засекречена на належному рівні та відповідно до чинного законодавства Співтовариства та країн-членів ЄС. Під «європейською критичною інфраструктурою», відповідно до статті 2 Директиви 2008/114/ЄК, розуміється критична інфраструктура, розташована на території країн-членів ЄС, пошкодження чи знищення якої може спричинити значні наслідки щонайменше для двох країн-членів ЄС. У вказаній статті подано також визначення таємної інформації про захист критичної інфра-

структури, якою є відомості про критичну інфраструктуру, які у випадку їх розголошення можуть бути використані з метою планування чи здійснення дій, направлених на пошкодження чи знищення об'єктів критичної інфраструктури.

Крім того, Директива містить і положення щодо особливостей поводження з таємною інформацією про захист критичної інфраструктури. Зокрема статтею 9 закріплено обов'язковість перевірки осіб, які здійснюють обробку відповідної інформації та вказано недопустимість використання переданої країнами-членами ЄС та Європейської комісії інформації для інших цілей, ніж здійснення захисту критичної інфраструктури [6].

Таким чином, можемо підсумувати, що серед можливих правових режимів інформації, нормативно-правовими актами ЄС, зокрема Директивою 2008/114/ЄК, визначено, що саме інформація про захист критичної інфраструктури визначається таємною та потребує відповідного захисту. Наша держава, в свою чергу, взявши зобов'язання з імплементації положень вказаного нормативного акту, у тому числі щодо правового режиму інформації про захист критичної інфраструктури, має забезпечити їх реалізацію на внутрішньодержавному рівні та передбачити конкретні організаційно-правові механізми в національній правовій системі.

**Література**

1. Про інформацію : Закон України від 02.10.1992 № 2657-XII зі змінами [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/2657-12/print1443726670080170. (дата звернення 04.03.2018).

2. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI (зі зміна- ми) [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/2939-17/print1443726670080170 (дата звернення 04.03.2018).

3. Ясечко С. В. Цивільно-правова відповідальність за порушення права на інформацію : автореф. дис. ... канд. юрид. наук : спец. 12.00.03 «Цивільне право і цивільний процес; сімейне право; міжнародне приватне право» / С. В. Ясечко. – Х., 2011. – 21 с. (дата звернення 04.03.2018).

4. Про затвердження плану заходів на 2016 рік з реалізації Стратегії кібербезпеки України: Розпорядження Кабінету Міністрів України від 24 червня 2016 р. № 440-р [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/440-2016-%D1%80 (дата звернення 04.03.2018).

5. Про затвердження плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України: Розпорядження Кабінету Міністрів України від 10 березня 2017 р. № 155-р [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/155-2017-%D1%80 (дата звернення 04.03.2018).

6. Council Directive 2008/114/EC "On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection". – [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/ (дата звернення 04.03.2018).

*УДК 351.86 (477)*
**Панченко В.М.**
кандидат технічних наук,
старший науковий співробітник
Національна академія СБ України

# ЗАГРОЗИ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ В УМОВАХ ВПРОВАДЖЕННЯ BIG DATA-ТЕХНОЛОГІЙ

Одним із ключових пріоритетів політики національної безпеки України на найближчі роки залишається захист інформаційної сфери. Поряд із збереженням тенденції до реалізації вже відомих інформаційних загроз (поширення фейків, маніпулювання суспільною свідомістю через ЗМІ та соціальні медіа, залучення хакерів до реалізації політичних цілей, кібератаки на критичну інфраструктуру тощо), спецслужби іноземних держав, зокрема Російської Федерації, намагаються взяти на озброєння сучасні ІТ-рішення для отримання переваг у міждержавному протистоянні, оволодіваючи методами цілеспрямованого інформаційного впливу на користувачів мобільних послуг з використанням їх персональних даних та технологій обробки BigData на основі штучного інтелекту.

Аналіз наукових публікацій свідчить про відсутність досліджень, у яких розглядаються загрози національній безпеці України, обумовлені впровадженням BigData-технологій у різноманітні сфери життєдіяльності. Низка вітчизняних науковців вивчала переваги від застосування BigData-аналітики у бізнес-процесах, страховій сфері та правоохоронній діяльності [1, 2, 3, 4]. Серьогін В.О. досліджував загрозу «прайвесі» (недоторканості приватного життя) в умовах динамічного розвитку BigData [5].

Більш широко проблемні питання, пов’язані із застосуванням BigData-технологій представлено у публікаціях зарубіжних експертів:

– загрози «прайвесі», незаконна дискримінація (висунення підозр про здійснення терористичної діяльності, відмова у видачі кредитів тільки на підставі висновків BigData-алгоритмів), створення бірж приватних даних (торгівля персональними даними без відома їх власників), компрометація особи, маніпулювання особистістю та суспільною думкою через рекламу, стратифікація суспільства за ознакою доступу до інтернету, що призводить до збільшення розриву між багатими та бідними [6, 7];

– проблеми забезпечення інформаційної безпеки в умовах поширення BigData-технологій (використання хакерами BigData-технологій у злочинних цілях, багатогранність проблем цілісності та конфіденційності через необхідність об’єднання та співставлення даних з різних джерел та платформ, отримання доступу до інформації з обмеженим доступом та раніше невідомої інформації шляхом аналізу зв’язків між елементами загальнодоступних даних) [8];

– загрози національній безпеці (отримання даних про об'єкти критичної інфраструктури, здобування критично важливої інформації шляхом аналізу публічних даних) [9].

Метою даного дослідження є визначення актуальності для України загроз національній безпеці, обумовлених впровадженням BigData-технологій.

Якщо раніше компанії здійснювали управління майном, грошима, інтелектуальною власністю, то сьогодні з'явився новий актив – дані, які не лише використовуються для прийняття управлінських рішень, в інтересах отримання додаткового прибутку, зокрема шляхом таргетингової реклами, але і самі стали товаром [10].

Із розвитком інформатизації та технологій обробки великих масивів інформації, джерелами даних сьогодні стали смартфони, ноутбуки, квитанції супермаркетів, соціальні мережі, інтернет-покупки, банкомати, смарт-телевізори тощо, які надають деталізовану інформацію про погляди та поведінку їх власників. Тисячі елементів такої «інформаційної мозаїки» щоденно збираються в єдиний профіль користувача, «віртуальну» скриньку із пов'язаних між собою баз даних, який використовується без відома їх власника для отримання прибутку третіми особами.

Якщо раніше загроза порушення права особи на недоторканність приватного життя внаслідок використання BigData-технологій розглядалась виключно у контексті дотримання норм моралі та етики, сьогодні, як засвідчили результати останніх виборів Президента США, – це вже питання національної безпеки. Так, під час слухань комітету з розвідки американського сенату щодо ролі соціальних мереж при втручанні Росії у вибори 2016 року, Google, Facebook і Twitter визнали, що стали інструментом для маніпуляцій з боку спецслужб РФ [11].

Водночас, дані соціальних мереж, які використовуються BigData-алгоритмами, не такі точні, як дані з месенджерів мобільних телефонів, оскільки телефоном люди частіше говорять те, що думають та передають відомості про свої реальні дії, не усвідомлюючи цього. Як відомо, мобільні оператори, що функціонують на території України, розвивають власні месенджери (наприклад, Veon від «Київстар»), завдяки яким отримають необмежений доступ до персональних даних українських користувачів [12]. Зауважимо, що ці мобільні оператори на 97% належать російським власникам. Так, «Київстар» та «Лайф» через дочірні компанії з різних холдингів, через підставних осіб належать «Альфа-Груп», керівником та співвласником якої є російський бізнесмен М. Фрідман. «Vodafone» - бренд, який використовує російська телекомунікаційна компанія МТС [13].

І це в умовах жорстких вимог до захисту контенту мобільних абонентів російських операторів від іноземних дата-провайдерів при одночасному формуванні підконтрольної спецслужбам РФ інфраструктури для збе-

рігання та обробки великих масивів даних (створення дата-центрів, розробка технологій обробки даних тощо), а також легітимізації процедури передачі персональних даних з соціально-орієнтованих сервісів до силових відомств. Так, за даними компанії SAP, протягом останніх 10 років держструктури Росії вклали близько 23 млрд. руб. в сферу штучного інтелекту. Зазначені проекти переважно призначені для державного сектора, транспорту, оборони й безпеки, нафтової галузі та охорони здоров'я [14]. Прийнятий у 2015 році закон зобов'язує іноземні ІТ-компанії зберігати персональні дані росіян на серверах, що знаходяться в межах РФ [15]. У 2016 році прийнято т.зв. «пакет Ярової», який набуває чинності з 1 липня 2018 року та передбачає зобов'язання операторів зв'язку зберігати відомості про факти комунікації абонентів (аудіозаписи дзвінків, переписку, зображення, відео тощо). З метою виконання цих вимог, тільки "ВимпелКом" планує будівництво відразу п'яти дата-центрів із загальним обсягом інвестицій 30-40 млн. дол. [16]. Крім цього, у 2017 році Мінкомзв'язку РФ підготувало низку нормативних змін, відповідно до яких розповсюджувачі інформації, зареєстровані Роскомнаглядом, у тому числі месенджери та соцмережі, будуть зобов'язані передавати до правоохоронних органів такі дані як ідентифікатор користувача, дату і час реєстрації, ПІБ, псевдонім, дату народження, IP-адресу, адресу, номер телефону, паспортні дані, список родичів, надіслані повідомлення, файли, записи аудіо- та відеодзвінків, а також інформацію про здійснені ними електронні платежі [17]. Отже, РФ цілеспрямовано розвиває технології штучного інтелекту для обробки великих масивів даних та інфраструктуру для зберігання таких даних, зокрема персональних даних користувачів мобільних послуг. Покладаючи фінансування цих проектів на бізнес, влада зберігає над ними контроль через кадрові призначення, законодавчі обмеження або входження до складу співвласників компаній.

Таким чином, в умовах динамічного розвитку BigData-технологій російські спецслужби найближчим часом отримають доступ до даних українських користувачів мобільних послуг, а відтак - і нові засоби інформаційного впливу, які становлять цілком реальну загрозу національній безпеці України. Якщо раніше це були ЗМІ та соціальні медіа, сьогодні - це соціально-орієнтовані сервіси мобільних телефонів. Внаслідок антидержавної політики у сфері телекомунікацій та зв'язку протягом десятків років, Україна на сьогодні фактично втратила одну із складових суверенітету, і залишається надзвичайно вразливою до нових викликів в інформаційній сфері: розпорядниками персональних даних соціальних мереж є американські компанії, а даних мобільних сервісів – підконтрольні російській владі оператори зв'язку.

Питанням вирішення зазначеної проблеми будуть присвячені наступні публікації автора.

**Література**


1. Ерастов В.І. Використання Big Data у страховій діяльності / Василь Ігорович Ерастов // Финансовые услуги. – 2016. - №5 (119). – С. 11-13.
2. Впровадження інтернет-технологій у діяльність національної поліції України для отримання оперативно-розшукової інформації / С.В. Пеньков, В.В. Шендрик // Право і безпека. - 2017. - № 2 (65). – С. 80-85.
3. Актуальність використання моделі Big Data в бізнес-процесах / В.П. Мінакова, К.О. Шіковець // Математичні методи, моделі та інформаційні технології в економіці. – 2017. – № 10. – Сер.: Економіка і суспільство. – С. 892-896.
4. Самойленко Л. Б. Можливості та проблеми застосування технологій Big Data вітчизняними компаніями [Електронний ресурс] / Л. Б. Самойленко // Електронне наукове фахове видання «Ефективна економіка». – 2018. – №1. – Режим доступу: http://www.economy.nayka.com.ua/pdf/1_2018/59.pdf.
5. Серёгин В.А. «Big Data»: новая угроза для прайвеси в условиях информационного общества / В.А.Серегин // Науковий вісник Ужгородського національного університету. – 2015. – Випуск 35. – Ч. І. – Том 1. – Сер.: Право. – С. 93-97.
6. Security and Privacy Issues of Big Data [Електронний ресурс] / Jose Moura, Carlos Serrao // Режим доступу: https://arxiv.org/ftp/arxiv/papers/1601/1601.06206.pdf.
7. Stanley J. Eight Problems With “Big Data” [Електронний ресурс] / Jay Stanley // Режим доступу: https://www.aclu.org/blog/privacy-technology/eight-problems-big-data.
8. Фактор информационной безопасности в процессе эволюции гетерофазных мультиагентных когнитивных систем [Електронний ресурс] / А.У. Заммоев, Ю.Х. Хамуков, Л.З. Шауцукова // Режим доступу: https://www.science-education.ru/ru/article/view?id=16000.
9. Harris Sh. Irony Alert: Pentagon Now Sees Big Data as ‘National Security Threat’ [Електронний ресурс] / Shane Harris // Foreign Policy. - Режим доступу: http://foreignpolicy.com/2013/08/12/irony-alert-pentagon-now-sees-big-data-as-national-security-threat/.
10. Fuel of the future: Data is giving rise to a new economy [Електронний ресурс] // Режим доступу: http://www.economist.com/news/briefing/21721634-how-itshaping-up-data-giving-rise-new-economy.
11. «Троянський кінь» Кремля: соцмережі визнали, що їх використали для маніпуляцій у США [Електронний ресурс] / Остап Яриш, Наталія Гуменюк // Режим доступу: https://hromadske.ua/posts/rosiya-cherez-socmerezhi-manipulyue-amerikancyami.
12. Владелец «Киевстар» запускает в Украине мессенджер с бесплатными сообщениями, звонками и новостями [Електронний ресурс] / Павел Красномовец // Режим доступу: https://ain.ua/2017/07/19/veon-kyivstar-prilozheniye.
13. Мобильные операторы Украины или кого могут слушать спецслужбы РФ [Електронний ресурс] / Дмитрий Мацкевич // Режим доступу: https://stopterror.in.ua/info/2017/06/mobilnye-operatory-ukrainy-ili-kogo-mogut-slushat-spetssluzhby-rf/.

14. Путин назвал условия появления будущего властелина мира / Евгений Калюков [Електронний ресурс] // РБК. - Режим доступу: https://www.rbc.ru/technology_and_media/01/09/2017/59a947189a79470f49873a14.

15. Федеральный закон от 27 июля 2006 г. N 152-ФЗ О персональных данных [Електронний ресурс] // Российская газета - Федеральный выпуск №4131 (0). - Режим доступу: https://rg.ru/2006/07/29/personaljnye-dannye-dok.html.

16. «Вымпелком» запланировал строительство сразу пяти дата-центров [Електронний ресурс] / Кирилл Седов // Режим доступу: https://www.vedomosti.ru/technology/articles/2017/05/15/689789-vimpelkom-stroitelstvo.

17. Минкомсвязи подготовило список данных пользователей для передачи ФСБ [Електронний ресурс] / Наталья Селиверстова // Режим доступу: https://ria.ru/society/20170811/1500232246.html?inj=1.

*УДК 343.543*

**Петров В. В.**
кандидат політичних наук, доцент СК-31
Національна академія СБ України,
керівник служби з питань інформаційної безпеки
Апарату РНБО України

## ЩОДО УДОСКОНАЛЕННЯ ВІТЧИЗНЯНОГО ЗАКОНОДАВСТВА У СФЕРІ КІБЕРБЕЗПЕКИ

Враховуючи важливість формування повноцінної законодавчої бази для забезпечення функціонування національної системи кібербезпеки Радою національної безпеки і оборони України було прийнято низку важливих рішень.

Так, рішенням РНБО України від 28.04.2014 «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» (Указ Президента України від 01.05.2014 №449) визначено підготувати та подати в установленому порядку проект Стратегії кібернетичної безпеки України та проект Закону України про кібернетичну безпеку України. Рішенням РНБО від 27.01.2016 «Про Стратегію кібербезпеки України» (Указом Президента України від 15.03.2016 № 96) вказана Стратегія була затверджена.

Крім того, рішенням РНБО України від 29.12.2016 «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації» (Указ Президента України від 13.02.2017 № 32) передбачено внесення у встановленому порядку на розгляд Верховної Ради України законодавчих пропозицій щодо:

- імплементації окремих норм Конвенції про кіберзлочинність;

- визначення вимог щодо кіберзахисту об'єктів критичної інформаційної інфраструктури, прав і обов'язків основних суб'єктів забезпечення кібербезпеки та власників (розпорядників) об'єктів критичної інформаційної інфраструктури, механізму взаємодії між ними під час виявлення, попередження, припинення кібератак та кіберінцидентів, усунення їх наслідків, запровадження відповідальності за порушення відповідних об'єктів;

- посилення відповідальності за невиконання вимог законодавства стосовно захисту інформації в інформаційно-телекомунікаційних системах та законних вимог посадових осіб органів Державної служби спеціального зв'язку та захисту інформації України, а також щодо запровадження відповідальності за невиконання законних вимог посадових осіб Служби безпеки України;

- за участю Служби безпеки України підготувати законодавчі пропозиції щодо визначення обмежувальних заходів стосовно використання на об'єктах критичної інфраструктури програмного забезпечення та телекомунікаційного обладнання, розробленого/ виготовленого суб'єктами господарювання держави-агресора;

У відповідності до рішення РНБО України від 29.12.2016 «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», введеного в дію Указом Президента України від 13.02.2017 № 32» (Указ Президента України від 30.08.2017 №254) Кабінету Міністрів України доручено підготувати і внести в установленому порядку законопроекти щодо:

- встановлення обов'язкового погодження з Державною службою спеціального зв'язку та захисту інформації України проектів (завдань) Національної програми інформатизації;

- розмежування кримінальної відповідальності за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, вчинені щодо державних та інших інформаційних ресурсів, щодо об'єктів критичної інформаційної інфраструктури та інших об'єктів, а також відповідного розмежування підслідності;

- непоширення дії мораторію на здійснення заходів державного нагляду (контролю) суб'єктів господарювання незалежно від форми власності у сфері криптографічного та технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом.

Розроблений за участі основних суб'єктів забезпечення кібербезпеки, а також міжнародних експертів та партнерів, проект Закону України «Про основні засади забезпечення кібербезпеки України» 05.10.2017 прийнятий Верховною Радою України та набуде чинності впродовж півроку від дати опублікування.

Службою безпеки України на виконання зазначених вище рішень РНБО України опрацьовано питання щодо врегулювання на законодавчому рівні запровадження процедури блокування (обмеження) операторами та провайдерами телекомунікацій доступу до визначеного (ідентифікованого) інформаційного ресурсу (інформаційного сервісу) на підставі рішення суду.

За результатом роботи до якої залучались фахівці СБ України, Держспецзв'язку, інших суб'єктів забезпечення кібербезпеки розроблено проект Закону України «Про внесення змін до деяких законодавчих актів України щодо протидії загрозам національній безпеці в інформаційній сфері», який перебуває на розгляді у Верховній Раді України ( реєстр. № 6688 від 12.07.2017).

Також фахівцями Служби безпеки України на виконання рішення РНБО України від 10.07.2017 (Указ Президента України від 30.08.2017 № 254, підготовлено законодавчі пропозиції щодо розмежування кримінальної відповідальності за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, вчинені щодо державних та інших інформаційних ресурсів, щодо об'єктів критичної інформаційної інфраструктури та інших об'єктів, а також відповідного розмежування підслідності.

*УДК 640.4.012.8*

**Полотай О.І.**
кандидат технічних наук, доцент
Львівський державний університет безпеки життєдіяльності
**Полотай Б.Я.**
старший викладач
Львівський торговельно-економічний університет

## АНАЛІЗ ПОРУШНИКІВ ТА ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОБ'ЄКТІВ ГОТЕЛЬНО-РЕСТОРАННОГО ГОСПОДАРСТВА

Готельно-ресторанне господарство – це особлива самостійна галузь економіки, що складається з групи галузей і підприємств, функції яких полягають у задоволенні різноманітного попиту на різні види відпочинку і розваг.

Готельно-ресторанне господарство складається з готелів, ресторанів та організацій, які випускають товари і надають послуги, що тісно пов'язані з готельно-ресторанним бізнесом: транспортні підприємства; навчальні заклади готельно-господарського профілю; інформаційні та рек-

ламні служби; науково-дослідні та проектні організації готельно-ресторанного профілю, тощо.

Для будь-якого готелю чи ресторану безпека клієнтів є найважливішим аспектом його діяльності, яку повинні гарантувати, як ресторатори, так і готельєри.

Одним із актуальних питань безпеки об'єкту готельно-ресторанного господарства є інформаційна безпека готелю, який в своєму складі обов'язково має ресторан, оскільки будь-яка цілеспрямована й недружня акція проти інтересів підприємства починається зі збору інформації. У зв'язку з погіршенням таких складових інформаційних ресурсів, як конфіденційність, цілісність, доступність і достовірність, спостерігаються збої у функціонуванні систем управління, розголошуються відомості, що становлять комерційну таємницю, порушується достовірність фінансової документації [2, с. 126].

Проаналізувавши усі загрози інформаційної безпеки готельно-ресторанного господарства, можна їх згрупувати в такі основні групи (табл. 1).

Таблиця 1

Загрози інформаційної безпеки
готельно-ресторанного господарства

| Загроза | Опис |
|---|---|
| Програмні | Комп'ютерні віруси, програми закладки, фішинг, кіберсвотинг, логічні бомби. |
| Технічні | Загрози, що пов'язані з використанням технічних каналів витоку інформації з обмеженим доступом, як слабких місць об'єктів готельно-ресторанного господарства. Серед таких каналів можуть бути канали витоку акустичної, видової, електронної та електромагнітної інформації. Зняття інформації з перерахованих каналів відбувається за допомогою засобів технічної розвідки (стетоскопи, жучки, спрямовані та лазерні мікрофони, тощо). |
| Фізичні | Безпосереднє знищення важливих даних та інформації, які зберігаються як в електронному так і в паперовому форматі. |
| Режимні | Так звані організаційні загрози, які виникають внаслідок недосконало розроблених або недотриманих правил поведінки на об'єкті готельно-ресторанного господарства, режиму доступу до секретного об'єкту чи інформації з обмеженим доступом, несанкціонованого доступу до конфіденційної інформації. |
| Людський фактор | Підкуп або введення в оману осіб, що мають відповідний допуск для доступу до інформації, необережне поводження з інформацією, навмисні чи ненавмисні помилки техперсоналу. |

До основних типів зловмисників, які виступають порушниками інформаційної безпеки готельно-ресторанного господарства, можна віднести категорію внутрішніх та зовнішніх порушників (табл. 2).

Таблиця 2

Порушники інформаційної безпеки на об’єктах готельно-ресторанного господарства

| Тип порушника | Характеристика |
|---|---|
| Внутрішні | |
| Робочий персонал | Навмисні чи ненавмисні дії працівників, які призводять до втрати інформації з обмеженим доступом. |
| Обслуговуючий персонал | Технічні працівники, які мають доступ до певних приміщень. |
| Адміністрація | Працівники, які мають найвищий рівень доступу до інформації з обмеженим доступом. |
| Зовнішні | |
| Клієнти | Споживачами послуг об’єктів готельно-ресторанного господарства можуть бути замасковані зловмисники з прихованими засобами технічної розвідки для незаконного заволодіння інформацією з обмеженим доступом. |
| Мережеві хакери | Комп’ютерні злочинці, які за допомогою мережевих ресурсів можуть здійснити дистанційний несанкціонований доступ до мережі чи бази даних об’єкту готельно-ресторанного господарства і таким чином незаконно заволодіти інформацією з обмеженим доступом. |
| Зовнішній обслуговуючий персонал | Під видом працівників підприємств, які надають певні послуги, наприклад встановлення кондиціонерів, жалюзей, доставка піци тощо, можуть бути завербовані спецслужбами зловмисники, які можуть встановити жучок, для несанкціонованого зняття інформації з обмеженим доступом. |
| Колишні працівники | Працівники, яких на їхню думку безпідставно звільнили, можуть помститись керівництву та заподіяти шкоди. |
| Конкуренти | Недобросовісні працівники фірм-конкурентів можуть намагатись заволодіти інформацією з обмеженим доступом, з метою отримання, наприклад, фінансової інформації. |

Отже, готельно-ресторанне господарство є однією з найбільш бажаних галузей для злочинців і для забезпечення інформаційної безпеки на необхідно:

– аналізувати оцінку появи та створювати перелік можливих загроз;
– розробляти методики оцінки інформаційних ризиків;
– проводити інформаційні обстеження ресурсів підприємства;
–розробляти політику та концепції інформаційної безпеки [1, с. 120].

**Література**

1. Гоблик-Маркович Н.М. Інформаційна безпека в готельно-ресторанному господарстві / Н.М. Гоблик-Маркович, Д.І. Молнар, Т.І. Ільтьо // Економіка та управління національним господарством. – 2017. № 8. – С. 116-120.

2. Іванченко Н.О. Інформаційна складова економічної безпеки підприємства та її значення для забезпечення стійкого розвитку національної економіки /Н.О. Іванченко // Стратегія розвитку України. – 2011. – № 3. – С. 124–128.

*УДК 351*

**Прощаєв В.В.**
доцент спеціальної кафедри,
кандидат юридичних наук, доцент
Інститут СЗР України

## ІНФОРМАЦІЙНА БЕЗПЕКА У ДІЯЛЬНОСТІ ЗОВНІШНЬОЇ РОЗВІДКИ ЗА ЗАКОНОДАВСТВОМ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ

Серед колишніх пострадянських країн питання інформаційної безпеки у функціонуванні зовнішньої розвідки найбільш повно і детально визначено у законодавстві Російської Федерації (РФ). Це цілком зрозуміло, бо керівництво РФ ставить перед зовнішньою розвідкою завдання добування розвідувальної інформації за глобальним принципом, витрачає на її діяльність величезні бюджетні кошти, в інформаційних базах центральних органах розвідки концентруються дуже важливі відомості та інформація, що становлять державну таємницю найвищого рівня.

Крім загальних федеральних законів «Про державну таємницю», «Про безпеку», «Про забезпечення доступу до інформації про діяльність державних органів та органів місцевого самоврядування», в яких правовими нормами визначаються загальні питання збереження та поводження з таємною інформацією, російський законодавець вважав за необхідне саме у Федеральному Законі від 10 січня 1996 року «Про зовнішню розвідку» детально визначити правовими приписами інформаційну безпеку у діяльності зовнішньої розвідки.

Для цього законодавець надав зовнішній розвідці такі спеціальні повноваження:

здійснення заходів щодо зашифровування кадрового складу та організації його діяльності із застосуванням іншої відомчої належності;

використання документів прикриття, що зашифровують особистість співробітників кадрового складу, відомчу належність підрозділів, організацій, приміщень та транспортних засобів до органів зовнішньої розвідки;

створення організаційних структур прикриття (підрозділів і організацій), необхідних для функціонування органів зовнішньої розвідки;

розроблення, створення та експлуатація інформаційних систем, систем зв'язку і передачі даних, а також засобів захисту інформації від її витоку по технічних каналах.

У Законі окремими правовими приписами визначається захист відомостей про органи зовнішньої розвідки, а саме:

особа, що допускається до відомостей про органи зовнішньої розвідки, обов'язково проходить процедуру оформлення допуску до державної таємниці;

документи архівів органів зовнішньої розвідки передаються на постійне збереження до Державної архівної служби РФ лише після їх розсекречування відповідно до федерального закону;

документи органів зовнішньої розвідки, що містять відомості про їх кадровий склад, про осіб, що сприяють (сприяли) на конфіденційній основі органам розвідки, а також про методи і засоби діяльності зберігаються виключно в архівах органів зовнішньої розвідки.

В окремій статті Закону визначається порядок опублікування матеріалів про зовнішню розвідку засобами масової інформації. Перед опублікуванням таких матеріалів автори або редакції ЗМІ звертаються за експертним висновком до відповідного органу зовнішньої розвідки. У разі опублікування матеріалів про розвідку, у яких містяться відомості про державну таємницю, без попереднього отримання експертного висновку, а також якщо наслідком опублікування стало нанесення матеріальної або моральної шкоди співробітникам розвідки, настає відповідальність відповідно до чинного законодавства.

Дуже цікавим є припис стосовно порядку використання негласних методів та засобів розвідувальної діяльності, який передбачає надання органам розвідки права на розробку та видання спеціальних відомчих нормативно-правових актів про визначення цього порядку, зміст яких становить державну таємницю.

Для забезпечення інформаційної безпеки суттєве значення має правовий припис в Законі про фінансування та матеріально-технічне забезпечення органів зовнішньої розвідки. Згідно із приписом проекти кошторисів витрат на утримання органів розвідки розглядаються виключно на за-

критих засіданнях відповідних комітетів (підкомітетів) палат Федерального Зібрання та затверджується на закритих засіданнях Державної Думи та Ради Федерації.

У Законі є бланкетна правова норма, яка передбачає відповідальність керівників та інших посадових осіб органів законодавчої, виконавчої і судової влади, підприємств, установ та організацій, членів Ради Федерації і депутатів Державної Думи, яким надається розвідувальна інформація, у випадках її розголошення.

В окремій главі Закону детально визначено умови для прийняття громадян РФ на службу або роботу у зовнішній розвідці. Комплекс умов, аж до обов'язкової державної дактилоскопічної реєстрації, значно підвищує ефективність інформаційної безпеки у діяльності зовнішньої розвідки. Подібні умови визначено також стосовно осіб, що сприяють на конфіденційній основі розвідувальним органам. Відомості про цих осіб становлять державну таємницю та розсекречуванню за будь-яких обставин не підлягають. Доступ до них мають лише керівники та уповноважені ними співробітники відповідного розвідувального органу. Також відомості про осіб-конфідентів не входять до предмету прокурорського нагляду.

Розміщення інформації про діяльність розвідки в Інтернет-ресурсах регулюється окремим Указом Президента РФ від 10 серпня 2011 р. № 1074 «Про затвердження переліку інформації про діяльність Служби зовнішньої розвідки Російської Федерації, яка розміщується у мережі Інтернет».

*Висновок:* правове регулювання інформаційної безпеки на рівні законів та указів свідчить про її високий рівень, що у свою чергу створює надійний комплекс правових умов для функціонування російських органів зовнішньої розвідки.

*УДК 341.824*

**Рижиков В.С.**
доктор педагогічних наук, професор,
старший науковий співробітник
Науково-дослідного центру
Військового інституту Київського
національного університету імені Тараса Шевченка

## КЛАСИФІКАЦІЯ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ, ЖИТТЄВО ВАЖЛИВІ ФАКТОРИ ДЕРЖАВИ В ІНФОРМАЦІЙНІЙ СФЕРІ

Інформаційна безпека є однією із суттєвих складових частин національної безпеки країни, її забезпечення завдяки послідовній реалізації грамотно сформульованої національної інформаційної стратегії в значній мірі сприяла б забезпеченню досягнення успіху при вирішенні задач у полі-

тичній, військово-політичній, військовій, соціальній, економічній та інших сферах державної діяльності. Так, проведення в життя вдалої інформаційної політики може суттєво вплинути на розв'язання внутрьошньополітичних, зовнішньополітичних та військових конфліктів.

Інтереси держави в інформаційній сфері полягають у створенні умов:

– для гармонійного розвитку державної інформаційної інфраструктури;

– для реалізації конституційних прав і свобод людини та громадянина в галузі одержання інформації та користування нею з метою забезпечення непорушності конституційного ладу, суверенітету та територіальної цілісності держави, політичної, економічної та соціальної стабільності, у безумовному забезпеченні законності та правопорядку, розвитку рівноправного та взаємовигідного міжнародного співробітництва [1, с. 47-48].

Загрози інформаційній безпеці [information security threat] – сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства і держави в інформаційній сфері. Основні загрози інформаційній безпеці можна розділити на три групи:

– загрози впливу неякісної інформації (недостовірної, фальшивої, дезінформації) на особистість, суспільство, державу;

– загрози несанкціонованого і неправомірного впливу сторонніх осіб на інформацію і інформаційні ресурси (на виробництво інформації, інформаційні ресурси, на системи їхнього формування і використання);

– загрози інформаційним правам і свободам особистості (праву на виробництво, розповсюдження, пошук, одержання, передавання і використання інформації; праву на інтелектуальну власність на інформацію і речову власність на документовану інформацію; праву на особисту таємницю; праву на захист честі і достоїнства та ін.).

Фактори загроз за видовою ознакою поділяються на політичні, економічні та організаційно-технічні [2, с. 15].

Під політичними факторами загроз інформаційній безпеці розуміють:

– зміни геополітичної обстановки внаслідок фундаментальних змін у різноманітних регіонах світу, зведення до мінімуму ймовірності світової ядерної війни;

– інформаційна експансія розвинених країн, які здійснюють глобальний моніторинг світових політичних, економічних, воєнних, екологічних та інших процесів, та розповсюджують інформацію з метою здобуття односторонніх переваг;

– становлення нової державності в пострадянських країнах на основі принципів демократії, законності, інформаційної відкритості;

– низька загальноправова та інформаційна культура сторін.

Основними економічними факторами загроз безпеці інформації є:

– перехід на ринкові відносини в економіці, поява на ринку великої кількості вітчизняних та зарубіжних комерційних структур – виробників та споживачів інформації, засобів інформатизації та захисту інформації, включення інформаційної продукції в систему товарних відносин;

– критичний стан вітчизняних галузей промисловості, яка виробляє засоби інформатизації та захисту інформації;

– розширення кооперації із зарубіжними країнами в розвитку інформаційної інфраструктури.

Основними організаційно-технічними факторами загроз інформаційній безпеці є:

– недостатня нормативно-правова база у сфері інформаційних відносин, у тому числі в галузі забезпечення інформаційної безпеки;

– недостатнє регулювання державою процесів функціонування та розвитку ринку засобів інформатизації, інформаційних продуктів та послуг;

– широке використання у сфері державного управління та кредитно-фінансової сфери незахищених від витоку інформації імпортних технічних та програмних засобів для зберігання, обробки та передавання інформації;

– зростання обсягів інформації, яка передається відкритими каналами зв'язку;

– загострення криміногенної обстановки, зростання числа комп'ютерних злочинів, особливо в кредитно-фінансовій сфері [3, с. 16-17].

Інтереси держави в інформаційній сфері в основному зводяться до гармонійного розвитку інформаційної структури держави. Інформаційна безпека держави – це стан її захищеності, при якій спеціальні інформаційні операції, акти зовнішньої інформаційної агресії, інформаційний тероризм, незаконне зняття інформації за допомогою спеціальних технічних засобів, комп'ютерні злочини та інший деструктивний інформаційний вплив не завдає істотної шкоди національним інтересам.

**Література**

1. Бондарь И. Проблемы информационной безопасности в условиях переходного общества // Персонал. – 2003. – № 8. – С. 47-48.

2. Катренко А. Особливостіінформаційноїбезпеки за міжнародними стандартами // Альманах економічноїбезпеки. – 1999. – № 2. – С. 15-17.

3. Система забезпеченняінформаційноїбезпекиУкраїни // Національнабезпека і оборона. – 2001. – № 1. – С. 16-28.

*УДК 004.424.6:004.6 (045)*

**Савченко Д. С.**
Національна академія СБ України

## ДО ПРОБЛЕМ АВТОМАТИЗОВАНОГО ПОШУКУ В НЕСТРУКТУРОВАНИХ ТЕКСТАХ В КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Виклики, що постали перед Україною на сьогодні в інформаційній сфері, вимагають автоматизованої обробки величезних масивів інформації

з мережі Інтернет – як потокової, так і текстової. В першу чергу на сьогодні існує потреба у більш досконалих методиках автоматизованої обробки неструктурованих текстів, що дозволяють ефективно працювати з неструктурованими даними значних обсягів. Особливістю таких текстів, що викладені природною мовою людини, крім використання специфічної лексики, є також наявність у них випадкових помилок, в першу чергу тих, що пов'язані із неправильним написанням окремих слів. Внаслідок цієї обставини сучасні системи з автоматизованої обробки таких текстів повинні бути здатними враховувати можливу наявність будь-яких випадкових помилок, особливо при виконанні завдань з пошуку, як першої стадії перед подальшим аналізом. Як зрозуміло, наявні методи точного пошуку, що виявляють збіг певних фрагментів тексту з пошуковою послідовністю, за цих обставин працюватимуть неефективно.

З огляду на зазначене, задача виявлення та виправлення помилок у неструктурованих текстах традиційно вирішується через оцінювання схожості (або розбіжності) між кожним словом тексту, та записами у словнику автоматизованої системи. При цьому в першу чергу інтерес становлять такі методи оцінювання схожості слів, що були б максимально наближеними до рішень, одержаних за допомогою людей-експертів.

Однією з проблем подібних методів пошуку є кількісна оцінка схожості різних текстових одиниць між собою. Для забезпечення такої кількісної оцінки схожості слів з дотриманням зазначеного принципу можна використовувати метод аналізу співпадіння символів і біграм (комбінацій з 2-х сусідніх символів), з яких вони складаються, на основі коефіцієнту схожості Серенсена.

Сутність такого методу полягає у наступному.

Розглянемо слова $X$ та $Y$ довжиною відповідно $n$ та $m$ символів. Вважатимемо умовно, що перед і після кожного із цих слів знаходяться пусті символи. Розкладемо слова $X$ та $Y$ на біграми, починаючи з їх перших пустих символів і закінчуючи їх останніми пустими символами. Тоді слово $X$ утворить $n+1$ таких біграм, а слово $Y$ утворить $m+1$ біграм. Розкладемо додатково слова $X$ та $Y$ на окремі символи. Позначимо всі символи і біграми в слові $X$, які присутні також у слові $Y$. Підрахуємо вагу позначених символів і біграм: кожний символ та біграму з пустим символом зарахуємо як 2 умовні одиниці ваги, а кожну біграму із двох символів – як 1 одиницю ваги.

Тоді кількісну оцінку схожості $\sigma_{XY}$ слів $X$ та $Y$ можна визначити за наступною формулою на основі коефіцієнту схожості Серенсена:

$$\sigma_{XY} = \frac{2W}{3(n+m+2)}, \qquad (1)$$

де: $n$ – кількість символів у слові $X$, $m$ – кількість символів у слові $Y$, $W$ – сума ваги символів і біграм, однакових для обох слів.

Як видно з формули (1), кількісна оцінка схожості двох однакових слів завжди дорівнює 1, а кількісна оцінка схожості слів, у яких немає жодного спільного символу, завжди дорівнює 0. В інших випадках кількісна оцінка схожості, як і потрібно, знаходиться в діапазоні $(0;1)$.

Наприклад, розглянемо схожість слів „ТЕКСТ” і „ТЕСТ”. Перше слово утворює наступну сукупність символів і біграм: „Т”, „Е”, „К”, „С”, „Т”, „¤Т”, „ТЕ”, „ЕК”, „КС”, „СТ”, „Т¤”. Друге слово утворює наступну сукупність символів і біграм: „Т”, „Е”, „С”, „Т”, „¤Т”, „ТЕ”, „ЕС”, „СТ”, „Т¤”. Як видно, 8 з них спільні: “Т”, “Е”, “С”, “Т”, “Т”, “ТЕ”, “СТ”, “Т”. Їх вага дорівнює 14 одиниць, а кількісна оцінка схожості слів становить 28/33 або приблизно 0,85.

Отже, подібна інтерпретація схожості слів враховує не тільки кількісне співпадіння їх символів, але й також співпадіння порядку слідування цих символів, при цьому враховуються не абсолютні, а саме відносні позиції символів.

Іншою проблемою методів неточного пошуку є проблема оптимізації за швидкодією. Метод аналізу збігу символів і біграм на основі коефіцієнту схожості Серенсена також не є виключенням: важливим його недоліком для практичного використання в контексті вирішення завдань з автоматизованої обробки неструктурованих текстів є неможливість уникнути повного перебору словника і подальшого сортування результатів для встановлення кожного разу найбільш імовірних еквівалентів словникових статей для заданого текстового фрагменту. Для мінімізації зазначеного недоліку можна використовувати паралельні обчислення (наприклад, через розподілену комп’ютерну мережу) або апаратно-програмні рішення на основі нейромереж. Утім, не виключено, що подібні рішення зможуть вирішити проблему лише частково.

**Література**

1. Левенштейн В. И. Двоичные коды с исправлением выпадений, вставок и замещений символов / Докл. Академий Наук СССР, 1965. С. 845-848. [т.163.4]

2. Hyyrö H., Navarro G. Faster bit-parallel approximate string matching. In Proc. 13th Combinatorial Pattern Matching (CPM’2002), LNCS 2373, pages 203-224, 2002.

3. Navarro G. A guided tour to approximate string matching. ACM Computing Surveys, 33(1):31-88, 2001.

4. Sörensen T. A method of establishing groups of equal amplitude in plant sociology based on similarity of species content // Kongelige Danske Videnskabernes Selskab. Biol. krifter. Bd V. № 4. 1948. P. 1-34.

*УДК 378.14*
**Самойленко О.О.**
кандидат педагогічних наук
Національна академія СБ України
**Кащук В.І.**
Національна академія СБ України

# MOBILE TECHNOLOGIES У ПРОЦЕСІ ПІДГОТОВКИ МАЙБУТНІХ ФАХІВЦІВ З ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Проблема якості інтелектуальних ресурсів і, насамперед, якості підготовки фахівців з вищою освітою, здатних вирішувати найскладніші проблеми у всіх сферах суспільства, є першочерговою національною проблемою кожної держави. Існуючі реалії дають змогу стверджувати, що роль майбутніх фахівців з інформаційної та кібернетичної безпеки, їх функції і завдання стають незрівнянно складнішими, особливо в умовах сучасного інформаційного суспільства. Звідси, вибір методів, форм і засобів навчання повинен бути, у першу чергу, орієнтований на перехід від групових до індивідуальних, з власною особистісно орієнтованою траєкторією навчання. Тому в контексті дослідження такі поняття як «технології хмарних обчислень», «мобільні засоби» були виділені як базові.

Серед значної кількості інформаційних середовищ звертаємо увагу саме на LMS MOODLE. Це обумовлене тим, що систему MOODLE можна використовувати також на мобільних пристроях та інтегрувати з хмарними сервісами, а саме: Google Apps for Education та Office 365, використовуючи при цьому мобільну версію MOODLE Mobile [5]. Становлення наукового інтересу до можливостей використання mobile technologies в освітньому процесі пов’язане: 1) зі стрімким розвитком зазначених технологій сьогодні (мобільні пристрої стають загальною тенденцією життя людини в інформаційному суспільстві та надають можливість навчатися будь-де і будь-коли); 2) інтегруючи mobile technologies у традиційну систему освіти, тим самим створюємо передумови для підвищення продуктивності взаємодії учасників освітнього процесу за рахунок емерджентності.

Власне, дослідницька компанія Statcounter, що відстежує використання Інтернету через 2,5 млн сайтів, зазначає, що в лютому 2018 р. близько 51,82% інтернет-сторінок були завантажені саме на мобільних пристроях, а в лютому 2017 р. цей показник становив 45,23% [3].

Таким чином, ситуація, що склалася вимагає від вітчизняної системи освіти пошуку шляхів максимального задіяння потенціалу Mobile technologies при побудові навчального процесу з метою його оптимізації, адаптації традиційних форм навчання до Mobile learning (мобільне на-

вчання). Тож, це стає сучасною дидактичною проблемою, пов'язаною з розвитком професійних здібностей майбутніх фахівців у галузі управління та адміністрування, в основі професійної діяльності яких стане прийняття рішень в умовах невизначеності, новизни і ризику. Популярність і поширеність мобільних пристроїв передбачає інтерес до їх використання, чим можна скористатися і в навчальних цілях. Враховуючи це положення, можна прийти до висновку, що існуюче сьогодні різноманіття мобільних додатків (у тому числі LMS Moodle) безсумнівно забезпечує всіх учасників навчального процесу корисним інструментом, що дозволяє побудувати освітню траєкторію максимально ефективно і результативно. Аналіз підходів до розуміння сутності поняття «мобільне навчання» (Mobile learning), дозволив виділити такі його трактування: розглядається як нова освітня парадигма, на основі якої створюється нове навчальне середовище, яке робить навчальний процес всеохоплюючим [3]; передбачає використання мобільних технологій, як окремо так і спільно з іншими інформаційно-комунікаційними технологіями для організації навчального процесу без залежності від часу та місця [4]; з одного боку, є різновидом дистанційного навчання, а з іншого – навчанням з використанням інформаційно-комунікаційних технологій, але у порівнянні з цими видами навчання мобільне навчання надає суб'єкту, що навчається, більшу кількість «ступенів вільності» – вищу інтерактивність, більшу свободу руху, більшу кількість технічних засобів для навчання [2].

Використання мобільних пристроїв в освітньому процесі з бездротовими мережами сприятиме: наданні майбутньому фахівцю більшої інтерактивності, розширенню простору навчання за межами навчального закладу; створенню нових можливостей для взаємодії викладачів і студентів на аудиторних заняттях, забезпеченню швидкого зворотного зв'язку в умовах незалежності від місця знаходження та ін.

Проведене дослідження не вичерпує всіх аспектів зазначеної проблеми. Перспективою подальших досліджень є вивчення світових інноваційних тенденцій в Mobile learning, з метою пристосування найбільш вдалих підходів до умов вітчизняної освіти.

**Література**

1. Desktop vs Mobile vs Tablet Market Share Worldwide [електронний ресурс]. – Режим доступу : http://gs.statcounter.com/platform-market-share/desktop-mobile-tablet#.

2. Tryus Yu. V. Organizatsiini i tekhnichni aspekty vykorystannia system mobil'noho navchannia [The Organizational and Technical Aspects of The Using of Mobile Learning] / Yu. V. Tryus, V. M. Franchuk, N. P. Franchuk // Naukovyi chasopys NPU im. M. P. Dragomanova. Seriia 2. Kompiuterno-oriiuntovani systemy navchannya [M. P. Dragomanov NPU Journal. Line 2. Computer-Oriented Learning System]. – 2012 – Series 2 (12). – S. 53–62.

3. Рашевська Н. В. Технології мобільного навчання / Н.В. Рашевська, В. В. Ткачук // Педагогіка вищої та середньої школи, 1 (35). – С. 295-301.

4. Рекомендації ЮНЕСКО щодо політики в сфері мобільної освіти [електронний ресурс]. − Режим доступу: http://iite.unesco.org/pics/publications/ru/files/3214738.pdf.

5. Франчук В.М. Використання web-орієнтованих комп'ютерних систем в освітньому закладі [електронний ресурс]. – Режим доступу : http://vfranchuk.ii.npu.edu.ua/images/files/statty/65.pdf.

*УДК 355.40: 356.35*

**Саричев Ю.О.**
кандидат технічних наук,
старший науковий співробітник
Національний університет оборони України
імені Івана Черняховського
**Хоменко Л.В.**
Національний університет оборони України
імені Івана Черняховського

## СУТНІСТЬ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ В СИСТЕМІ ДЕРЖАВНОГО УПРАВЛІННЯ У ВОЄННІЙ СФЕРІ

Термін "інформаційно-аналітичне забезпечення" досить часто використовується в різних сферах діяльності держави, зокрема з питань державного управління у воєнній сфері. Загальний аналіз показує, що інформаційно-аналітичне забезпечення в складному процесі інформаційного забезпечення в системі державного управління займає одне з ключових місць. Проте сьогодні, на жаль, немає єдиного розуміння цього важливого поняття, в наукових та публіцистичних статтях воно має змістову суперечливість. Наслідком є проблема, що заважає розробці власне як методологічних засад інформаційно-аналітичного забезпечення, так і інформаційного забезпечення загалом, зокрема в системі державного управління у воєнній сфері, а також перешкоджає його практичній реалізації.

Об'єктними сферами, де застосовується інформаційно-аналітичне забезпечення, є державне управління, місцеве самоврядування, воєнна сфера, банківська сфера, фондовий ринок, охорона довкілля, соціологія тощо. Незважаючи на важливість функції інформаційно-аналітичного забезпечення в процесі інформаційного забезпечення певної галузі, на практиці має місце плутанина сутності у використанні зазначеного поняття з іншими взаємопов'язаними (спорідненими) з ним поняттями – "інформаційне", "довідкове", "інформаційно-довідкове", "системний аналіз", "аналітичне" тощо. На наш погляд, зазначене є системною методологічною помилкою, яка шкодить реалізації ін-

формаційного забезпечення, зокрема в системі державного управління у воєнній сфері.

Більше того, не лише на практиці, але і у фахових теоретичних працях існуючі на сьогодні трактування інформаційно-аналітичного забезпечення в системі державного управління також засвідчують певну розбіжність у розумінні цього поняття, що досить детально розглянуто в [1]. Тому в цій роботі, а також у [2] подається більш акцентоване визначення: "інформаційно-аналітичне забезпечення – комплекс заходів, що реалізує процеси створення документованих інформаційних продуктів (аналітичних матеріалів) на основі використання статичних інформаційних ресурсів (документованих даних та інформації), їх аналізу і синтезу, а також проведення розрахунків та моделювання ситуацій з метою підтримки прийняття необхідних рішень на всіх рівнях державного управління".

Підкреслимо, що інформаційно-аналітичне забезпечення як процес виробляє та надає в інтересах управління саме *документовані* інформаційні продукти (аналітичні матеріали), про що стверджується в авторитетній праці з проблематики державного управління [3], тобто цим створюються виключно *статичні інформаційні ресурси* в інтересах прийняття управлінських рішень, що є принциповою ознакою цього виду інформаційного забезпечення. Зауважимо, що у ряді випадків управлінські рішення приймаються на основі наявних *динамічних інформаційних ресурсів*, тобто таких, що отримуються в масштабі реального часу і які ще не документовані. Це особливо характерно для воєнної сфери, наприклад, такими є процеси отримання поточної інформації щодо швидкоплинної обстановки у ході бойових дій або вербальне спілкування командування з підлеглими чи його заяви. Такі інформаційні процеси документуються згодом, стаючи статичним інформаційним ресурсом або не документуються взагалі. Вони інформаційно забезпечують хід управління, але це не процеси інформаційно-аналітичного забезпечення, оскільки при цьому аналітичний матеріал (документ) безпосередньо для управління не продукується, а управлінські рішення на основі такого інформаційного ресурсу приймаються та реалізуються оперативно, наближено до масштабу реального часу.

Зазначена особливість, як правило, не враховується, що призводить до певної плутанини як в теорії, так і на практиці. Найчастіше спостерігаються теоретичні спроби та практичні дії інтегрувати складові споріднених функцій двох взаємопов'язаних підпроцесів загального процесу управління – моніторингу та власне інформаційно-аналітичного забезпечення. Усунення означеної методологічної помилки полягає в необхідності точного дотримання фундаментального правила щодо реалізації цілісного контуру управління за кібернетичним принципом, де місце та роль кожної із складових найбільш чітко зрозумілі, а блок моніторингу є просто відокремленим та невід'ємним для реалізації усього кібернетичного циклу управління. Вихідним інформаційним продуктом моніторингу можуть бути як документовані аналітичні

матеріали (статичний інформаційний ресурс), так і недокументовані інформаційні продукти в масштабі реального часу (динамічний інформаційний ресурс).

Тому інформаційно-аналітичне забезпечення органу державного управління у воєнній сфері грунтується на документованих інформаційних матеріалах (результатах), які продукуються, як правило, в ході повільного або прискореного моніторингу (з метою підтримки рішення на майбутні дії, наприклад, блокування загрозливої ситуації або її нейтралізація), а також документованих інформаційних матеріалах, які продукуються за результатами оперативного моніторингу (з метою аналізу дій, що вже відбулися у кризовій ситуації, на основі об'єктивного документування швидкоплинних подій, процесів та явищ).

**Література**

1. Інформаційно-аналітичне забезпечення як вид інформаційного забезпечення в системі державного управління / Ю.О. Саричев // Вісник НАДУ при Президентові України ; [за заг. ред. Ю.В. Ковбасюка]. – 2017. – № 3(86).

2. Роль та місце інформаційного забезпечення в системі державного управління / П.М. Сніцаренко, Ю.А. Саричев // Державне управління: теорія та практика (електронне наукове фахове видання НАДУ). – 2016. – № 1. – С. 46-56.

3. Енциклопедія державного управління: у 8 т. / Нац. акад. держ. упр. при Президентові України ; наук.-ред. колегія: Ю.В. Ковбасюк (голова) та ін. – К. : НАДУ, 2011. – Т. 2: Методологія державного управління / наук.-ред. колегія: Ю.П. Сурмін (співголова), П.І. Надолішній (співголова) та ін. – 2011. – 692 с.

*ДК 378(477)(094)*

**Сафонов Ю.М.**
доктор економічних наук, професор,
заступник директора з наукової роботи
**Дашковська О.В.**
кандидат хімічних наук, доцент,
старший науковий співробітник
**Погребняк В.П.**
кандидат технічних наук, професор,
старший науковий співробітник,
ДНУ «Інститут модернізації змісту освіти»

## ПІДГОТОВКА ФАХІВЦІВ У СФЕРІ КІБЕРЗАХИСТУ – ПРІОРИТЕТИ ДЕРЖАВИ

Проблеми захисту інформації виникли одночасно з її появою, були і є актуальними протягом усієї історії розвитку людського суспільства.

Особливої ваги набуває ця проблема з виникненням і розвитком комп'ютеризованих глобальних інтернет-мереж, здійснення через них об-

міну інформацією, починаючи від персональних даних особи до управління у різних сферах суспільної діяльності і «електронного урядування».

Такі поняття як «кіберпростір», «кіберзлочин», «кібератака», «кіберзброя» тощо почали активно використовуватися серед широкого загалу та у ЗМІ фактично з середини 1990-х. Міжнародні нормативно-правові акти досить широко визначають поняття «кіберзлочин» та протизаконні дії пов'язані з ним [1]. Виходячи з приблизних підрахунків у світі близько 750 тисяч потенційних порушників-кіберзлочинців. За минулий рік збитки світової економіки від кіберзлочинів склала більше 600 млрд. доларів [2]. В Україні тільки у 2017 році було зареєстровано більше 2,5 тисяч кримінальних правопорушень у сфері кібербезпеки, що у три рази більше, ніж у 2016 році. Зважаючи на зазначене, суттєво зростає необхідність розробки і впровадження системних заходів, які охоплюють програмні, технологічні, технічні, організаційні та кадрові проблеми захисту інформаційного простору держави.

Підготовка фахівців з вищою освітою власне для сфери захисту інформації (кіберзахисту) була розпочата в Україні, коли Постановою КМУ від 13 грудня 2006 року № 1719 була затверджена галузь знань 1701 Інформаційна безпека і бакалаврські напрями підготовки «Безпека інформаційних і комунікаційних систем», «Системи технічного захисту інформації», «Управління інформаційною безпекою». У 2010 році Постановою КМУ від 27 серпня 2010 року № 787 [3] в межах зазначеної галузі знань і бакалаврських напрямів були введені спеціальності «Безпека інформаційних і комунікаційних систем», «Безпека державних інформаційних ресурсів», «Системи технічного захисту інформації», «Управління інформаційною безпекою», «Адміністративний менеджмент у сфері захисту інформації»; в галузі знань 0403 «Системні науки та кібернетика» - спеціальність «Криптологія» для освітньо-кваліфікаційних рівнів спеціаліста, магістра. За цей час НМК з Інформаційної безпеки були розроблені і введені в дію всі галузеві стандарти, біля 40 закладів вищої освіти розпочали підготовку кваліфікованих кадрів із зазначених вище спеціальностей.

Постановою Кабінету Міністрів України від 29.04.2015 № 266 [4] затверджено новий Перелік галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти (далі – Перелік-2015). У ньому вилучені існуючі в попередній редакції зазначені вище галузь знань 1701 «Інформаційна безпека» та відповідні спеціальності, замість яких введена «інтегрована» спеціальність 125 «Кібербезпека» в галузі знань 12 «Інформаційні технології».

У контексті обговорюваного питання слід відзначити успішне завершення розробки СВО зі спеціальності 125 Кібербезпека. Комісією у складі 9-ти провідних фахівців України у сфері інформаційної безпеки (голова − Олександр Юдін) у тісній співпраці з університетами, які здійснюють під-

готовку ІТ-фахівців, компаніями-роботодавцями, Держспецзв'язку, СБУ, МОН, ІМЗО створено проект стандарту, що пройшов усі етапи рецензування і експертизи та першим був погоджений Національним агентством із забезпечення якості вищої освіти та направлений на затвердження МОН.

Проблеми впровадження СВО та розроблення профільно-орієнтованої освітньої програми першого (бакалаврського) рівня зі спеціальності «Кібербезпека» неодноразово обговорювались на нарадах в МОН за участю представників ВНЗ, ІТ-спільноти, Держспецзв'язку. Була створена робоча група для розроблення освітніх програм, підготовки фахівців зі спеціальності «Кібербезпека» та координації співпраці всіх зацікавлених сторін.

Заміна цілої галузі «Інформаційна безпека» однією спеціальністю «Кібербезпека» визвала зрозуміле занепокоєння служб у сфері національної безпеки, практичних фахівців тому, що скорочення спеціальностей з підготовки фахівців у сфері інформаційної безпеки не дозволить організувати і забезпечити в Україні системну боротьбу з кіберзлочинністю. Світовий досвід підтверджує про необхідність комплексного системного підходу до забезпечення успіху у цій сфері.

Концептуально необхідно підтримати багаторічні і планомірні дії Держспецзв'язку, який спільно з НМК та іншими зацікавленими структурами вносить пропозиції щодо першочергових заходів з удосконалення системи підготовки та перепідготовки фахівців не тільки з питань кіберзахисту, а й з інших питань удосконалення підготовки фахівців з безпеки інформації. Серед них:

- відновлення галузі знань «Інформаційна безпека» із спеціальностями «безпека інформаційних і комунікаційних систем», «криптологія», «системи технічного захисту інформації» та «управління інформаційною безпекою»;

- розроблення професійних стандартів за названими вище спеціальностями з визначенням необхідних компетентностей;

- організація системи підвищення кваліфікації кадрів у сфері інформаційної безпеки;

- затвердження бакалаврського стандарту вищої освіти за спеціальністю 125 «Кібербезпека».

Станом на початок 2018 року ситуація з розробленням СВО в цілому по МОН України є такою:

- із запланованих 113 СВО освітнього рівня бакалавра та 121 СВО освітнього рівня магістра розроблено 109 бакалаврських і 86 магістерських проектів, які пройшли громадське обговорення, були направлені на фахову і методичну експертизи та погодження;

- майже половина розроблених проектів СВО освітнього рівня «бакалавр» в повному обсязі пройшли необхідні процедури експертиз та пого-

джень, але відсутність діючого НАЗЯВО не дає змоги НМР МОН розпочати процес затвердження СВО. На початок 2018 року Міністерством не було затверджено жодного стандарту вищої освіти, що гальмує процеси створення закладами вищої освіти освітніх програм та акредитаційних справ;

- науково-методичним комісіям НМР МОН України ще належить відкоригувати проекти стандартів вищої освіти відповідно до вимог нових методичних рекомендацій.

Міністерство освіти і науки України, НМР, ІМЗО у пошуках шляхів для розв'язання проблем введення в дію стандартів вищої освіти.

**Література**

1. Конвенція про кіберзлочинність [Електронний ресурс]. − Режим доступу: http://zakon3.rada.gov.ua/laws/show/994_575.

2. Дані подано за публікацією «Народний банкір», газета «Сегодня», № 51, 21.03.2018, с. 12.

3. Постанова КМУ від 27 серпня 2010 року № 787 «Про затвердження переліку спеціальностей, за якими здійснюється підготовка фахівців у вищих навчальних закладах за освітньо-кваліфікаційними рівнями спеціаліста і магістра».

4. Постанова КМУ від 29.04.2015 р. № 266 «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти». [Електронний ресурс]. − Режим доступу: http://tntu.edu.ua/nv/files/266.pdf.

*УДК 004.056.53*

**Скіцько О.І.**
кандидат технічних наук,
старший науковий співробітник
Національна академія СБ України
**Павлючук С.О.**
Національна академія СБ України

## ВПЛИВ ТІНЬОВИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ ДЕРЖАВИ

Інформаційна безпека (ІБ) стала невід'ємною складовою національної безпеки й водночас важливою самостійною сферою забезпечення безпеки держави. На сьогодні інформаційні простір, інфраструктура та технології значною мірою впливають на рівень і темпи соціального, економічного та технічного розвитку держави. Тому все актуальнішою стає дослідження загрози, що набирає все більших масштабів в інформаційній сфері і пов'язана з використанням мобільних або носимих пристроїв (wearable device) на робочому місці.

Мобільні пристрої стали не лише переворотом у розвитку інформаційних технологій, але і кардинально змінили життя сучасних людей. Сьогодні немає необхідності знаходитись в офісі, використання сучасних мобільних пристроїв – головним чином смартфонів та планшетів – дозволило людям отримувати віддалений доступ до своїх даних та пошти, спілкуватись на відстані у реальному часі та зберігати інформацію на віртуальних носіях. Проте розширення можливостей і широкий спектр використання мобільних пристроїв призводить до появи нових загроз. А враховуючи, що ринок саме таких пристроїв є відносно молодим, то і програмних засобів для якісного адміністрування та захисту від вірусів та витоку даних є не достатньо [1].

Обсяг світового ринку носимих цифрових пристроїв (тільки типу розумних годинників, окулярів і носимих сканерів), які використовуються в компаніях, в 2017 році склала 10,6 млрд. дол., а в період 2017-2022 роках зростатиме із середньорічними темпами понад 41% і до 2022 року досягне 60 млрд. дол.[2].

Однак зростання популярності і збільшення числа носимих при собі пристроїв (wearable device) в мережі підвищують ризики безпеки. Тому особливу роль в таких мережах починають відігравати рішення управління парком мобільних пристроїв підприємств (enterprise mobility management, EMM).

Проте таких заходів не достатньо без врахування дій користувачів (співробітників) суб’єкта господарювання, організації. Від використання методів соціальної інженерії не захистять жодні технічні засоби. Озброївшись знаннями з людської психології зловмисники надсилають небезпечні посилання на нову композицію улюбленої музичної групи чи направляють бухгалтеру лист з вкладенням "акт звірки", в якому насправді прихований вірус. Співробітникам необхідно передавати відповідальність за ІБ, навчати їх, контролювати і обов’язково давати зворотний зв’язок (і, якщо необхідно, то і передбачати відповідальність). Тобто всіляко розвивати культуру ІБ, заохочувати усвідомлене використання інформаційних активів.

Якщо цього не робити, то працівники будуть орієнтуватися на свій колишній досвід і поведінку колег, що не завжди добре і може привести до появи нових або зростання старих ризиків ІБ. Одним з таких ризиків, а скоріше навіть "викликом" для ІБ, стає Shadow IT (тіньові інформаційні технології) [3]. Іноді ще зустрічається термін "Stealth IT"[2].

Shadow IT (тіньові інформаційні технології) - неконтрольовані (незареєстровані) пристрої, програмне забезпечення та послуги, що не належать до власності або контролю організації, але використовуються в ній.

Це, наприклад, персональні хмарні сховища і скачане неліцензійне програмне забезпечення, і використання для роботи особистого ноутбуку, і персональна пошта, в якій не встановлені обмеження щодо отримання та

відправлення файлових повідомлень, і особиста WiFi-точка доступу, на якій теж не встановлені обмеження і не налаштований визначеним чином firewoll (мережевий екран), і багато іншого, що використовується працівниками на робочому місці. Причому мотив такої поведінки, зазвичай, є конструктивним і раціональним: це мотивується обмеженими строками виконання поставленого завдання, ігнорування співробітниками технічної підтримки звернень щодо налаштування робочого місця, необхідністю підвищити ефективність, для виконання завдань і таке інше.

Великі компанії в інформаційній сфері наводять таку аналітику використання Shadow IT:

- Skyhigh: 72% організацій не розуміють сферу охоплення Shadow IT, але усвідомлюють проблему [4].

- Cisco: тільки 8% організацій розуміють сферу охоплення Shadow IT у себе [5].

- Forbes: 71% співробітників використовують несанкціоноване програмне забезпечення [6].

- Cisco: 80% співробітників використовують несанкціоноване програмне забезпечення [5].

Використання хмарних сервісів:

- Skyhigh: в середньому співробітники використовують 30 хмарних сервісів [4].

- Cisco: в середньому організації використовують 91 хмарний сервіс [5].

- ITP.net: у 83% організацій використовуються несанкціоновані хмарні сервіси, при цьому більше третини респондентів заявили, що це заборонено в їх організації [7].

І, найважливіше, Gartner (провідна світова дослідницька і консалтингова компанія у сфері інформаційних технологій): до 2020 року третина успішних атак на суб'єкти господарювання (організації) буде реалізовано за допомогою Shadow IT [8].

Характерним прикладом забезпечення безпеки від Shadow IT можна привести роботу підрозділу кібербезпеки міноборони Данії. У березні 2017 року датські депутати приїхали до Росії без мобільних пристроїв та ноутбуків через небезпеку зламування (англ. software cracking) та впровадження шкідливих програм-шпіонів (spyware) у ці носимі електронні пристрої. Але депутатів не залишили без стільникового зв'язку, всім видали кнопочну модель телефону Nokia, який дозволили взяти з собою в Росію [9].

Shadow IT створює нові вразливості і точки входу в IT-інфраструктуру держави, збільшуються ризики витоку інформації, нецільове встановлення та використання неліцензованого програмного забезпечення, що може бути шкідливим для діяльності. в цілому. Shadow IT - досить нова загроза, а зважаючи на те, що темпи використання носимих і мобільних пристроїв збільшується в геометричній прогресії, дослідження в цій галузі стають актуальними.

Врегулювання цієї загрози на рівні держави можливе лише щодо державних інформаційних ресурсів і лише при чіткому знанні та дотриманні всіма користувачами системи протоколів забезпечення інформаційної безпеки.

**Література**

1. Жованик М.О. «Загальні принципи захисту мобільних пристроїв в корпоративній мережі», журнал «Молодий вчений», № 5 (20), с. 39-42, 2015.

2. Gartner «Make Mobile Part of Your Digital Workplace Strategy». URL:https://www.gartner.com/doc/3015425?ref=SiteSearch&sthkw=Shadow%20IT%20refers%20to%20IT&fnl=search&srcId=1-3478922254.

3. А.С. Прозоров, «Когда мало контроля ИБ». URL: https://www.securitylab.ru/blog/personal/80na20/342486.php.

4. Skyhigh «Shadow IT Security Checklist». URL: http://info.skyhighnetworks.com/CH-Shadow-IT-Security-Checklist_Banner-Cloud.html.

5. Joann Starke, «The Shadow IT Dilemma». URL: https://blogs.cisco.com/cloud/the-shadow-it-dilemma.

6. Christopfer Frank, «Shadow IT». URL: https://www.forbes.com/sites/forbesproductgroup/2017/02/22/shadow-it/#66e90c3c79fd.

7. Mark Sutton, «Unauthorised cloud adoption growing issue for CIOs». URL: http://www.itp.net/603235-unauthorised-cloud-adoption-growing-issue-for-cios.

8. Kasey Panetta, «Gartner's Top 10 Security Predictions 2016». URL: http://www.gartner.com/smarterwithgartner/top-10-security-predictions-2016/?cm_mmc=social-_-rm-_-gart-_-swg.

9. Facebook. URL: https://m.facebook.com/martin.lidegaard/photos/a.451142271606144.111938.447217575331947/1215056811881349/?type=3&source=54.

*УДК 355.40*

**Сніцаренко П.М.**
доктор технічних наук,
старший науковий співробітник,
Національний університет оборони України
ім. Івана Черняховського

## ДЕРЖАВНА ІНФОРМАЦІЙНА ПОЛІТИКА ТА ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ: ЩОДО СУТНОСТІ І ВЗАЄМОЗВ'ЯЗКУ

В законодавчих актах України щодо інформаційної сфери досить часто зустрічаються положення з питань регулювання державної інформаційної

політики. Так в Законі України "Про інформацію" [1] закріплено основні напрями державної інформаційної політики, а в Доктрині інформаційної безпеки України [2] йдеться про пріоритети державної політики в інформаційній сфері. В той же час, ні у цих документах, ні в інших чинних законодавчих актах немає визначення поняття *"державна інформаційна політика"*, що шкодить усім практичним діям у цій сфері. Тому потреба такого визначення в законодавстві України була і залишається актуальною, що також потягне за собою відчутні наслідки.

Логіку цього визначення диктує Конституція України, зокрема стаття 17, яка визначає забезпечення інформаційної безпеки однією із найважливіших функцій держави, справою всього Українського народу. Отже і інформаційна політика України має бути спрямована на реалізацію якраз цієї конституційної норми, а не будь-якої іншої. У зв'язку із цим пропонується таке визначення.

*Державна інформаційна політика України* – складова державної політики як сукупність політичних, економічних, соціальних, воєнних, наукових, науково-технічних, інформаційних, правових та організаційних завдань і заходів, спрямованих на забезпечення інформаційної безпеки України.

Таким чином, сенс державної інформаційної політики України полягає у забезпеченні інформаційної безпеки держави, чим визначається прямий та безпосередній зв'язок між цими сутностями. При цьому механізми реалізації державної інформаційної політики України випливають із визначення сутності власне інформаційної безпеки України та шляхів її забезпечення. Така сутність та відповідні положення містяться лише в Законі України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки" [3], чинність якого не відмінено.

З урахуванням положень цього закону, забезпечення інформаційної безпеки України, отже виконання вимоги статті 17 Конституції України, полягає у реалізації запобіжних заходів проти нанесення шкоди через *неповноту, невчасність та невірогідність інформації, що використовується, а також відсутність інформації за її потреби, негативний інформаційний вплив, нерегульоване або злочинне застосування інформаційних технологій, а також несанкціоноване розповсюдження, використання, порушення цілісності, конфіденційності й доступності інформації та інших інформаційних ресурсів.*

При цьому, можливість реалізації запобіжних заходів проти нанесення шкоди визначається рівнем успішності дій (діяльності) на шляхах *створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів, підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації наслідків у випадках їх реалізації, здійснення міжнародного співробітництва з цих питань, вдосконалення нормативно-правової бази щодо забезпечення*

*інформаційної безпеки, з пріоритетом захисту інформаційних ресурсів, протидії комп'ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері.*

Успішне розв'язання проблеми забезпечення інформаційної безпеки України з позиції чинного законодавства, у першу чергу в теоретичній площині, потребує чіткого тлумачення ряду термінів, за допомогою яких законодавством визначені сутність інформаційної безпеки України та шляхи її забезпечення. До таких термінів, що потребують окремого законодавчого визначення, слід віднести наступні:

"інформація", як неоднозначне поняття в законодавстві України;

"інформаційний ресурс", як неоднозначне поняття в законодавстві України;

"повнота інформації";

"вчасність інформації";

"вірогідність інформації";

"цілісність інформації";

"конфіденційність інформації";

"доступність інформації";

"інформаційний вплив", зокрема негативний;

"інформаційна технологія",

"інформаційна інфраструктура держави",

"критичний елемент (об'єкт) інформаційної інфраструктури";

"загроза інформаційній безпеці";

"реалізація загрози інформаційній безпеці";

"захист інформаційних ресурсів";

"комп'ютерна злочинність";

"протидія комп'ютерній злочинності";

"персональні дані";

"захист персональних даних";

"правоохоронна діяльність в інформаційній сфері", а також терміни і поняття, які є родовими від зазначених та потребують роз'яснення .

Дотримання вищенаведеного підходу, а також роз'яснення та зрозуміле тлумачення наведених термінологічних елементів дасть підставу для розробки коректних теоретичних основ забезпечення інформаційної безпеки України, якраз виходячи із вимог Конституції України та чинних базових законодавчих норм держави в інформаційній сфері, що, у свою чергу, сприятиме найбільш ефективній реалізації державної інформаційної політики України за усіма напрямами.

**Література**

1. Закон України "Про інформацію" від 13.01.2011 р. № 2938-VI // [Електронний ресурс]. – Режим доступу: http: // zakon3.rada.gov.ua.

2. Доктрина інформаційної безпеки України, затверджена Указом Президента України від 25.02.2017 р. № 47/2017 [Електронний ресурс]. – Режим доступу: http: // president.gov.ua.

3. Закон України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки" від 09.01.2007 р. № 537-V // [Електронний ресурс]. – Режим доступу: http: // zakon3.rada.gov.ua.

*УДК 378:004.92*

**Спірін О.М.**
доктор педагогічних наук, професор
ДНУ «Інститут модернізації змісту освіти»
**Юдін О.К.**
доктор технічних наук, професор
Національний авіаційний університет

## КОНЦЕПТУАЛЬНІ ПИТАННЯ ПРОФЕСІЙНОЇ СЕРТИФІКАЦІЇ ФАХІВЦІВ З ІНФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ В УКРАЇНІ

В умовах зовнішньої агресії з боку інших держав та дестабілізації соціальних, політичних, економічних відносин в країні, гостро постає проблема розвитку та забезпечення процесів інформаційної та кібернетичної безпеки України.

Концептуальними та життєво важливими стають питання стабілізації і підвищення рівня захисту інформаційного простору країни та безпосередньо критичних інфраструктур. Поставлені стратегічні завдання можуть бути виконані, тільки за наявністю в державі висококваліфікованих кадрів галузі інформаційних технологій та їх безпеки. Професійна підготовка фахівців повинна ґрунтуватись на плідній співпраці закладів вищої освіти з змовниками освітніх послуг.

***Метою*** *досліджень* є – визначити концептуальні підходи та проблемні питання надання освітніх послуг з професійної сертифікації у відповідності до вимог сектору індустрії інформаційної та кібербезпеки.

Згідно законодавчої та нормативно-правової бази України та у встановленому законом порядку основу національної системи кібербезпеки становлять: Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи. На зазначені структури покладені основні завдання забезпечення безпеки кіберпростору країни [1]. Зрозуміло, що визначені вище державні установи, разом з Міністерством науки і культури України, повинні формувати

стратегію розвитку сучасної системи підготовки фахівців освітнього напряму інформаційних технологій з спеціальності «кібербезпека».

Враховуючі світовий досвід університетів США, Англії, Європи, Азії можна зробити висновки про системність роботи університетів у напряму впровадження, так званої *«дуальної освіти»* або професійної системи навчання. Підґрунтям успіху «дуальності», є надання базової академічної освіти та додаткової професійної атестації у напрямах інформаційної або кібернетичної безпеки. В рамках цих проектів, жорстко встановлено зв'язок, між вищим закладом освіти та замовником, а також характером індустріального ринку послуг. Взаємодія: *Університет - Замовник – Ринок послуг галузі*, спрямована на впровадження професійно орієнованих предметів та спеціалізованих фахових курсів з метою організації якісного рівня підготовки кадрів. Велику роботу, щодо академічної та професійної атестації в зазначеному напрямі повинні проводити професійно-спрямовані галузеві громадські об'єднання.

Прикладом всесвітньо відомих організацій професійного спрямування, можуть бути громадські асоціації університетів та груп інвесторів сектору індустрії, так звані – «Групи робочої ініціативи» або «Групи робочої Сили та Освіти». Зазначені об'єднання формують стандарти академічної та професійної освіти у відповідності до індустріального кластеру промисловості. Наприклад, громадські Асоціації США з кібербезпеки (*National Cybersecurity Work Force Framework, National Initiative for Cybersecurity Education's),* є розробниками освітніх стандартів, системи професійної сертифікації а також вимог, компетентностей фахівців з кібербезпеки [2, 3].

Нажаль, на території нашої держави, така практика спільної діяльності всіх членів Асоціацій ринку послуг індустріального сектора відсутня. Існуючі громадські організації, тим більш базових замовників, таких як: Міністерства оборони України, Адміністрації Держспецзв'язку, тощо, мають іншу спрямованість своєї діяльності та не займаються питаннями організації професійної сертифікації фахівців, розробки сучасних планів, глосаріїв, програм дисциплін у відповідності до вимог замовника і ринку послуг.

Можна констатувати, що існує світова стала система загальногалузевої стандартизації освітніх послуг, а також професійної сертифікації кадрів, включно до надбання різних класів компетентностей фахівців з інформаційної і кібербезпеки. Прикладами таких підходів, є існуюча освітньо-професійна доктрина Громадського об'єднання Information Systems Audit and Control Association (ISACA) або Certified Information Systems Security Professional (CISSP).

Світова громадськість в сфері ІТ та їх безпеки, визначає перелік базових освітніх «Доменів» підготовки фахівців з інформаційної та кібербезпеки, а також перелік освітніх установ для проходження професійної сер-

тифікації. Зазначені домени є складовою світової системи підготовки фахівців в галузі та мають, як приклад, наступні складові: організація інформаційної безпеки на базі ризик менеджменту, менеджмент систем ідентифікації та доступу, криптографія, безпека інформаційно-комунікаційних систем, управління інцидентами інформаційної безпеки, тощо.

**Висновки.**

Визначено концептуальні підходи та проблемні питання надання освітніх послуг з професійної сертифікації у відповідності до вимог сектору індустрії інформаційної та кібербезпеки. Встановлено, що світовою спільнотою та університетами різних країн, введено систему професійної сертифікації кадрів.

**Література**

1. Закон України «Про основні засади забезпечення кібербезпеки України», [Електронний ресурс]. - Режим доступу: http://zakon.rada.gov.ua.

2. Certified Information Systems Security Professional (CISSP), [Електронний ресурс] - Режим доступу: https://www.isc2.org/Certifications/CISSP.

3. Computing Technology Industry Association,[Електронний ресурс]. - Режим доступу: https://www.comptia.org/.

4. Cybersecurity Competency Model, [Електронний ресурс]. - Режим доступу: https://www.careeronestop.org/competencymodel/competency-models/cybersecurity.aspx.

*УДК 341.824:338.47 (043.2)*

**Тиква В.Л.**
Національна академія СБ України

## КЛАСИФІКАЦІЯ ДЕСТРУКТИВНОЇ ДІЯЛЬНОСТІ ХАКЕРІВ

Розглянувши ймовірність кіберзагроз, варто зазначити, що за поняттям кіберзлочину стоять цілком реальні люди, яких називають хакерами. За звичайною класифікацією, хакери поділяються на піратів, браузерів та крекерів.

Пірати – непрофесіонали, найменш технічно досвідчені, їхня діяльність обмежується здатністю проникати до систем (їх налічується близько 90%). Браузери – люди, які мають значно ширші технічні знання та можливості, вони отримують несанкціонований доступ до файлів інших людей, до чужих систем, але суттєвої шкоди не завдають (близько 9%). І лише 1% хакерів припадає на крекерів – це, по суті, кіберзлочинці, котрі мають великі технічні можливості, знання та навички. Саме вони шкодять найбільше: від копіювання файлів до цілковитого нищення програм та систем.

Український дослідник О. Чернавський аналізує хакерську спеціалізацію. Він виділяє хакерів-дослідників, хакерів-зламників, хакерів-вандалів, крекерів, піратів, кібертерористів, вірмейкерів (тих, хто працює над створенням комп'ютерних вірусів), кардерів (махінації з кредитними картками та банкоматами), фрікерів (спеціалізуються на незаконному підключенні до телефонних мереж). Вітчизняний дослідник В. Голубєв наводить статистичні співвідношення різних мотивів при вчиненні комп'ютерних злочинів. Так, експертна комісія Інтерполу зазначила, що корисливі мотиви присутні в 66% випадків, політичні – в 17%, дослідницький інтерес превалював у 7% випадків, хуліганство – 5%, помста – 4%.

Незаперечним є те, що кіберактивісти сьогодні намагаються перенести до кіберпростору реальні рухи громадянської непокори. На думку Д. Деннінг, Інтернет сьогодні вважається впливовим важелем для зміни курсів внутрішньої та зовнішньої політики будь-якої держави і передбачає в цьому аспекті три види діяльності: 1) соціальна активність; 2) хактивізм (від англ. *hack* і *activism*); 3) кібертероризм.

*Перший вид діяльності – соціальна (політична) активність* – не передбачає якоїсь підривної діяльності, а полягає в різних формах висловлення своїх поглядів. Форми можуть бути різними: створення сайтів, розсилання поштових повідомлень, написання електронних публікацій, обговорення проблем, створення певних коаліцій на форумах та в чатах, організація діяльності останніх.

*Друга категорія соціально та політично активних користувачів* мережі Інтернет використовує переважно незаконні методи діяльності. Їхні дії не завдають суттєвих збитків. Приклади – страйки в Інтернеті, цілеспрямовані бомбардування чиєїсь електронної пошти, веб-хакерство, комп'ютерні злами, віруси та «хробаки». *Хактивізм* – це поєднання соціальної (політичної) активності та хакерства. Останні використовують спеціалізоване програмне забезпечення. Переважна більшість соціально активних хакерів прагне якомога більшого інформування про свої дії, тому широко використовує медіаскладову.

Страйки в Інтернеті полягають у відвідуванні хакерами певного сайту та створенні такого трафіку, за якого інші користувачі не можуть цей сайт відвідати. Під час передвиборних кампаній різних років українські політики відчували на собі дії хакерів: їхні персональні сайти не працювали і по кілька діб, і протягом тижня. Одним із найвідоміших фактів страйку була атака 2007 року на сайт колишнього народного депутата – політолога Дмитра Видріна. Результатом стали заголовки в Інтернеті на кшталт «Видріна вбито!» – таким чином політик використав неприємний факт кількаденного страйку та зробив собі на цьому PR. До речі, дуже нетривіальний хід, коли медіаскладова стала значно ефективнішим засобом не для хакерів, а для їхньої жертви.

Так, тисяча або кілька тисяч листів, надісланих одночасно за допомогою спеціальних програм конкретній особі-політику (бомбардування електронної пошти, яке ще називається «роїнням»): поштова скринька переповнюється, інші відвідувачі сайту не можуть зв'язатися із її власником, відсутність транспарентності в діях політика та його політичної сили дратує, викликає невдоволення, в цьому починають вбачати політичний підтекст. Як наслідок – певні збитки для політичного рейтингу. Якщо такі дії хакерів помічають не відразу або ж вони системні, фактор часу – за тиждень чи за кілька днів перед виборами – може стати фатальним.

Приклади соціальної та політичної активності хакерів з інших країн вражають. А політичну складову українських знавців роботи Інтернету в нас ставлять під сумнів: більшість хакерів в Україні використовують свої спеціальні знання з метою збагатитися і працюють на замовлення представників політичних чи бізнесових кіл.

Комп'ютерні віруси та «хробаки» використовуються хактивістами, зазвичай, для розповсюдження повідомлень, що містять протестні заклики та пошкоджують програмне забезпечення або ж можуть завдати комп'ютеру фізичної шкоди (перепрограмувати його на самознищення). З історії, перший протест, пов'язаний з використанням «хробака», стався 1989 року: раптом учені Адміністрації національної аеронавтики та космонавтики США побачили картинку з надписом: «Хробаки проти ядерних убивць! Ви говорите про мир для всіх, а самі готуєтеся до війни». Таким чином протестувальники вимагали зупинити запуск на Юпітер космічного човника з обладнанням, що мало живитися від радіоактивного плутонія. Так ніхто й не довідався, що то за автор «хробака» з посланням… Але може здатися, що хакери – це просто бешкетники, які мають спеціальні знання, така собі секта втаємничених, мета якої налагодити дієвий громадський контроль на рівні користувачів Інтернету. На жаль, дії хакерів межують із діями, що мають ознаки кібернетичного тероризму. Так, 1999 року ізраїльський підліток Нір Зигдон оголосив, що знищив іракський урядовий сайт. Невдовзі хлопець став мало не національним героєм. Підліток дав інтерв'ю: «… сайт містив брехню про США, Велику Британію та Ізраїль, а також безліч жахливих заяв про євреїв… Я подумав, що коли Ізраїль боїться вбити Саддама Хусейна, то я зможу, принаймні, знищити його сайт!». Хитромудрий хакер послав на іракський сайт комп'ютерний вірус у додатку до електронної пошти. Не було гарантії, що службовці, які опікуються сайтом, відкриють лист та подивляться заражене вкладення. Тоді Нір Зигдон вдався до хитрощів: він написав у листі, що є палестинським прихильником Саддама і створив вірус, здатний знищити ізраїльські сайти. Довірливі іракці відкрили додаток, і вірус знищив їхній сайт протягом години. Максимум, що хакер отримав у відповідь – це побажання «піти до дідька», відправлене йому іракськими потерпілими…

Вірусова та «хробакова» активність в Україні доволі висока. Проте колективів, що цілеспрямовано продукують віруси та розповсюджують їх, переслідуючи якусь мету, не зареєстровано. Зараження комп'ютерів і систем відбувається на рівні провайдерів, котрі нехтують безпекою своїх користувачів, або ж на рівні пересічних Інтернет-користувачів, котрі взагалі не користуються антивірусними програмами або ж не слідкують за їхнім регулярним поновленням. Хакери успішно сканують Інтернет і вишукують заражені комп'ютери, з хибними конфігураціями і належним чином не захищені. Такі машини можуть стати частиною «мережі ботів» (бот – це почасти автономна комп'ютерна програма, що контролюється віддаленим користувачем та здатна заражати комп'ютери). Часто виявляється, що хакер-одинак контролює тисячі заражених комп'ютерів, у різних куточках планети. Він може давати команди комп'ютерам із своєї «мережі ботів» та через зашифрований комунікаційний канал відслідковувати всі дії власників заражених комп'ютерів – сканувати їхню інформацію, переписувати файли, передавати копії їхніх даних або ж давати їм команду, одночасно здійснивши атаку на будь-який комп'ютер-мішень або мережу (так сталося із сайтом Д. Видріна). Власники про це навіть не здогадаються…

*УДК 351.746:007*

**Ткачов І.В.**
кандидат юридичних наук,
старший науковий співробітник
Національна академія Служби безпеки України

## ЩОДО УДОСКОНАЛЕННЯ КОНЦЕПТУАЛЬНИХ ЗАСАД ПРОТИДІЇ ТЕРОРИЗМУ В УКРАЇНІ: ІНФОРМАЦІЙНИЙ АСПЕКТ

Стратегія національної безпеки України 2015 року до актуальних терористичних загроз національній безпеці України відносить: 1) агресивні дії Росії, що здійснюються для виснаження української економіки і підриву суспільно-політичної стабільності з метою знищення держави Україна і захоплення її території, а саме: розвідувально-підривна і диверсійна діяльність, дії, спрямовані на розпалювання міжетнічної, міжконфесійної, соціальної ворожнечі і ненависті, сепаратизму і тероризму, створення і всебічна підтримка, зокрема військова, маріонеткових квазідержавних утворень на тимчасово окупованій території частини Донецької та Луганської областей (п.3.1); 2) неефективність системи забезпечення національної безпеки і оборони України: діяльність незаконних збройних формувань, зростання злочинності, незаконне використання вогнепальної зброї (п.3.2); 3) загрози 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 (п.3.8.) [1].

Враховуючи сучасну суспільно-політичну ситуацію в державі в умовах зовнішньої агресії проти України та проведення антитерористичної операції на сході України чинна Концепція боротьби з тероризмом, затверджена Указом Президента України від 25 квітня 2013 року №230 (далі – Концепція) потребує суттєвого переопрацювання (оновлення). Насамперед слід зазначити, що процес розробки такого нормативно-правового акту, на нашу думку, передбачає відпрацювання питання щодо структури документу, тобто тих розділів (глав, частин), які будуть становити його своєрідний каркас. Таку структуру, як вбачається, потрібно на першому етапі одержати у погодженому вигляді із зацікавленими підрозділами Центрального управління СБУ, суб'єктами боротьби з тероризмом. Наступним кроком відповідно має бути наповнення його змістовною частиною. На нашу думку, чинна Концепція за своєю структурою як загальнодержавний нормативно-правовий акт відповідає принципам побудови таких документів концептуального характеру, має власну логіку (проблема – мета – принципи – напрями реалізації – шляхи розв'язання проблеми). Інша справа – змістовне наповнення цього каркасу в сучасних умовах, тобто мова йде про актуалізацію існуючих структурних елементів Концепції. У ході оновлення вбачається така структура цього документу: 1) преамбула (характеристика сучасної суспільно-політичної ситуації в державі і світі); 2) проблема, що потребує розв'язання (власне з чим має боротися держава в у мовах зовнішньої збройної агресії); 3) мета, принципи, напрями реалізації; 4) шляхи і засоби розв'язання проблеми; 5) очікувані результати.

Щодо змістовного наповнення та внесення коректив до чинної Концепції:

1) доцільно виключити абзац ІІ розділу 1, в якому містяться неактуальні положення, у т.ч. посилання на Стратегію національної безпеки України "Україна у світі, що змінюється" 2012 року, яка втратила чинність; абзаци 5 – 13 розділу 1 потребують суттєвого переопрацювання, де йдеться зокрема про те, що «… Україна не належить до держав із високою ймовірністю вчинення на їх територіях міжнародними терористичними організаціями терористичних актів …», «в Україні відсутні внутрішні передумови для виникнення організацій, які б використовували терористичні методи …» і т.ін.; тут слід передбачити положення виходячи із визначених Стратегією національної безпеки України 2015 року актуальних терористичних загроз національній безпеці України (пункти 3.1, 3.2., 3.7, 3.8);

3) у цьому розділі слід передбачити положення з урахуванням наступного. У розділі 4 Доктрини інформаційної безпеки України 2017 року [3] визначені загрози національним інтересам та національній безпеці Украї-

ни в інформаційній сфері. У порівнянні з попередньою Доктриною 2009 року в цілому врахований досвід участі України в гібридній війні, проведенні антитерористичної операції на сході країни. Водночас, по-перше, в останньому абзаці розділу 4 міститься визначення загрози як «поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні». На наш погляд, доцільно в Концепції розкрити положення про «іноземний інформаційно-психологічний та пропагандистський вплив в інформаційному просторі України на шкоду національним інтересам та безпеці держави».

4) доцільно передбачити, що до загрозливих чинників, що сприяють поширенню тероризму в Україні, відносяться у т.ч.: активний інформаційно-психологічний та пропагандистський маніпулятивний вплив на населення в окремих районах Донецької та Луганської областей; активне використання ресурсів мережі Інтернет (соціальних мереж) з метою пропаганди терористичних методів, ведення вербування до лав терористичних угруповань та здійснення фінансування терористичної діяльності, а також розповсюдження матеріалів і технологій вироблення засобів ураження та тактики ведення терористичної діяльності тощо.

**Література**

1. Стратегія національної безпеки України, затверджена Указом Президента України від 26 травня 2015 року № 287/2015 // Офіційний вісник України від 09.06.2015.– № 43, стор. 14, стаття 1353.

2. Концепція боротьби з тероризмом, схвалена Указом Президента України від 25 квітня 2013 року №230 // Офіційний вісник України від 10.05.2013. –№ 34, стор. 30, стаття 1202.

3. Доктрина інформаційної безпеки України, затверджена Указом Президента України від 25 лютого 2017 року №47/2017 // Офіційний вісник України від 10.03.2017. – № 20, стор. 3, стаття 554.

*УДК 35.078.3+004.056*

**Ткачук Н.А.**
кандидат юридичних наук,
НДІІП НАПрН України

## ДО ПРОБЛЕМИ ФОРМУВАННЯ ПЕРЕЛІКУ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ

Забезпечення надійного кіберзахисту об'єктів критичної інфраструктури є однією з ключових умов безпечного функціонування кіберпросто-

ру, його використання в інтересах особи, суспільства і держави. Наслідки масованих кібератак на комп'ютерні мережі банківського, енергетичного, транспортного секторів, галузі зв'язку, а також органів державної влади України, які відбулися у червні 2017 року, викликали значний резонанс у суспільстві та засвідчили невідповідність існуючого стану захисту критичної інформаційної інфраструктури держави актуальним та потенційним кіберзагрозам сьогодення.

Підвищення ефективності та удосконалення організаційно-правових засад забезпечення кіберзахисту об'єктів критичної інфраструктури, в тому числі, тих які перебувають у приватній власності, а також встановлення відповідних вимог у цій сфері до їх власників та операторів неможливі без визначення на загальнодержавному рівні безпосереднього переліку їх інформаційно-телекомунікаційних систем (ІТС), що потребують пріоритетного захисту від кібератак та повинні належати до критичної інформаційної інфраструктури держави.

Водночас, незважаючи на ініціативи вищих органів влади щодо формування такого переліку, наразі, це питання в Україні залишається невирішеним, що негативно впливає на подальший розвиток спроможностей держави з протидії кіберзагрозам.

Існуючі організаційно-правові засади формування переліку інформаційно-телекомунікаційних об'єктів критичної інфраструктури держави (далі - Перелік), на сьогодні, не можуть забезпечити його дійсне формування і затвердження та потребують удосконалення. При цьому основними проблемними питаннями визначаються наступні:

– відсутність у державі переліку об'єктів критичної інфраструктури, який повинен бути основою при подальшому формуванні переліку інформаційно-телекомунікаційних систем таких об'єктів;

– відсутність чітких, нормативно-закріплених критеріїв щодо оцінки негативних наслідків, до яких може призвести кібератака на інформаційно-телекомунікаційну систему, що визначатиме належність ІТС до критичної інформаційної інфраструктури держави та обумовлюватиме необхідність включення до Переліку;

– низький рівень співпраці з приватним сектором та небажання власників і операторів об'єктів критичної інфраструктури брати на себе додаткові зобов'язання у сфері кіберзахисту;

– формальний підхід відповідальних посадових осіб центральних органів виконавчої влади до формування Переліку, зокрема, подання несвоєчасної та неповної інформації щодо ІТС, які мають бути до нього включені.

Отже, завдання із формування переліку ІТС об'єктів критичної інфраструктури та їх кіберзахист доцільно реалізовувати в рамках системи комплексного захисту критичної інформаційної інфраструктури держави та на

підставі попередньо сформованого переліку таких об'єктів, а також визначеної методики щодо оцінки потенційних негативних наслідків кібератак на їх інформаційно-телекомунікаційні системи.

Потребує уточнення поняття «критична інформаційна інфраструктура», яке повинно включати не лише інформаційно-телекомунікаційні системи об'єктів критичної інфраструктури, але й національні електронні інформаційні ресурси (державні реєстри, бази даних тощо), кібератака на які може призвести до завдання суттєвої шкоди національним інтересам.

Крім того, необхідним є налагодження ефективної співпраці з приватним сектором у напряму забезпечення включення до Переліку інформації щодо об'єктів критичної інфраструктури, які перебувають у приватній власності, та організації належного рівня її кіберзахисту.

З метою якісного виконання відповідальними посадовими особами органів державної влади завдань, передбачених чинними нормативно-правовими актами, щодо реалізації заходів з розбудови ефективної системи кіберзахисту ІТС об'єктів критичної інфраструктури держави, у тому числі формування Переліку, вбачається доцільним підвищити контроль з боку компетентних держаних органів, зокрема Національного координаційного центру кібербезпеки при РНБО України, за станом їх виконання та вжити в установленому порядку заходів щодо притягнення до відповідальності осіб, які не забезпечили своєчасне виконання зазначених завдань.

*УДК 340+35.078.3*

**Ткачук Н.І.**
кандидат юридичних наук,
головний спеціаліст ДІАЗ СБ України

## НАЦІОНАЛЬНІ КОНСТИТУЦІЙНІ ТА МІЖНАРОДНІ НОРМИ ПРО ІНФОРМАЦІЙНІ ПРАВА ЛЮДИНИ

Конституція України, як Основний закон нашої держави, слугує вектором вітчизняного суспільного розвитку, зокрема й інформаційного суспільства, що відображено в документі «Стратегія розвитку інформаційного суспільства в Україні» від 15 травня 2013 р. № 386-р [1]. Згідно з цим документом, під інформаційним суспільством розуміється суспільство, орієнтоване на інтереси людей, відкрите для всіх, в якому кожна людина може створювати і накопичувати інформацію та знання, мати до них вільний доступ, користуватися і обмінюватися ними, мати можливість повною мірою реалізувати свій потенціал, сприяти суспільному і особистісному розвиткові та підвищувати якість життя [1]. При цьому важливо, щоб ін-

формаційні права і свободи відповідали високим світовим стандартам і загальнолюдським цінностям в цій сфері, які створювалися і уточнювалися протягом багатьох десятиліть.

Основні інформаційні права та свободи людини і громадянина закріплені як на міжнародному, так і на національному законодавчих рівнях. Загальновідомо, що спочатку інформаційні права і свободи були відображені в основоположних документах стосовно прав і свобод людини і громадянина. Вони і сьогодні не втратили своєї актуальності як справжній орієнтир розвитку позитивного права багатьох держав [2]. Серед таких документів слід згадати, насамперед, Білль про права від 15 грудня 1791 р. та Поправку І Конституції США. Зокрема, ними встановлено, що Конгрес не повинен видавати жодного закону, що забороняє вільне віросповідання, або обмежує свободу слова чи друку або право народу мирно збиратися і звертатися до уряду з петиціями про задоволення скарг. Французькою Декларацією прав людини і громадянина від 26 серпня 1789 у ст. 11 проголошено, що вільне вираження думок і поглядів є одним з дорогоцінних прав людини; тому кожен громадянин може вільно висловлюватися, писати, друкувати, відповідаючи лише за зловживання цією свободою у випадках, передбачених законом. Стаття 16 Декларації встановлює, що суспільство, в якому не забезпечена гарантія прав і немає поділу влади, не має конституції. Отже, можна вважати, що ці базові статті становлять основу міжнародної системи захисту прав людини та її основних свобод, в тому числі і в інформаційній сфері.

Конституція України віддає пріоритет саме ратифікованим міжнародним документам, до яких приєдналася наша країна. До таких актів, в яких в загальному вигляді (в силу їх комплексності) закріплено норми-принципи, присвячені правам і свободам в інформаційній сфері, можна віднести наступні.

Загальна декларація прав людини від 12 грудня 1948 р. проголошує в преамбулі як високе прагнення людей створення такого світу, в якому люди матимуть свободу слова і переконань і будуть вільними від страху і нужди. Крім цього, декларацією передбачено, що ніхто не може зазнавати безпідставного втручання у його особисте і сімейне життя, безпідставного посягання на недоторканність його житла, тайну його кореспонденції або на його честь і репутацію. Кожна людина має право на законний захист від такого втручання або таких посягань (ст. 12). Даний документ закріплює також право на свободу думки, совісті і релігії (ст. 18); право на свободу переконань і на вільне їх виявлення; це право включає свободу безперешкодно дотримуватися своїх переконань та свободу шукати, одержувати і поширювати інформацію та ідеї будь-якими засобами і незалежно від державних кордонів (ст. 19) [3].

Конвенція про захист прав людини і основоположних свобод від 4 листопада 1950 р. встановлює, що кожен має право на свободу вираження поглядів. Це право включає свободу дотримуватися своїх поглядів, одер-

жувати і передавати інформацію та ідеї без втручання органів державної влади і незалежно від кордонів (ст. 10) [4].

Міжнародний пакт про громадянські і політичні права від 16 грудня 1966 р. визначає право кожної людини на вільне вираження своїх поглядів свободу шукати, одержувати і поширювати будь-яку інформацію та ідеї, незалежно від державних кордонів, усно, письмово чи за допомогою друку або художніх форм вираження чи іншими способами на свій вибір (ч. 2 ст. 19) [5].

У національному законодавстві основні інформаційні права і свободи людини і громадянина закріплені нормами Конституції України, а також положеннями цілого масиву нормативно-правових актів. Інформаційні права і свободи людини та громадянина, як такі, що належать до громадянських, політичних прав, котрі є невід'ємною частиною людської гідності, отримали в літературі назву права «першого покоління».

**Література**

1. Розпорядження Кабінету міністрів України «Про схвалення Стратегії розвитку інформаційного суспільства в Україні» від 15 травня 2013 р. № 386-р: [Електронний ресурс]. - Режим доступу: http://zakon5.rada.gov.ua/laws/show/386-2013-%D1%80/page.

2. Лапина М. А. Информационное право / М. А. Лапина, А. Г. Ревин, В. И. Лапин. – М. : Юнити : Закон и право, 2004. – 335 с.

3. Загальна декларація прав людини, прийнята і проголошена в резолюції 217 А (III) Генеральної Асамблеї ООН від 10 грудня 1948 р. [Електронний ресурс]. – Режим доступу: http://zakon0.rada.gov.ua/laws/show/995_015.

4. Конвенція про захист прав людини і основоположних свобод від 4 листопада 1950 р .№ 995-004: [Електронний ресурс]. - Режим доступу: http://zakon5.rada.gov.ua/laws/show/995_004.

5. Міжнародний пакт про громадянські і політичні права від 16 грудня 1966 р. № 995-043 : [Електронний ресурс]. - Режим доступу: http://zakon3.rada.gov.ua/laws/show/995_043.

*УДК 340+35.078.3*

**Ткачук Т.Ю.**
кандидат юридичних наук, доцент
заступник завідувача СК-32
Навчально-наукового інституту
інформаційної безпеки НА СБ України

## АКСІОЛОГІЧНІ КОНСТАНТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Коли люди ведуть мову про засоби масової інформації, вони мають на увазі у першу чергу засоби зв'язку, чи навіть канали зв'язку. З найдревні-

ших часів зв'язок асоціювався з магією. Одним з різновидів магії був звук. Людський голос (звук, який видався людиною) вважався магічним за своєю природою. У книзі Буття Адам виконував магічну за своєю суттю дію, дававши імена рослинам і тваринам. Таким чином він підтверджував дану йому Богом могутність, а проголошення назв стало справжньою демонстрацією магічних можливостей. Самі імена теж наділялися магічною силою. Так, в древньому іудаїзмі ім'я Бога само по собі було ототожненням могутності і проголошувати його міг лише первосвященик один раз в рік, знаходячись наодинці у найсвятішій частині Храму. У багатьох культурах особи, які проходили певні ритуали посвячення, отримували нові і часто утаємничені імена. Як говорить древня ірландська легенда, поет, який завдяки своїй магічній особливості управляти мовою, міг прокляти іншу особу, давши йому ім'я з «вплетеним» у нього прокляттям.

Якщо зв'язок вважався за своєю природою магічним, то таким був і процес підтримки цього зв'язку. До прикладу, Тот в єгипетській міфології був богом як магії, мудрості так і писемності, причому різниці між цими поняттями практично не існувало. У древньоєврейському алфавіті, а пізніше і в Кабаллі, букви і слова самі по собі були носіями магічної сили. Так слова «*вимовляти*» та «*читати заклинання*» ставали синонімами. У багатьох древніх культурах ті, хто мав доступ до цієї особливої магії - до загадкових тайн знаків і звуків, які забезпечували і оберігали зв'язок – вважалися хранителями магії.

Чим менше доступними були засоби зв'язку, вони перетворювалися в прерогативу посвячених, тим більше асоціювалися з тайною та магією. Відомо, що німецький гуманіст, лікар, алхімік, натурфілософ, окультист, астролог і відомий адвокат Агріппа Неттесгаймскій переписувався з вченими з інших країн, а пізніше укріплював свій образ мага, видаючи отриману від них інформацію за повідомлення духів.

Абсолютно не важливо, що наш розум сьогодні привик сприймати ці речі як продукти технології, а не магії. До того як картезіанське мислення призвело до фрагментації знання, магія і технології були єдині. Зараз вони залишаються нероздільними тільки в метафоричному смислі. Проте, незалежно від термінології багато до цих пір продовжують говорити про «мистецтво створювати події». Від Агріппи до нас пройшло дуже багато часу. Змінилися й технології. Ми живемо в епоху цифрових технологій і вже не уявляємо нашого буття без Інтернету, електронної пошти та інших результатів технологічного прогресу. Проте, і сьогодні «*Хто володіє інформацією, той володіє світом*», – як сказав колись Уїнстон Черчілль, залишається певним магічним дійством, здатним впливати на маси, результати виборів до парламенту чи президента, ставати поштовхом до революції, війн тощо. І якщо цей світ являє собою найбільш яскраву на сьогодні демонстрацію магічної сили, то він також є потужною потенційною силою для маніпуляцій свідомістю, а це і є свого роду магія.

Інформаційна безпека держави це завжди сутнісно діалектичне поняття, так як безпека може існувати лише в контексті небезпеки, постійних загроз, постійного процесу виявлення цих загроз, їх локалізації, зменшення негативного впливу, прогнозу на майбутнє.

Виходячи із сучасної ситуації, ускладненої подіями на сході України та в Криму, а також постійної модифікації загроз в інформаційній сфері на глобальному рівні, інформаційну безпеку держави слід визначати як постійний процес діяльності компетентних органів, направлений на попередження, протидію загрозам в інформаційній сфері, а також застосування активних заходів інформаційного впливу та сукупність умов такої діяльності, які реалізуються й здатні контролюватися тривалий час. Оскільки під дією інформаційних впливів може цілеспрямовано змінюватися світогляд та мораль як окремих осіб, так і суспільства в цілому, нав'язуватися чужі інтереси, мотиви, спосіб життя, на перший план випливає аналіз сутності та форм проявів сучасних методів прихованого агресивного впливу, вияву дій, що мають цілеспрямований агресивний характер і які суперечать інтересам національної безпеки, вироблення механізмів протидії їм у всіх напрямах, інформаційна безпека держави включає в себе не тільки захист, а й вміння та здатність створювати інформаційні загрози противнику. На нашу думку, таке визначення базується на комплексному функціональному визначенні національної безпеки та врахуванні особливостей інформаційної сфери, а також акцентує увагу не лише на пасивній (протидія інформаційним загрозам), але й на активній складовій (створення інформаційних загроз) інформаційної безпеки. Останнє є особливо актуальним у світлі завдань, визначених Стратегією національної безпеки, щодо протидії інформаційній війні, яка ведеться проти України.

*УДК 004.056.5.378.1*

**Толюпа С.В.**
доктор технічних наук, професор
Київський національний університет
імені Тараса Шевченка
**Браіловський М.М.**
кандидат технічних наук, доцент
Київський національний університет
імені Тараса Шевченка

## ПРОБЛЕМИ ПІДГОТОВКИ ФАХІВЦІВ ПО КІБЕРБЕЗПЕЦІ ТА ЗАХИСТУ ІНФОРМАЦІЇ

В умовах протистояння України зовнішній агресії, становлення її як демократичної держави, прагнення щодо вступу до європейських та євроатлантичних структур, кількість та якість загроз і небезпек, спрямованих проти України, суттєво збільшуються. Виходячи з цього, проблематика

національної безпеки стає особливо актуальною та гостро ставить питання про «розвиток системи підготовки кадрів для потреб органів сектору безпеки і оборони України та розвиток науково-виробничого потенціалу такої системи» [1].

Для України, як на наш погляд, одною із головних проблем залишається при цьому саме незадовільне кадрове забезпечення фахівцями із кіберзахисту та їх розподілення на працевлаштування. Про таке свідчать матеріали аналітичної доповіді Національного інституту стратегічних досліджень при Президентові України «Кібербезпека: світові тенденції та виклики для України», а також результати аудиту нещодавно виведених з обігу стандартів вищої освіти у галузі знань 1701 «Інформаційна безпека», які показали, що професійні компетентності, задекларовані в цих галузевих стандартах, неповною мірою враховують стан та перспективу розвитку методів і засобів забезпечення кібербезпеки. Імовірно, саме це стало відправною точкою для прийняття постанови Кабінету Міністрів України від 29 квітня 2015 року № 266, яка внесла зміни до «Переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти» та визначила для України лише одну безпекову спеціальність – 125 «кібербезпека». Виходячи з цього та з врахуванням вимог Закону України «Про вищу освіту» стають актуальними питання щодо змісту, обсягу та оцінювання якості змісту і результатів освітньої діяльності вищих навчальних закладів (ВНЗ) за спеціальністю «кібербезпека» [2], запровадження спеціалізацій, що відповідають спеціальностям колишньої галузі знань «інформаційна безпека», розроблення нових освітніх програм та проведення їх акредитації. Формування професійної компетентності майбутніх фахівців кібернетичної безпеки розглядається при цьому, як трирівневий педагогічний процес, який відповідно до вимог закону України «Про вищу освіту» включає послідовну й неперервну фахову підготовку відповідно до Галузевих стандартів вищої освіти на першому (бакалаврському) і другому (магістерському) освітньо-професійних та третьому (доктор філософії) освітньо-науковому рівнях й здійснюється у вищих навчальних закладах ІІІ – ІV рівнів акредитації або у спеціалізованих структурних підрозділах – навчально-наукових інститутах. Підготовка фахівців в галузі кібернетичної та інформаційної безпеки ведеться у багатьох ВНЗ України, але мало які з них відстежують працевлаштування своїх випускників. Тому існує велика ймовірність використання знань, отриманих у вишах, проти суспільства та держави у основних сферах життєдіяльності України [3].

Зважаючи, що останнім часом інформаційні технології все частіше використовуються для досягнення воєнно-політичних цілей, втручання у внутрішні справи суверенних держав та порушення суспільного порядку, здійснення актів агресії проти інших держав, здійснення деструктивного

впливу на об'єкти критичної інфраструктури, то це дає можливість застосування проти нашої держави низки кібератак і кібероперацій, які можуть призвести до проблем, пов'язаних із забезпеченням безперебійного функціонування об'єктів критичної інфраструктури, цілісності та конфіденційності інформації, а також її збереження, тобто всього того, з чим вже зіштовхнулась більшість країн Заходу – залишається актуальною. З метою убезпечення від таких дій постає потреба у проведенні, перш за все, інформаційно-пропагандистської кампанії про значимість проблематики інформаційної та кібербезпеки, а також підвищенні компетентності фахівців різних сфер діяльності з цих питань. При цьому за доцільне вбачається фахову підготовку фахівців з інформаційної і кібербезпеки для потреб як силових структур та органів державного управління, так і виробничої та банківської сфери проводити у єдиній системі освіти України, а спеціальну підготовку офіцерського складу ЗС України та інших силових структур із загальних питань – в системі командирської підготовки та на курсах підвищення кваліфікації [4].

Таким чином, автори вважають, що необхідно посилити контроль за працевлаштуванням випускників ВНЗ. Перевіряти куди вони йдуть, в державні чи приватні структури, де ті знаходяться і кому підпорядковуються.

При вступі абітурієнтів до навчального закладу на спеціальності, пов'язані з інформаційною та кібернетичною безпекою, необхідно проводити додатково профвідбір (наприклад, тести) за морально-психологічними якостями, тому що не дивлячись на підвищення в останні роки патріотизму, все одно є велике бажання молоді переїхати і попрацювати за кордоном. Тим паче, що знання іноземних мов є також пріоритетною програмою нашої держави. Таким чином ми можемо просто готувати за держбюджетні кошти кадри, які не тільки ніколи не будуть приносити користі Україні, а у деяких випадках навіть можуть шкодити.

**Література**

1. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 15 березня 2016 р. №96/2016 [Електронний ресурс]. - Режим доступу: http://www.president.gov.ua/documents/962016-19836.

2. «Про вищу освіту». Закон України від 1.07.2014 року № 1556-VII.

3. Buryachok V., Bogush V. Guidelines for the development and implementation training profile «cyber security» in Ukraine // Ukrainian Scientific Journal of Information Security, 2014, vol. 20, issue 2, p. 126-131.

4. В.Л. Бурячок, І.Р. Пархомей, М.М. Степанов, В.Б.Толубко Проблемні питання та актуальні завдання підготовки фахівців з кібернетичної безпеки галузі знань «інформаційні технології». Сучасний захист інформації. № 2, 2016.

*УДК 355.233-049.65:004.0562(045) У-48*
**Уліч В.Л.**
кандидат педагогічних наук, доцент
Військовий інститут Київського національного
університету імені Тараса Шевченка

# ТЕХНОЛОГІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОСВІТНЬОГО ПРОЦЕСУ У ВИЩИХ ВІЙСЬКОВИХ НАВЧАЛЬНИХ ЗАКЛАДАХ

Сучасні інформаційно-технологічні революції, що відбуваються на всіх континентах і у багатьох країнах світу, зумовили необхідність пошуку нових підходів до професійної підготовки майбутніх фахівців у сфері інформаційної безпеки. Темпи науково-технічного прогресу сьогодні вимагають від майбутніх фахівців уміння адаптуватися в умовах швидкої зміни інформаційних технології, поповнювати протягом короткого часу свої професійні знання та постійно підвищувати професійну компетентність.

Система навчання, що відповідає таким вимогам, повинна включати інноваційні технології, які забезпечили б відповідний рівень мобільності фахівця щодо оволодіння професійно значущими знаннями захисту інформаційного простору, вміннями та формування необхідних навичок.

Без використання інформаційного захисту технологій навчання у ВВНЗ застосування у практичній діяльності відповідних знань є неможливим. Тому перш ніж застосовувати на практиці теоретичні знання про навчання, їх необхідно технологізувати. Будь-якому викладачу необхідна система знань про інформаційний захист навчального процесу, яка подана на технологічному рівні.

На початку 2000-х років з'явився термін інформаційні технології захисту навчання (ІТЗН). В. М. Монахов дає наступне тлумачення цьому терміну: "Під новими інформаційними технологіями захисту навчання ми будемо розуміти систему сучасних інформаційних методів і засобів цілеспрямованого створення, збирання, зберігання, опрацювання, подання та використання даних і знань в навчанні та систему захисту її функціонування, що спрямована на удосконалення навчального процесу з найменшими затратами" [4].

ІТЗН в освітньому процесі використовують засоби інформатизації навчання (насамперед, це комп'ютер), причому використовують як засіб управління учбовою діяльністю. Комп'ютерні технології навчання – це, насамперед, комп'ютер та комп'ютерні навчальні програми. Це допомагає кращому засвоєнню матеріалу, завдяки використанню різних видів пам'яті: зорової, слухової, асоціативної. При розробці таких систем особлива увага повинна приділятися захисту даних від несанкціонованого ко-

піювання, від модифікації програмного коду в інтересах користувача, приховування від користувача частини даних, збереження паролів, захист від перевантажень, а також ряду організаційних і технічних питань.

Практика показує, що корпоративна мережа ВВНЗ являє собою досить живий організм, і важко заздалегідь визначити ту ділянку мережі, яка потребує підвищеного рівня контролю з боку адміністратора безпеки. Необхідність встановлення стаціонарних аналізаторів в конкретних точках корпоративної мережі визначається у відповідності з політикою безпеки, прийнятої у ВВНЗ.

Захист інформації освітнього процесу можна розглядати за чотирма напрямками: апаратний захист, програмний захист, захисні перетворення організаційний захист [1, 2].

Важливою проблемою в області організації навчального процесу є і слабка захищеність освітнього програмного забезпечення від «злому» з метою доступу до правильних відповідей комп'ютерних тестів, і підробці результатів контролю [3]. Ця проблема випливає з того, що в основному сучасні контролюючі системи будуються на антропоморфному принципі, суть якого полягає у використанні пам'яті комп'ютера для зберігання еталонних відповідей разом із завданнями. Як правило, вони шифруються, але, як показує практика, їх завжди можна розшифрувати. Ця проблема особливо гостро постала з потребою надання віддаленого доступу до даних, де зовнішній контроль знань здійснюється в основному комп'ютером за відсутності викладача.

Існує також проблема захисту навчального програмного забезпечення від модифікації його коду, з метою зміни алгоритму оцінювання результатів тестування, зміна часу для проходження тестування або іншого коду. Слабка захищеність від «злому» будь-яких антропоморфних контролюючих систем створює труднощі при проведенні контролю.

З вище викладеного випливає, що проблема захисту освітнього процесу дійсно актуальна і вимагає до себе уваги. При цьому, на даний момент напрацювань у цій галузі досить мало. Велика частина системи захисту лежить поза сферою можливості програмного забезпечення і вимагає відповідної адміністративної організації та контролю. Що говорить про необхідність розробки теоретичних і практичних методик застосуванням систем захисту даних. Цей розділ, мабуть, можна віднести до педагогічних наук. Але сама по собі педагогіка не здатна, без технічної підтримки побудувати таку систему інформаційного захисту, яка б відповідала всім вимогам, як з боку якості навчання, так і з точки зору організації контролю при такому навчанні. А, отже, основним завданням інформаційних технологій захисту інформаційної безпеки освітнього процесу у вищих військових навчальних закладах є побудова необхідної технічної бази, для подальшого їх використання в безпечній діяльності ВВНЗ.

**Література**

1. Гейша О. О. Методики забезпечення захищеності систем дистанційної освіти : дис... канд. тех. наук: 05.13.06 / Олександр Олександрович Гайша. – К., 2008. – 165 с.

2. Турко Ю. М. Проблеми захисту авторського права в ситтемах дистанційної освіти / Ю.М. Туркот, О. С. Ворокін // Всеукраїнський конкурс студентських наукових робіт з природничих, технічних та гуманітарних наук у 2011/2012.

3. Герасименко І.В. Технології захисту даних в системі підтримки навчання // Черкаський державний технологічний університет, м. Черкаси, Україна.

4. Монахов В.М. Что такое новая информационная технология // Математика в школе. – 2000. – № 2. – С. 47-52.

*УДК 351.862.4*

**Устименко О.В.**
кандидат наук з державного управління,
старший науковий співробітник
НУОУ імені Івана Черняховського

# МЕРЕЖА СИТУАЦІЙНИХ ЦЕНТРІВ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ ЯК ЄДИНИЙ ОРГАНІЗАЦІЙНО-ТЕХНІЧНИЙ КОМПЛЕКС, В УМОВАХ КРИЗОВОГО РЕАГУВАННЯ У СФЕРІ ОБОРОНИ

В чинних нормативно-правових документах зазначено, що “для вдосконалення державного управління сектором безпеки і оборони, своєчасного виявлення загроз національній безпеці України передбачається:

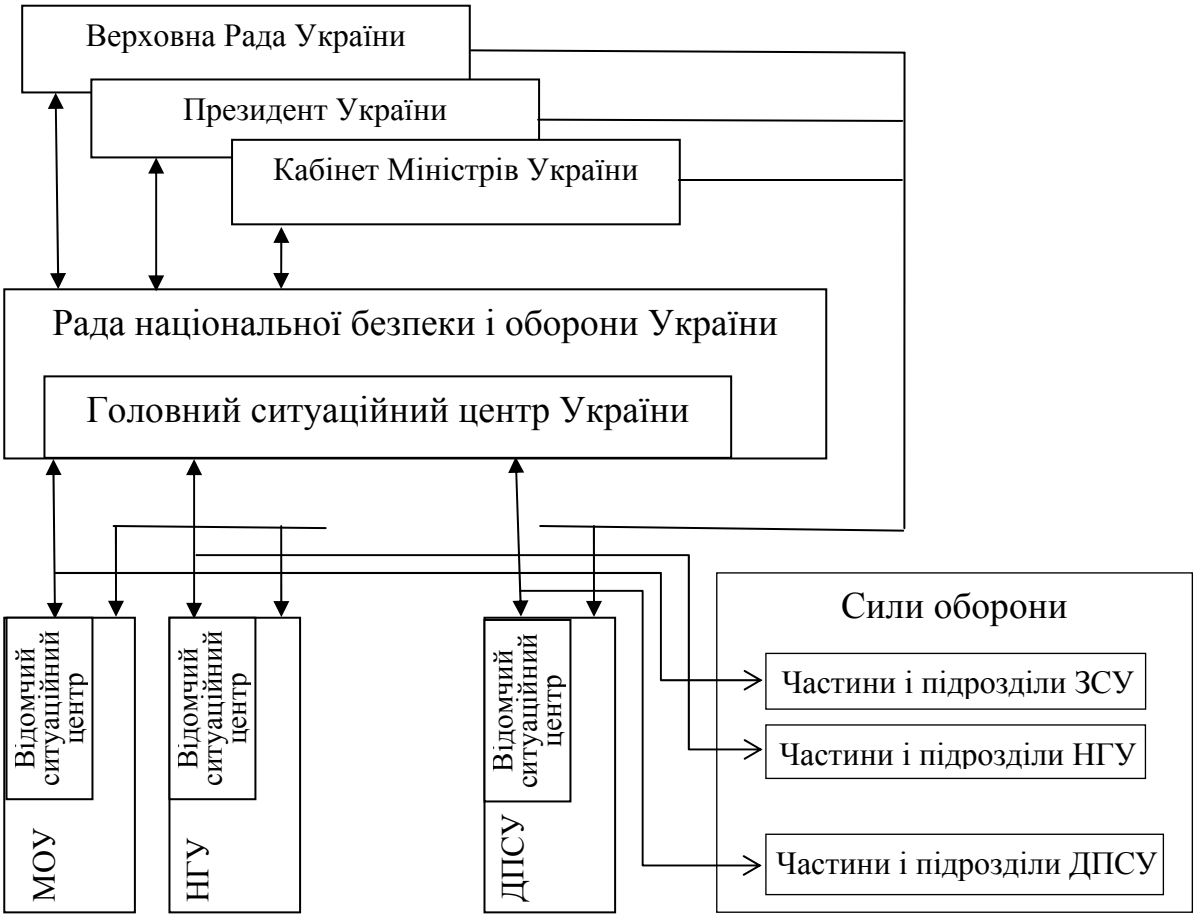
підвищити рівень стратегічного управління у сфері забезпечення національної безпеки шляхом створення мережі ситуаційних центрів, які взаємодіятимуть між собою та з Головним ситуаційним центром України;

забезпечити кіберзахист мережі ситуаційних центрів держави, впровадити ефективні заходи і засоби захисту інформації ситуаційних центрів у процесі її отримання, оброблення, передачі та збереження …” [1].

Ситуаційний центр це організаційно-технічна система, яка забезпечує збір, накопичення, обробку і аналіз інформації (моніторинг), необхідної для прогнозування, планування та прийняття рішень у сфері національної безпеки і оборони [2]. Мережа ситуаційних центрів сектору безпеки і оборони формуватиметься як єдиний організаційно-технічний комплекс, оснащений цільовим апаратно-програмним забезпеченням та унікальним інформаційно-комунікаційним обладнанням, що дасть змогу підвищити якість інформаційно-аналітичного забезпечення та мінімізувати строки для прийняття важливих управлінських рішень [1]. Стратегічним оборонним бюлетенем України передбачається, що до кінця 2020 року буде

“створено систему ситуаційних центрів для сектору оборони на базі захищених інформаційно-телекомунікаційних систем” [3]. Планується, що результати моніторингу будуть подаватися до Апарату Ради національної безпеки і оборони (РНБО) України щоквартально. Водночас, у разі виявлення під час моніторингу раптових змін індикаторів, які свідчать про кризу - різке погіршення стану національної безпеки України, орган державної влади зобов’язаний невідкладно надати результати моніторингу до Апарату РНБО України [4].

На нашу думку доцільно передбачити можливість, щоб у разі критичного рівня національної безпеки України відповідні сигнали з ситуаційних центрів надходили не лише до Апарату РНБО України та керівництва держави, а й до частин і підрозділів сил оборони, активізуючи механізми приведення у вищі ступені бойової готовності – див. рис. 1.




Частини і підрозділи ЗС України (сил оборони) приводяться у вищі ступені бойової готовності бойовими розпорядженнями, які закладені в відповідних пакетах. Сигнали на їх розпечатування доводяться з пунктів управління ГШ ЗС України.

Як свідчить досвід, під час захоплення Російською Федерацією Криму та міста Севастополь у 2014 році система стратегічного керівництва обороною знаходилася в колапсі, а механізми приведення у вищі ступені бойової готовності частин і підрозділів ЗС України виявилися недієздатними. В частини і підрозділи сил оборони не надходили адекватні ситуації

вказівки і розпорядження, сигнали на приведення у вищі ступені бойової готовності. Як бачимо зазначена система потребує удосконалення. При цьому необхідно врахувати загрози: деструктивного впливу на систему військового управління; порушення роботи штатної системи приведення у вищі ступені бойової готовності частин і підрозділів сил оборони; політичної кризи, що може спричинити колапс системи державного управління в цілому тощо.

Отже вже у процесі створення системи ситуаційних центрів складових сектору безпеки і оборони доцільно завчасно передбачити можливість їх використання як резервної системи приведення у вищі ступені бойової готовності частин і підрозділів сил оборони.

**Література**

1. Концепція розвитку сектору безпеки і оборони України: Указ Президента України від 14 березня 2016 року № 92 "Про рішення РНБО України від 4 березня 2016 року" URL: http://www.president.gov.ua/documents/922016-19832 (дата звернення 01.03.2018).

2. Устименко О. В. Моніторинг національної безпеки як складова механізму стратегічного планування // Вісник НАДУ. 2016. № 4. С. 50–55.

3. Стратегічний оборонний бюлетень України: Указ Президента України від 06.06.2016 № 240 Про рішення РНБО України від 20 травня 2016 року "Про Стратегічний оборонний бюлетень України" // Офіційне інтернет-представництво Президента України. URL: http://www.president.gov.ua/documents/2402016-20137 (дата звернення 02.03.2018).

4. Устименко О. В., Пеньковський В.І. Індикатори (показники) стану національної безпеки як результат моніторингу національної безпеки за певний проміжок часу // Науково-інформаційний вісник Академії національної безпеки. 2016. – № 1-2 (9-10). – С. 62–75.

*УДК 004.056.5*

**Фесенко А.О.**
кандидат технічних наук, асистент
КНУ імені Тараса Шевченка
**Оксіюк О.Г.**
доктор технічних наук, зав. кафедрою, професор
КНУ імені Тараса Шевченка

## ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БЕЗПІЛОТНИХ АВІАЦІЙНИХ СИСТЕМ

Останнім часом, особливо з початком АТО, помітно пожвавилось використання безпілотних літальних апаратів (БпЛА). Причиною цього є привабливість цього виду техніки для ефективного використання в різних сферах діяльності. Це насамперед пов'язана з наявністю ряду переваг,

якими володіють безпілотні авіаційні системи - це: порівняна дешевизна, порівняно не великі розміри літального апарату і, відповідно, забезпечення непомітності переміщення, виключення ризику людських втрат або шкоди здоров'ю при виконанні задач. Але, при використанні БпЛА виникає ряд проблем, пов'язаних, головним чином, з безпекою експлуатації безпілотних літальних систем, а саме - проблем забезпечення інформаційної безпеки. Основною причиною загроз, які можуть виникнути при використанні дистанційно пілотованих БпЛА є втрата контролю над самим безпілотником, і, як наслідок, втрата самого літального апарату, а також можлива втрата цінної інформацію, яку фіксував БпЛА, а також його технічне оснащення.

Безпілотна авіаційна система (БАС) - комплекс технічних засобів з БпЛА, в який, крім літальних апаратів, входить наземний пункт дистанційного керування, канали зв'язку і управління, а також організаційна штатна структура, яка здійснює управління комплексом і забезпечує його функціонування.

Дистанційно пілотований літальний апарат (ДПЛА) - літальний апарат, безперервне управління всіма функціями і пристроями якого здійснюється тим чи іншим способом з пункту управління. Таким чином, в БАС з ДПЛА всі функції управління функціональною поведінкою літального апарату віддані оператору, який знаходиться в наземному пункті управління.

Прикладом недосконалої системи інформаційної безпеки було повідомлення в світових ЗМІ, які посилаючись на інформацію іранських джерел, повідомили, що засоби радіоелектронної боротьби Ірану посадили на сході країни американський розвідувальний безпілотник RQ-170 Sentinela, а вже за 4 дні Іран оприлюднив короткий відеозапис, з якого ясно, що апарат знаходиться в руках іранських військових. Управління цим БпЛА здійснювалося за допомогою супутника, причому канал управління був зашифрований, а ключі шифрування змінювалися один раз в декілька секунд. Для безпосереднього злому такого сигналу треба було б дуже багато часу і потужні обчислювальні системи. Однак, іранські військові за допомогою комплексу радіоелектронної боротьби заглушили канал управління RQ-170. Втративши сигнал, безпілотник перейшов в автоматичний режим і, відповідно до налаштувань, попрямував на базу ВПС США в Афганістані за сигналами GPS. Вважається, що іранські військові зуміли успішно підмінити або спотворити навігаційний сигнал GPS, в результаті чого RQ-170 збився з курсу і здійснив посадку на території Ірану. Через кілька місяців іранці оголосили, що зуміли зламати бортові системи американського апарату і розгорнути серійне виробництво його копій.

Основними проблемами при забезпеченні інформаційної безпеки БАС з ДПЛА є:

- формулювання відповідних політик безпеки, які будуть враховувати створення комплексних систем захисту з використанням невеликих габаритів і малого енергоспоживання;

- виконання жорстких вимог щодо стійкості до зовнішніх впливів;

- створення системи захисту для обробки інформації, що містить відомості, що становлять державну таємницю, з урахуванням високого ступеня ймовірності компрометації;

- вирішення питань захищеного єдиного управління декількома БпЛА;

- вирішення проблеми стандартизації засобів захисту інформації при застосуванні БпЛА в багатоцільових бойових системах.

Теперішній стан справ щодо забезпечення інформаційної безпеки у вітчизняних БАС з ДПЛА можна охарактеризувати як неприпустимо низький, хоча з початком АТО в нашій країні є позитивні зміни в цьому напрямку, але створення відповідних надійно захищених інформаційних підсистем управління є нагальним питанням. Швидке і якісне вирішення поставлених проблем захисту інформації в вітчизняних БАС можливо при тісній взаємодії фахівців з БАС і компетентних фахівців з інформаційної безпеки.

**Література**

1. Правила виконання польотів безпілотними авіаційними комплексами державної авіації України, затверджені Наказом Міністерства оборони України від 08.12.2016 № 661.

2. Проценко М. М. Аналіз та варіанти побудови безпілотних авіаційних комплексів — Вісн. ЖДТУ. – 2012. – № 2. – С. 114.

3. Рэндал У.Биард, Тимоти У.МакЛэйн. Малые беспилотные летательные аппараты: теория и практика. – Москва: Техносфера, 2015. – 312 с. – (Мир радиоэлектроники).

4. Общие виды и характеристики беспилотных летательных аппаратов : справ. Псоб. / А.Г.Гребеников, А.К.Мялица, В.В.Парфенюк и др. – Х. : Нац.а эрокосм. ун-т "Харьк. авиац. ин-т", 2008. – 377 с.

5. Корченко А.Г., Ильяш О. С. Обобщённая классификация беспилотных летательных аппаратов // Збірник наукових праць Харківського національного університету Повітряних Сил. – 2012. – № 4. – С. 27-36.

*УДК 341.824:338.47 (043.2)*
**Хлань В.Г.**
кандидат технічних наук,
старший науковий співробітник
Український науково-дослідний інститут
спеціальної техніки та судових експертиз СБ України
**Драчук С.М.**
кандидат юридичних наук
Український науково-дослідний інститут
спеціальної техніки та судових експертиз СБ України

# СУЧАСНІ АСПЕКТИ РОЗВИТКУ ЄВРОПЕЙСЬКОЇ ТА АМЕРИКАНСЬКОЇ ІНІЦІАТИВ CBRN В УКРАЇНІ В КОНТЕКСТІ МІЖНАРОДНОЇ ВЗАЄМОДІЇ У СФЕРІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Сьогодні у світовому безпековому середовищі досить уживаними стали абревіатура та словосполучення: CBRN risks, CBRN incident, CBRN agents, CBRN materials, CBRN policy, CBRN information, CBRN structure тощо.

Ініціативна програма Європейського Союзу щодо запобігання хімічним, біологічним, радіологічним та ядерним ризикам EU CBRN Centre of Excellence Initiative (EU CBRN CoE) почала діяти з 2010 року. Метою даної ініціативи є зменшення загроз та ризиків, пов'язаних із використанням хімічних, біологічних, радіологічних та ядерних матеріалів шляхом поглиблення інституційного співробітництва між країнами ЄС з одного боку, та країнами не членами ЄС з іншого [1].

Останнім часом до зазначеної програми все частіше стали додавати ще одну літеру CBRNe, що означає включення до неї ризиків, пов'язаних з застосуванням саморобних вибухових пристроїв (explosive). Американський аналог EU CBRN CoE має назву US Chemical, Biological, Radiological, and Nuclear Defense Program (CBRND). Існує також міксований продукт – об'єднаний CBRN Centre of Excellence (CoE) організований НАТО в Чехії, який здійснює тренінги та експертну допомогу для військовиків країн НАТО та країн партнерів [2].

Водночас на нашу думку загальносвітова програма CBRNe має включати також і актуальні як для України так і для ЄС та США кіберзагрози, які по суті пронизують всі інші складові існуючої програми. Тож в найближчій перспективі існує потреба у розширенні можливостей реалізації програми CBRNe за рахунок включення до неї кібернетичних (Cyber) ризиків - CBRNeC.

Актуальність зазначеного питання для України зросте з вступом в дію в 2018 році Закону України «Про основні засади забезпечення кібербезпеки України», в якому визначено, що забезпечення кібербезпеки в Україні ґрунтується серед іншого на принципі міжнародного співробітництва з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в терористичних, воєнних, інших протиправних цілях [3].

Механізм співробітництва в рамках програми CBRN CoE, яка охоплює безпекові питання, подібний до інших програм ЄС: Горизонт (наукове співробітництво) та Еразмус (співробітництво в сфері освіти). Формат співробітництва в рамках EU CBRN CoE передбачає, що країни ЄС є донорами, відповідальною структурою від ЄС за реалізацію програм в рамках CBRN є Директорат з питань розвитку і співробітництва. Відповідальною особою від ЄС за реалізацію цілей програми CBRN є заступник Генерального директора Єврокомісії з питань розвитку і співробітництва - представник в Адміністративній Раді Українського науково-технологічного центру (УНТЦ) від ЄС. Задля реалізації цілей CBRN, Директоратом з питань розвитку і співробітництва було створено Головний центр CBRN в Брюсселі (Center of Excellence). Він координує роботу Регіональних секретаріатів (Regional Secretariats). Існує 8 таких секретаріатів: секретаріати Середнього Сходу; Південно-Східної та Східної Європи; Північної Африки; Африкано-Атлантичного регіону; Перської затоки; Центральної Азії; Південно-Східної Азії; Східної і Центральної Африки. Регіональні секретаріати, в свою чергу, керують роботою національних представників (National focal point, NFP). Для реалізації програм в рамках CBRN NFP формують національні команди (National team). Відповідно до законодавства ЄС NFP має призначатися на державному рівні кожною країною [4].

Загальнообов'язкові правила як щодо кандидатури представника, так і щодо органу, який його визначає відсутні. Але, оскільки дані питання носять безпековий характер та можуть стосуватися товарів та технологій військового та подвійного призначення або спеціальної техніки, національні представники, на нашу думку, мають формуватися з числа державних службовців (військовослужбовців), які представляють інтереси відповідних органів державної влади сектору безпеки та оборони України.

На сьогоднішній день в Україні немає єдиного налагодженого механізму реалізації проектів в рамках програми EU CBRN CoE. Такі проекти здійснюються через Український науково-технологічний центр (УНТЦ) та через програму НАТО «Наука заради миру і безпеки» (SPS Programme). Крім держав, до співпраці в рамках програми EU CBRN CoE залучаються близько 60 (станом на 2017 рік) організацій-партнерів (implement partners) [5].

В програмі НАТО «Наука заради миру і безпеки» CBRN виокремлено в один із пріоритетних напрямів поруч з такими напрямами як: контртероризм, енергетична безпека, кібернетичний захист, екологічна безпека. Так, заходи співпраці НАТО з Україною по лінії CBRN включають наукові дослідження, спрямовані на створення відповідних засобів захисту, курси підготовки та робочі семінари, тренінги, конференції тощо. У сфері боротьби з тероризмом наукові дослідження спрямовуються на створення новітніх антитерористичних засобів у тому числі інформаційних технологій, а співробітництво у сфері кібербезпеки спрямовується на розробку дієвих заходів захисту критичної інфраструктури [6].

Оскільки програма EU CBRN CoE охоплює широкий спектр безпекових питань, в тому числі й у сфері науки, пропонуємо почати розробку національного плану дій з метою подальшого підписання відповідної міжнародної угоди та після цього ініціювати зміни до постанови Кабінету Міністрів України від 13 вересня 2002 р. № 1371 «Про порядок участі центральних органів виконавчої влади у діяльності міжнародних організацій, членом яких є Україна». В зазначеній постанові пропонуємо визначити СБУ одним із органів державної влади, відповідальними за виконання зобов'язань, що випливають із співробітництва України в рамках програми EU CBRN CoE. Крім цього, існує нагальна потреба у розробці Плану дій для України (Action plan for Ukraine) щодо співробітництва з CBRN, який має стати основою для початку міжнародної співпраці на взаємовигідних умовах.

**Література**

1. CBRN Centres of Excellence [Електронний ресурс]. - Режим доступу: http://www.unicri.it/topics/cbrn/coe/.

2. NATO troops training for a CBRN emergency [Електронний ресурс]. - Режим доступу: https://www.cbrneportal.com/cbrn-defence-capabilities-in-us-and-europe/.

3. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII // Офіційний Вісник України 2017, 91 від 21.11.2017, ст. 2765.

4. CBRN Centres of Excellence [Електронний ресурс]. - Режим доступу: http:www.cbrn-coe.eu.

5. Science end Technology Center in Ukraine. Annual Report. [Електронний ресурс]. - Режим доступу: https://www.stcu.int.

6. The NATO Science for Peace and Security (SPS) Programme [Електронний ресурс]. – Режим доступу : http:// www.nato.int/science.

*УДК 34.096*
**Хом'яков Д.О.**
кандидат юридичних наук,
начальник науково дослідної лабораторії
проблем права воєнної сфери
ВІКНУ імені Тараса Шевченка

# НОРМАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Загальновизнано, що науково-технічний прогрес неможливий без широкомасштабного впровадження в суспільне життя та управлінську діяльність держави, у різні сфери науки, техніки і виробництва сучасних інформаційних технологій, електронно-обчислювальної техніки, інформаційних мереж і мереж електрозв'язку.

В сучасних умовах розвитку інформаційного суспільства активно розвивається інформаційна сфера, яка поєднує в собі інформацію, інформаційну інфраструктуру, зокрема інформаційні мережі, інформаційні відносини між суб'єктами цієї сфери, що складаються у процесі збирання, формування, розповсюдження і використання інформації. Інформаційні відносини займають чільне місце у формуванні інформаційної політики держави, в житті сучасного суспільства, а також в діловому та в особистому житті кожної людини. Це, в свою чергу, обумовлює необхідність розвитку й удосконалення правових засобів регулювання суспільних відносин у сфері інформаційної діяльності. Зрозуміло, що в демократичній правовій державі такі відносини мають базуватися на сучасній нормативно-правовій базі, що регулює діяльність в інформаційній сфері.

Законодавчі норми у цій сфері істотно впливають на нормативно-правове регулювання відносин між суспільством, його членами та державою, між фізичними та юридичними особами тощо. Тобто на сучасному етапі інформаційні відносини виступають, з одного боку, зовнішнім проявом будь-яких відносин у житті країни, суспільства та громадян, з іншого - тими підвалинами, на яких формується законодавство в інших сферах їх існування.

Під час створення сучасної та ефективної системи забезпечення інформаційної безпеки істотного значення набуває наявність відповідної нормативно-правової бази, без якої неможливо охопити усі сфери життєдіяльності суспільства в рамках єдиного правового поля, розробити загальнонаціональну концепцію розвитку держави й ефективно реалізовувати політику національної безпеки в інформаційній сфері. Це означає, що всі без винятку дії щодо захисту й реалізації національних інтересів України в будь-якій сфері й на будь-якому рівні мають передусім спиратися на чин-

не законодавство України, підтверджувати законність функціонування системи національної безпеки. Водночас у демократичному суспільстві такі дії суб'єктів забезпечення національної безпеки повинні відповідати національному законодавству, а також загальновизнаним міжнародно-правовим нормам та бути під контролем громадськості.

З огляду на викладене законність функціонування є однією з головних вимог до системи забезпечення інформаційної безпеки. Ця законність повинна базуватися на сукупності законів і підзаконних нормативних актів, які спрямовані на створення необхідних умов для захисту національних інтересів в інформаційній та інших сферах життя країни.

Так, зокрема, наявність необхідної та достатньої нормативної бази і механізмів її реалізації та контролю дозволяє системі забезпечення національної безпеки України ефективно функціонувати в сучасних умовах.

Найбільш актуальним завданням у сфері забезпечення інформаційної безпеки держави на сьогодні є формування відповідних положень національного інформаційного законодавства щодо правового забезпечення діяльності в інформаційній сфері відповідних суб'єктів, у першу чергу державних органів, на які державою покладено виконання пов'язаних з цим функцій.

Важливу роль у системі законодавства України з питань національної безпеки відіграють акти нормативного і директивного характеру місцевих органів влади - рішення з питань забезпечення національної безпеки (про боротьбу з наслідками стихійних лих, техногенних аварій і катастроф, з епідеміями, про підтримання громадського порядку тощо), які є обов'язковими для виконання всіма підприємствами, установами й організаціями, а також посадовими особами і громадянами на території, підпорядкованій цьому органу влади.

**Література**

1. Красноступ Г.М. Забезпечення основних принципів діяльності держави в інформаційній сфері /Г.М. Крас- ноступ. [Електроннийресурс]. Режим доступу: http://www.minjust.gov.ua/11922.

2. Указ Президента України від 08.07.2009 № 514/2009 «про Доктрину інформаційної безпеки України». [Електроннийресурс]. Режим доступу: http://zakon2.rada.gov.ua/laws/show/514/2009.

3. Про інформацію: Закон України від 02.10.1992 № 2657-XII //Відомості Верховної Ради. - 1992. - № 48. - Ст. 650.

4. Про Концепцію Національної програми інформатизації: Закон України від 04.02.1998 № 75/98-ВР // Відомості Верховної Ради. -1998. - № 27-28. - Ст. 182.

5. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 рр.: Закон України від 09.01.2007 № 537-У // Відомості Верховної Ради. - 2007. - № 12. - Ст. 102.

6. Розпорядження Кабінет Міністрів України від 15 травня 2013 р. № 386-р. «Про схвалення Стратегії розвитку інформаційного суспільства в Україні». [Електронний ресурс]. Режим доступу:

7. Окинавская хартия глобального информационного общества. (Окинава, 22 июля 2000 года). [Електроннийресурс]. Режим доступу: http://zakon4.rada.gov.ua/laws/show/998_163.

*УДК 378.147*

**Черних Ю.О.**
кандидат технічних наук, доцент,
Військовий інститут КНУ імені Тараса Шевченка
**Черних О.Б.**
НУОУ імені Івана Черняховського

## ТАКСОНОМІЯ БЛУМА ЯК ОСНОВНИЙ ЗАСІБ ФОРМУВАННЯ КОМПЕТЕНЦІЙ ФАХІВЦЯ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Сьогодні одною з важливих компетенцій фахівця, який опікується питаннями інформаційної безпеки держави, є навички використання інформаційно-комунікаційних технології. Для цього важливо, починаючи вже з першого курсу, розвивати у курсанта навички мислення високого рівня, творчий підхід до справи, уміння розв’язувати складні проблеми та приймати самостійні рішення. Тому завдання викладача сформувати у курсанта такі знання та вміння, які допоможуть їм знайти своє місце у світі високих інформаційних технологій.

Мислення високого рівня вимагає від тих, хто навчається, наступних важливих особистих якостей: вміння визначати пріоритети; вміння приймати індивідуальну відповідальність; наявність культури роботи з інформацією; вміння проводити оцінку мисленнєвих процесів. Для цього під час проведення навчальних занять необхідно: реалізувати навчання, засноване на запитаннях; застосовувати технології особистісно-орієнтованого навчання; використовувати різноманітні способи оцінювання навчальних досягнень; широко застосовувати завдання на класифікацію та систематизацію.

Найбільш відомою моделлю, що описує процес навчання та мислення, є таксономія Бенджамина Блума (Bloom’s Taxonomy) [1], яка включає до себе шість навиків мислення, що структуровані від самого базового до самого просунутого рівня. Б. Блум визначив три області навчальної діяльності:

- когнітивна (Cognitive domain): розумові навики (Mental skills);
- афективна (Affective domain): область почуття та емоцій (Attitude);

• психомоторна (Psychomotor): фізичні вміння і навики (Skills).

До цілей першої, когнітивної групи входять такі, які передбачають запам'ятовування і відтворення вивченого матеріалу, а також розв'язання проблем, у ході яких необхідно переосмислити наявні знання, будувати їх нові об'єднання, структури, створювати нові знання.

Другу групу цілей (афективна, емоційно-ціннісна сфера) становлять цілі формування емоційно-особистісного ставлення до навколишнього світу. Вони виражаються через сприймання, нахили, здібності, переживання почуттів, формування відношення, його осмислення і вияв у діяльності.

Цілі навчання психомоторної сфери становлять третю групу. Вони включають ті чи інші види моторної (рухливої) діяльності. Це навички письма, мовні навички, фізичні та трудові навички.

Використання чіткої, впорядкованої системи цілей навчання, на думку Б. Блума, дуже важливе для побудови навчального процесу в зв'язку з тим, що, по-перше, знаючи цілі навчання, викладач впорядковує їх, визначає першочергові, базові, порядок і перспективу подальшої роботи; по-друге, знання викладачем конкретних цілей дає можливість пояснити курсантам орієнтири в їх спільній роботі; по-третє, чітке формулювання цілей, які виражені через результати діяльності, піддається надійній і об'єктивній оцінці.

Розглянемо лише когнітивну групу цілій. Цілі навчання можуть бути виражені через такі елементи засвоєння (їх ще називають елементами таксономії Б. Блума): знання, розуміння, застосування, аналіз, синтез і оцінка.

Більшість процесів мислення, що характерні для навчальної діяльності, відповідають рівням «Знання» та «Розуміння», тому вони є найбільш розповсюдженими з розумових вмінь. Вони є базою або фундаментом, на якому будується всі розумові вміння більш високого рівня. З кожним наступним рівнем розумові вміння становляться більш складними та використовуються ріже. Для формування навиків мислення високого рівня необхідно використовувати рівні: «Аналіз», «Оцінка», «Синтез».

Як у будь якої теоретичної моделі, у таксономії Б. Блума є свої сильні та слабкі сторони. Основною перевагою є те, що мислення представлено в ній у структурованій і доступній для практиків формі. Ті викладачі, які користуються рекомендаціями з складання питань, що відносяться к різним рівням таксономії Б. Блума, краще вирішують завдання щодо формування навиків мислення високого рівня у тих, хто навчається, ніж ті викладачі, які це не використовують. Таксономії відіграють велику роль у теорії навчання. Вони важливі тому, що дозволяють вірно ставити цілі в навчанні, вірно формулювати проблеми та ставити завдання слухачам, визначати оціночні інструменти, що адекватні цілям.

Для того, щоб сформувати у курсантів навики мислення високого рівня викладач повинен використовувати наступні практичні рекомендації:

забезпечити розуміння того, які навики мислення необхідні курсанту; навчити курсанта формулювати питання; навчити виявляти причини явищ; навчити мистецтву аргументації; навчити оцінювати результати своєї діяльності. Гостра необхідність непросто навчати курсантів, а й розвивати їх мислення, творчій потенціал, генерування ідей та побудову логічних зв'язків вимагає від викладача сучасних поглядів на заняття, що він організує, потребує ретельної та продуманої підготовки на декілька навчальних занять вперед.

Використання чіткої, впорядкованої системи цілей навчання, дуже важливе для побудови навчального процесу в зв'язку з тим, що, по-перше, знаючи цілі навчання, викладач впорядковує їх, визначає першочергові, по-друге, знання викладачем конкретних цілей дає можливість пояснити курсантам орієнтири в їх спільній роботі; по-третє, чітке формулювання цілей, які виражені через результати діяльності, піддається надійній і об'єктивній оцінці. Таксономія Б. Блума спрямована на практичну допомогу викладачу, який розуміє важливість завдання щодо сформування у курсантів навиків мислення високого рівня.

**Література**

1. Bloom B.S. Taxonomy of educational objectives: The classification of educational goals. - New York: Longman. 2001. – 156 с.

*УДК 004.056.5*

**Шевченко А.С.**
кандидат технічних наук
Військовий інститут телекомунікацій
та інформатизації імені Героїв Крут

## МЕХАНІЗМИ ВИЯВЛЕННЯ КІБЕРНЕТИЧНИХ АТАК НА ОСНОВІ КОНТРОЛЬНИХ КАРТ ШУХАРТА

Виявлення та попередження кібернетичних атак є досить актуальним завданням в умовах загострення кібербезпеки в усьому світі. На сьогоднішній час для виявлення кібернетичних атак використовується безліч методів, які покладені в основу роботи систем запобігання вторгнень (СЗВ). Значний клас методів виявлення атак ґрунтується на статистичному аналізі трафіка та процесів в інформаційно-телекомунікаційних системах (ІТС), які здійснюють виявлення аномальних відхилень на основі аналізу параметрів.

Одними з таких методів є параметричні методи реєстрації змін характеристик на основі контрольних карт Шухарта. Дані методи мають широкий спектр застосування під час контролю якості виробництва.

Методи на основі контрольних карт Шухарта ґрунтуються на статистичному виявленні змінити параметрів трафіка та характеристик ІТС: обсягу трафіка, кількості та частоті запитів, часу затримки та обробки тощо.

Суть використання контрольних карт полягає в аналізі вибірок параметрів системи та виявлення відхилення від центральної лінії (*CL*). Центральна лінія визначається на основі середнього значення параметра – $\mu_0$. Контрольна карта Шухарта має дві статистичні контрольні межі, які розміщуються по обидві сторони від центральної лінії: верхня контрольна границя – $U_{CL}$, нижня контрольна границя – $L_{CL.}$ Вихід значення параметра за межі контрольних границь сигналізує про вихід системи зі стану статистичної керованості. У випадку застосування методу для виявлення кібернетичних атак, це свідчить про наявність аномалій в ІТС. Верхня та нижня контрольні границі знаходяться від центральної лінії на відстані 3σ, де σ – значення стандартного відхилення процеса. Дане значення вибрано з міркувань мінімізації кількості хибного спрацювання СЗВ (помилок першого роду).

Під час виявлення аномалій в ІТС аналізу підлягає велика кількість даних, які мають кількісні характеристики. У випадку використання кількісних даних прийнято використовувати пару контрольних карт. При використанні вибірки обсягом $n > 10$ та автоматизованої обробки даних ДСТУ ISO 8258-2001 рекомендовано використання карт середніх ($\overline{X}$-карт) та вибіркових стандартних відхилень (*s*-карт). $\overline{X}$-карти використовуються для контролю середнього значення параметра – $\mu_0$. На початку розробки та під час функціонування системи розраховуються середні значення параметра у кожній зі статистичних виборок. *S*-карти використовуються безпосередньо для контролю зміни параметру в межах від $L_{CL}$ до $U_{CL}$. Будь який вихід за контрольні границі розглядається як аномальна подія, передається для подальшої обробки СЗВ та прийняття рішення відносно протидії кібернетичній атаці.

Метод реєстрація аномалій в ІТС на основі контрольних карт Шухарта, як і будь-який статистичний метод виявлення аномалій, має недолік пов’язаний з необхідністю набору статистики даних про значення параметру відносно якого проводиться аналіз. Крім того, використання контрольних карт Шухарта вимагає попереднього визначення середніх значень та контрольних границь параметру. Для адекватного виявлення аномалій, дані значення під час функціонування повинні переглядатись.

На сьогоднішній час не існує універсального методу розпізнавання атак. Методи виявлення аномалій на основі контрольних карт Шухарта є відносно простими в реалізації, і забезпечують високу швидкодію СЗВ в реальному часі. При правильному виборі відстані до контрольних границь дані методи забезпечують досить малу кількість хибних спрацювань, дозволяють виявити тренди та закономірності у зміні параметрів, що забез-

печує виявлення складних та повільних кібератак. Всі ці переваги підкреслюють актуальність застосування контрольних карт Шухарта в алгоритмах роботи сучасних СЗВ.

*УДК 004.056.5*
**Шепета О.В.**
кандидат юридичних наук, доцент
Національна академія СБ України

## ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

У сучасних умовах перед підприємствами та організаціями гостро постає завдання збереження як матеріальних цінностей, так і інформації, у тому числі відомостей, що становлять комерційну або службову таємницю. Тому проблема забезпечення інформаційної безпеки є надзвичайно актуальною на сучасному етапі розвитку інформаційних технологій, який супроводжується введенням інформаційних систем у всі сфери діяльності людини, постійною взаємодією підприємств на теренах саме інформаційного простору [1].

Інформаційна складова безпеки підприємницької діяльності полягає у здійсненні ефективного інформаційно-аналітичного забезпечення господарської діяльності підприємства. Відповідні служби суб'єктів господарської діяльності виконують при цьому певні функції, які в сукупності складають процес створення та захисту інформаційної складової безпеки.

До таких функцій належать:

– збирання усіх видів інформації, що має відношення до діяльності суб'єкта господарювання (щодо всіх видів ринків, політичних події і тенденцій макроекономічного розвитку світової та національної економік, корисної науково-технічної інформації);

– аналіз одержуваної інформації з обов'язковим дотриманням загальноприйнятих принципів (систематизації, безперервності надходження, усебічного характеру аналітичних процесів) і методів (локальних із специфічних проблем, загальнокорпоративних) організації робіт;

– прогнозування тенденцій розвитку науково-технологічних, економічних і політичних процесів на підприємстві (в організації), в країні та у світі стосовно конкретної сфери бізнесу (діяльності), а також показників, яких необхідно досягти суб'єкту господарювання (наприклад, фінансові прогнози, прогнози об'єктів виробництва й технологічного розвитку);

–оцінка рівня економічної безпеки за всіма складовими та в цілому, розробка рекомендацій для підвищення цього рівня на конкретному підприємстві;

– інші види діяльності з розробки інформаційної складової економічної безпеки (зв'язки із громадськістю, формування ділової репутації та привабливого іміджу фірми, захист таємної та конфіденційної інформації).

На підприємство постійно надходять потоки інформації, яку поділяють на:

1) відкриту офіційну;

2) вірогідну нетаємну, одержану через неформальні контакти працівників з носіями такої інформації;

3) вірогідну таємну, отриману через неформальні контакти працівників з носіями такої інформації.

Дослідження показують, що 90-95% усієї необхідної інформації можна отримати легально, вивчаючи виступи учасників різноманітних наукових і виробничих форумів, відкриті публікації, експонати різних виставок, ярмарків, презентацій, дані товарних і фондових бірж, оголошення про наявні вакансії, конкурси на заміщення посади тощо [2]. Тому на підприємстві слід запровадити правові норми захисту таємниць, а також систему контролю за збереженням комерційної таємниці. Оперативна реалізація заходів з розроблення та охорони інформаційної складової безпеки підприємства здійснюється послідовним виконанням певного комплексу таких робіт:

– збирання різних видів необхідної інформації;

– оброблення та систематизація добутої інформації;

– аналіз цієї інформації;

– захист інформаційного середовища підприємства, що традиційно охоплює:

1) заходи захисту від промислового шпигунства з боку конкурентів чи інших юридичних та фізичних осіб;

2) технічний захист приміщень, транспорту, кореспонденції, переговорів, різної документації від несанкціонованого доступу зацікавлених юридичних і фізичних осіб до закритої інформації;

3) збирання інформації про потенційних ініціаторів промислового шпигунства та проведення необхідних запобіжних заходів з метою припинення відповідних спроб;

4) зовнішня інформаційна діяльність.

Отже, інформаційна безпека фактично відображається у ступені захищеності важливої для підприємства інформації від впливу дій випадкового або навмисного характеру, які можуть завдати збитків підприємству. Оптимальним варіантом забезпечення інформаційної безпеки є дотримання систематичного поєднання правових, організаційних та програмно-технічних методів у процесі управління підприємством.

**Література**

1. Сороківська О.А., Гевко В.Л. Інформаційна безпека підприємства: нові загрози та перспективи. [Електронний ресурс]. - Режим доступу: http://nbuv.gov.ua/portal/Soc_Gum/Vchnu_ekon/2010_2_2/032-035.pdf.

2. Бєгун А.В. Інформаційна безпека. - К.: КНЕУ, 2008. - 280 с.

*УДК 343.3*
**Штонда Р.М.**
Військовий інститут телекомунікацій та інформатизації
**Паламарчук Н.А.**
Військовий інститут телекомунікацій та інформатизації
**Островський С.М.**
Центральний науково-дослідний інститут
Збройних Сил України

# СОЦІАЛЬНІ МЕРЕЖІ В ІНТЕРНЕТІ ЯК ІНСТРУМЕНТ ЗАГРОЗИ НАЦІОНАЛЬНІЙ СИСТЕМІ КІБЕРБЕЗПЕКИ УКРАЇНИ

Кіберпростір поступово перетворюється на окрему, поряд із традиційними "Земля", "Повітря", "Море", "Космос", сферу ведення бойових дій [1], а отже і виникнення кібертероризму на сьогодення – це не міфи а реальність. Кібертероризм з кожним роком набуває свого піку слави за допомогою використання комп'ютера як інструмента злочину, існування Інтернету як міжнародного інформаційного простору, в якому перебуває об'єкт злочину та засобу впливу як соціальні мережі в Інтернеті. З кожним роком також зростає роль соціальних мереж в Інтернеті як в світі так і Україні. Усе більше користувачів всесвітньої павутини створюють акаунти у соціальних мережах в Інтернеті. Зареєстровано понад 30 мільйонів українських акаунтів у суспільних інтернет-майданчиках, тому можливо стверджувати, що 75% українців уже зареєстровано у соціальних мережах в Інтернеті [2].

Розглядаючи соціальні мережі в Інтернеті як засобу загрози національній системі кібербезпеки доцільно розглядати наступні інформаційні загрози.

У зовнішньополітичній сфері:

поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України;

зовнішні негативні інформаційні впливи на суспільну свідомість.

У сфері державної безпеки:

негативні інформаційні впливи, спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності і недоторканності кордонів України;

пропаганда сепаратизму за етнічною, мовною та іншими ознаками.

За результатами проведених досліджень виникнення інформаційних та інформаційно-психологічного загроз, які можуть бути реалізовані за допомогою соціальних мереж в Інтернеті, дослідники виділили, що за допомогою соціальних мереж в Інтернеті, можливе наступне [3]:

створення атмосфери бездуховності та аморальності, негативного відношення до культурної спадщини;

маніпулювання суспільною свідомістю і політичною орієнтацією соціальних груп населення країни з метою створення політичної напруженості та хаосу;

дестабілізація політичних відносин між партіями, об'єднаннями і рухами з метою провокації конфліктів, розпалення недовіри, підозрілості, загострення політичної боротьби, провокування репресій проти опозиції, провокація взаємознищення;

зниження рівня інформаційного забезпечення органів влади та управління, інспірація помилкових управлінських рішень;

дезінформація населення про роботу державних органів, підрив їхнього авторитету, дискредитація органів управління;

провокування соціальних, політичних, національних та релігійних зіткнень; ініціювання страйків, масових заворушень та інших акцій економічного протесту;

утруднення прийняття органами управління важливих рішень;

підрив міжнародного авторитету держави, його співробітництва з іншими країнами;

нанесення шкоди життєво важливим інтересам держави в політичній, економічній, оборонній та інших сферах.

Виходячи з цього можливо виділити такі напрямки протидії загрозам національній системі кібербезпеки, які створюють соціальні мережі в Інтернеті: силові методи – закриття серверів; юридично-правові методи – притягнення до кримінальної відповідальності учасників соціальних мереж та провайдерів, які надають послуги доступу до Інтернету; Інтернет – цензура; моніторинг соціальних мереж та протидія методами інформаційного впливу.

Одним із перших суттєвих кроків, було посилення уваги зі сторони держави до діяльності соціальних мереж в Інтернеті, а саме підписання Президентом України Указу № 133/2017. Указом було введено обмежувальні санкції щодо соціальних мереж "Vk.com", "Odnoklassniki.ru" та інших, а провайдерів з надання послуг Інтернету зобов'язали блокувати на системному рівні можливості входження до даних соціальних мереж [4]. Водночас, така увага не повинна порушувати прав людини, що зафіксовані у законодавстві.

Роботу необхідно проводити постійно для зменшення впливу загроз на національну систему кібербезпеки України, необхідно також впроваджувати заходи не зупиняючись на законодавчому рівні, радикально та практично діяти щодо виявлення кібертероризму. Останнім часом користувачі соціальних мереж в Інтернеті усвідомлюючи, що від них залежить стан кібербезпеки держави все менше довіряють соціальним мережам і все

частіше фільтрують інформацію, яку готові довірити мережі, дають неправдиву інформацію або взагалі видаляються з мережі, але слід пам'ятати навіть видалення не дає впевненості, часто інформація зберігається на серверах компанії і може використовуватися в подальшому проти користувача та національної системи кібербезпеки України.

**Література**

1. Указ Президента України від 15 березня 2016 року № 96/2016. Стратегія кібербезпеки України. [Електронний ресурс]. – Режим доступу: http://www.president.gov.ua.

2. Мудра І. Соціальні мережі в Інтернеті як інструмент просування "зараженої" інформації./ І.Мудра. – ISSN 2078-1911. Теле- та радіожурналістика. 2015. – Випуск 14. – С. 208–213.

3. Пелещишин А.М., Гумінський Р.В. Загрози інформаційної безпеки держави в соціальних мережах [Електронний ресурс]. – Режим доступу: http://www.hups.mil.gov.ua.

4. Указ Президента України від 15 травня 2017 року № 133/2016. Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року. "Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)". [Електронний ресурс]. – Режим доступу: http://www.president.gov.ua.

*УДК 342*

**Щербина Л.І.**
кандидат юридичних наук,
старший науковий співробітник,
головний науковий співробітник
науково-організаційного центру
Національна академія Служби безпеки України

## СУБ'ЄКТИ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ В ІНФОРМАЦІЙНІЙ СФЕРІ

Стаття 17 Конституції України [1] відносить забезпечення інформаційної безпеки, як і захист її суверенітету та територіальної цілісності, до найважливіших функцій держави, що реалізовуються через відповідні інституції – насамперед органи державної влади, військові формування й правоохоронну систему, організація і порядок діяльності яких визначається законом.

У вітчизняному законодавстві відсутня єдність поглядів на сутність та зміст інформаційної безпеки: в одних випадках вона розглядається як складова національної безпеки, а в інших – як самостійна та самодостатня

категорія. Не вдаючись до полеміки з цього питання зазначимо, що Законом України «Про основи національної безпеки України» [2], який визначає основні засади державної політики, спрямованої на захист національних інтересів і гарантування в Україні безпеки особи, суспільства і держави від зовнішніх і внутрішніх загроз в усіх сферах життєдіяльності, унормовано визначення терміну «національна безпека». Так, національна безпека представляє собою захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечується сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам у низці сфер, зокрема, й у сфері інформаційної безпеки.

Згідно пп. 3.6, 3.7 Стратегії національної безпеки України, затвердженої Указом Президента України від 26 травня 2015 р. № 287/2015, до актуальних загроз національній безпеці у інформаційній та кібернетичній сферах віднесено: ведення інформаційної війни проти України; відсутність цілісної комунікативної політики держави; недостатній рівень медіакультури суспільства; уразливість об'єктів критичної інфраструктури й державних інформаційних ресурсів до кібератак; фізична і моральна застарілість системи охорони державної таємниці й інших видів інформації з обмеженим доступом.

У ст. 4 Закону України «Про основи національної безпеки України» наведено перелік суб'єктів забезпечення національної безпеки, а в ст. 10 названого закону визначено їх основні функції, які вони здійснюють у межах своїх повноважень. Саме законодавчо визначені повноваження цих суб'єктів є тим критерієм, яким окреслено їх компетенцію у сфері забезпечення інформаційної безпеки.

Так, Президент України, Верховна Рада України, Кабінет Міністрів України та Рада національної безпеки і оборони України здійснюють загальне керівництво, координацію та контроль за діяльністю органів виконавчої влади у сфері національної безпеки і оборони.

Міністерство інформаційної політики України є головним органом в системі центральних органів виконавчої влади, який забезпечує формування та реалізує державну політику у сферах інформаційного суверенітету, державного іномовлення та інформаційної безпеки.

До компетенції Служби безпеки України відноситься контррозвідувальний захист інтересів держави у сфері інформаційної безпеки та забезпечення охорони державної таємниці. Міністерство оборони України забезпечує розроблення сучасних зразків засобів зв'язку, інформатизації та захисту інформації, а також використання інформаційного простору держави і контроль за ним в особливий період. Служба зовнішньої розвідки України та розвідувальний орган МО України здобувають розвідувальну інформацію, на підставі якої прогнозуються і плануються заходи із забезпечення інформаційної безпеки. Серед основних завдань Міністерства внутрішніх справ України визначено запобігання злочинам в інформацій-

ній сфері, їх припинення й розслідування, а також вжиття заходів з усунення причин і умов, що сприяють вчиненню цих кримінальних правопорушень. Діяльність Державної спеціальної служби зв'язку та захисту інформації України зосереджується на формуванні й реалізації державної політики у сфері кіберзахисту державних електронних інформаційних ресурсів, критичної інформаційної інфраструктури та її окремих об'єктів; здійсненні організаційно-технічних заходів із запобігання, виявлення і реагування на кібератаки та усунення їх наслідків; забезпеченні технічних складових інформаційної безпеки (технічний і криптографічний захист інформації; захист інформаційних ресурсів; забезпечення функціонування систем спеціального зв'язку тощо), а також захисті інтересів держави в інформаційній сфері.

Повноваження низки інших суб'єктів забезпечення національної безпеки, до компетенції яких відноситься виконання окремих завдань у сфері інформаційної безпеки, є менш системними.

Підсумовуючи викладене зазначимо, що серед основних завдань сектору безпеки і оборони на середньострокову перспективу, визначених в Концепції розвитку сектору безпеки і оборони України, затвердженій Указом Президента України від 14 березня 2016 р. № 92/2016, чільне місце займає забезпечення інформаційної безпеки, кібербезпеки, охорони державної таємниці та іншої інформації з обмеженим доступом. Їх вирішення вже сьогодні потребує від перелічених суб'єктів забезпечення національної безпеки невідкладного нарощування оперативних спроможностей та рівня готовності до реагування на сучасні виклики й загрози у зазначеній сфері.

**Література**

1. Конституція України. Відомості Верховної Ради України. – 1996. – № 30. – Ст. 141.

2. Закон України «Про основи національної безпеки України» // Відомості Верховної Ради України. – 2003. – № 39. – Ст. 351.

*УДК 654.02*

**Юрх Н.Г.**
Національна академія СБ України
**Блавацька Н.М.**
кандидат технічних наук, доцент
Національна академія СБ України
**Шваб В.К.**
кандидат технічних наук, доцент
ВІКНУ імені Тараса Шевченка

## МАСКУВАННЯ МОВНИХ ПОВІДОМЛЕНЬ

В останні роки захисту мовленнєвих повідомлень конфіденційного характеру приділяється все більша увага. З одного боку це обумовлено ви-

сокою інформативністю мовленнєвих повідомлень. З іншого боку, розмаїтістю інформаційних загроз стосовно акустичної інформації.

Для захисту інформації в мовленнєвих системах зв'язку застосовують наступні способи:

– інформаційне приховання мовленнєвої інформації, що забезпечується шляхом технічного закриття (аналоговим скремблеруванням) і шифруванням сигналів мовленнєвої інформації, які передаються по кабелях і радіоканалах;

– енергетичне приховання, що забезпечується шляхом глушіння (звукоізоляцією) акустичних сигналів, звукопоглинанням акустичної хвилі, зашумленням твердого середовища поширення іншими широкосмуговими звуками (шумами, перешкодами), що забезпечують маскування акустичних сигналів;

– виявлення, локалізація й вилучення закладних пристроїв.

Характерною рисою роботи скремблерів є розбиття вихідного мовленнєвого сигналу (МС) на окремі проміжки на частотно-часовий сітці з наступним їхнім перемішуванням, підсумовуванням і передачею по каналу зв'язку в аналоговій формі. Особливістю роботи пристроїв цифрового засекречування мови є криптографічні перетворення над цифровими даними хвильової форми або параметричного опису МС із наступною передачею по каналу зв'язку в цифровому вигляді.

Якщо виключити класичні криптографічні методи шифрування сигналу для забезпечення безпеки мовленнєвого зв'язку, то можна застосовувати нові комп'ютерні технології, які використовують підхід побудови спеціальних програмно-апаратних засобів. Ці засоби поєднують ідею перекладу звукового (мовленнєвого) сигналу у вид відповідних графічних образів і навпаки із зображення у звук або мову без втрати інформативності й/або розбірливості з можливостями відомих і перспективних методів цифрової обробки зображень.

Енергетичне приховання досягається шляхом застосування генераторів просторового зашумлення, генераторів акустичного й віброакустичного зашумлення.

Коли мова йде про виявлення закладних пристроїв проводити спеціальні заходи іноді дуже дорого й довго, тому, в якості засобів захисту інформації часто вигідніше використовувати такі пристрої захисту телефонних переговорів як генератори просторового зашумлення, генератори акустичного й віброакустичного зашумлення, мережеві фільтри.

В умовах шуму й перешкод поріг чутності для прийому слабкого звуку зростає. Таке підвищення порога чутності називають акустичним маскуванням. Для формування віброакустичних перешкод застосовуються спеціальні генератори на основі електровакуумних, газорозрядних і напівпровідникових радіоелементів.

На практиці найбільш широке застосування знайшли генератори шумових коливань. Шумогенератори першого типу застосовуються для придушення безпосередньо мікрофонів як у радіопередаючих пристроїв, так і диктофонів.

Але завжди існує можливість винайти новий спосіб зняття інформації, тому лише комплекс заходів допоможе уникнути витік мовленнєвої інформації і постійні дослідження в сфері захисту інформації.

**Література**

1. Куликов Е. И., Трифонов А. П. Оценка параметров сигналов на фоне помех. – М.: Сов. радио, 1978. – 254 с.

2. Yellott, John I. Jr., «Spectral Consequences of Photoreceptor Sampling in the Rhesus Retina.» Science. – том 221. – с. 382-385, 1983.

3. [Електронний ресурс]. – Режим доступу : ttp://dic.academic.ru/dic.nsf/ruwiki/1125760.

# РОЗВИТОК СТРАТЕГІЧНИХ КОМУНІКАЦІЙ ЯК ПЕРЕДУМОВА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

*УДК 316.77:[351.74+351.86] (075.8)*

**Аблазов І.В.**
кандидат політичних наук, доцент
Воєнно-дипломатична академія ім. Євгенія Березняка
**Рубель К.В.**
кандидат історичних наук, доцент
Воєнно-дипломатична академія ім. Євгенія Березняка

## АКТУАЛЬНІ ПРОБЛЕМИ ДОСЛІДЖЕННЯ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ У ВОЄННІЙ СФЕРІ В КОНТЕКСТІ ЗАВДАНЬ МІНІСТЕРСТВА ОБОРОНИ УКРАЇНИ ЩОДО ЇХ РЕАЛІЗАЦІЇ

Метою реалізації стратегічних комунікацій у воєнній сфері як складової національної системи стратегічних комунікацій є просування загальнодержавного наративу та формулювання й впровадження ключових повідомлень задля підвищення розуміння політики Міністерства оборони суспільством, ефективна протидія інформаційним викликам та загрозам у воєнній сфері [1]. Проте експертне середовище констатує, що саме вироблення загальнодержавного наративу поки що залишається найбільш складною задачею, вирішення якої виходить за межі повноважень лише оборонного відомства.

Разом з тим констатується, що в країнах НАТО – партнерах України в останні роки прослідковуються такі тенденції в сфері стратегічних комунікацій. Американські дослідники поступово відходять від вузького тлумачення стратегічних комунікацій, таких як «битва наративів» або змагання прес-служб. Дискусія щодо стратегічних комунікацій поступово зміщується в бік пошуку відповідей на питання щодо системних дій в інформаційному домені, дискусії щодо стратегічного лідерства в інформаційному просторі та розвитку спроможностей досягати в ньому мети збройного протиборства [2]. Серед американських військових сьогодні спостерігається спроба уточнення термінології сфери стратегічних комунікацій. Зокрема, в контексті збройного протиборства введені в обіг та активно використовуються такі терміни як «інформаційний простір» (Information Environment), «командирська комунікаційна синхронізація» (Commander’s Communication Synchronization), «військові комунікаційні спроможності та дії» (Military Communication Capabilities and Activities), «інформаційні спроможності» (Information-related capabilities) [3].

Активно розвивається теорія та практика інформаційних операцій, яка охоплює такі основні інформаційні спроможності як електронне протиборство (Electronic Warfare), операції в кіберпросторі (Cyberspace Operations), операції військової інформаційної підтримки (Military Information Support Operations), введення в оману (Military Deception), заходи щодо впливу (Influence Activities), безпеку операцій (Operations Security), розвідувальне забезпечення інформаційних операцій (Intelligence) тощо.

Проведений у Воєнно-дипломатичній академії імені Євгенія Березняка протягом 2017 року структурно-функціональний аналіз наявних в підрозділах Міністерства оборони України можливостей та повноважень щодо реалізації стратегічних комунікацій у воєнній сфері виявив низку проблемних аспектів, які потребують наукового осмислення, термінологічної концептуалізації або унормовування у поточних документах. Оскільки стратегічні комунікації включають в себе проведення інформаційно-психологічних операцій, то суттєвого уточнення потребує роль спецслужб України в цьому процесі.

Зокрема, Концепція стратегічних комунікацій Міністерства оборони та Збройних Сил України визначає її суб'єктів. Окремий пункт Концепції (3.3) визначає розподіл функцій у сфері реалізації стратегічних комунікацій у МО та у ЗС України. У ньому зазначено, що розвідувальне забезпечення проведення інформаційних заходів здійснюється Розвідувальним органом МО України. Зазначимо, що Концепція передбачає понад десяти напрямів реалізації стратегічних комунікацій, які в свою чергу визначені в контексті підходів та стандартів НАТО у даній сфері. Серед таких інформаційні заходи міжнародного співробітництва, демонстрація дій військ, всі напрями зв'язків з громадськістю, публічної дипломатії, заходи цивільно-військового співробітництва, психологічні операції та інші. Кожен з напрямів реалізується через власні сукупності та технології інформаційних та комунікаційних заходів. Проте концепція не роз'яснює, які саме інформаційні заходи мають мати забезпечення з боку спецслужб.

Аналогічно з функціональної точки зору потребуватимуть уточнення аспекти координації комунікаційної складової цивільно-військового співробітництва, реалізація якого є не лише міжвідомчою проблемою України, а в умовах конфлікту носить контекст багатосторонньої дипломатії.

Також актуальним напрямом дослідження в умовах нових підходів американських колег до розуміння військової дипломатії та публічної дипломатії в контексті стратегічних комунікацій є вивчення та узагальнення досвіду апаратів військових аташе у реалізації кінцевої мети стратегічних комунікацій. Для вітчизняної дипломатичної практики сам термін "військова підтримка публічної дипломатії", який використовує НАТО, є досить новим та потребує

уточнення за змістом та правового обґрунтування методів її реалізації в рамках міжнародного військового співробітництва.

Одним з основних шляхів розв'язання вказаних проблем має стати діяльність Координаційної групи зі стратегічних комунікацій Міністерства оборони України.

Уточнення функцій та завдань суб'єктів та методичного забезпечення їх реалізації в контексті розбудови системи стратегічних комунікацій являє собою багатопланову наукову проблему, розв'язання якої можливе в межах низки міжвідомчих науково-дослідних робіт.

**Література**

1. Концепція стратегічних комунікацій Міністерства оборони України та Збройних сил України. Затверджена Наказом Міністерства оборони України 22 листопада 2017 року № 612 // Офіційний сайт Міністерства оборони України. URL: http://www.mil.gov.ua/content/mou_orders/612_nm_2017.pdf (дата звернення 05.03.2018).

2. Попова Т. Стратегічні комунікації у США: 80% реальних дій і лише 20% слів // Сайт Детектор Медіа. URL: http://detector.media/infospace/article/ 130925/ 2017-10-13-strategichni-komunikatsii-u-ssha-80-realnikh-dii-i-lishe-20-sliv/ (дата звернення 05.03.2018).

3. Joint Publication 5-0. Joint Planning. (Планування застосування ЗС США) //Сайт National Defense University Press. URL: http://ndupress.ndu.edu/Media/ News/Article/1223888/joint-publication-5-0-joint-operations / (дата звернення 05.03.2018).

*УДК 340:007*

**Авдошин І.В.**
доктор юридичних наук,
старший науковий співробітник
Національна академія Служби безпеки України

## ІНФОРМАЦІЙНИЙ ПРОСТІР ЯК ОБ'ЄКТ РОСІЙСЬКОЇ АГРЕСІЇ ПРОТИ УКРАЇНИ

Аналіз сучасної оперативної обстановки в Україні свідчить про тотальне використання інформаційних технологій та зброї в сучасній інформаційній війні російської експансіоністської машини проти нашої держави з метою забезпечення умов інформаційному впливу Росії для геополітичного контролю українського інформаційного простору.

Розвиток комунікаційних системних мереж створює далеко не віртуальну можливість цільового маніпулювання свідомістю тих чи інших груп

людей у визначених регіонах чи державах з метою нав'язати потрібні оціночні характеристики, погляди, норми поведінки, а за потреби – для дестабілізації владних і суспільних структур.

Інформаційна агресія становить найнебезпечніший вид гуманітарного терору, і полягає у спрямуванні функціонування і розвитку гуманітарного комплексу держави чи її окремих регіонів у інтересах агресора. Вона може здійснюватися у жорсткій і м'якій формах чи мати змішаний характер.

Так, основним висновком і уроком з інформаційно-пропагандистської війни Росії проти України як важливої складової «гібридної війни» є її безпрецедентний характер за своїми змістом, масштабами і спрямованістю, якій характерні такі риси:

по-перше, інформаційна війна розпочалась задовго до військової агресії Росії проти України і продовжує супроводжувати її на всіх етапах, завчасно адаптуючись під поточні цілі і задачі;

по-друге, інформаційно-пропагандистські та дезінформаційні проекти, операції і заходи спрямовані на всі верстви населення і всі регіони України, а також населення Росії і країн Заходу – відповідно, з різними цільовими установками і задачами;

по-третє, головна мета інформаційної війни в Україні – ліквідація державності України; в Росії – отримання підтримки населення для виправдання дій керівництва Росії; для країн Заходу – дискредитація дій керівництва України та її Збройних Сил [2].

І як зазначається у підготовленому Європейською службою зовнішньої дії огляді Disinformation Review, російська військова агресія, починаючи з 2014 року також супроводжувалася потужною кампанією дезінформування, яка мала на меті розмити правду про стан справ в Україні та полегшити дії Росії. І хоч проросійські ЗМІ ніколи не припиняли поширювати дезінформацію про цю країну, останніми тижнями обсяг та агресивність спрямованої на Україну дезінформації значно зросли [1].

При цьому європейськими експертами зазначається, що інформаційна агресія щодо України оживилася саме тоді, коли відновилися бойові дії на Донбасі. Саме такий зв'язок між військовою та інформаційною агресією Росії можна було спостерігати також у випадках із російським втручанням у Сирії та збиттям російського військового літака над Туреччиною.

Також в огляді експерти відзначають, що окрім звичних уже новин про переслідування росіян та російської мови в Україні, російська пропаганда почала розробляти нову тему – присутність бойовиків «Ісламської держави» в українській армії і навпаки. Саме це вкладається у шаблон «одного великого ворога», з яким бореться Росія.

Тобто, з початком опору України військовій агресії Російської Федерації на території Донецької і Луганської областей, а також окупації і анексії українського Криму, інформаційна політика Російської Федерації

трансформувалася у тотальну військову дезінформаційну агресію, спрямовану на демонізацію в очах російського та світового суспільства діючого керівництва України.

Водночас, складається таке враження, що Україна, яка перебуває у стані фактичної війни з Росією, повністю інформаційно роззброїлася, залишила майже неконтрольованим в районі збройного протистояння інформаційний простір від московських ворожих зазіхань [3].

Необхідно визнати, що не дивлячись на окремі (правда безсистемні, повільні і непередбачувані за змістом) позитивні кроки з боку влади до формування національного інформаційного простору та інформаційної безпеки, український істеблішмент програє інформаційну війну Кремлю на власній території.

І справа не в кількісних показниках, не в мільярдах коштів, що виділяються на проведення інформаційних війн, кампаній, операцій чи акцій, а в мотивації продуцентів та якості створеного ними інформаційного продукту, здатного ліквідувати інформаційні прогалини та забезпечити інформаційний суверенітет держави. Тому, український гуманітарний простір має бути захищений, в тому числі, і владою від агресивних кремлівських зазіхань.

Реагуючи на вимоги часу і планомірну інформаційну війну проти України, в нашій державі має бути створена ефективна інформаційна зброя для ведення інформаційних війн. України має здійснювати на упередження інформаційні напади на супротивників, підтримувати інформативно співвітчизників за межами держави, формувати підґрунтя перенесення «гібридних загроз» інформаційного характеру з території України на територію Росії.

При цьому, виготовляючи цей вид зброї та використовуючи сучасні механізми інформаційного впливу, Україна має обмежуватися ефективною інформацією. Зокрема, розкриттям правдивих тем національно-визвольної боротьби, Голодомору, висвітлення життя історичних персоналій, пропаганда української культури, мови, цінностей – наша ефективна інформаційна зброя, шкідлива для тих, хто не сприймає незалежність України, на свій розсуд інтерпретує історію, нав’язує українцям свою культуру та ідеологію [3].

Протистояти російській дезінформаційній політиці можливо лише у тісній взаємодії з інформаційними ресурсами демократичних країн Заходу, спрямовуючи та координуючи спільну роботу не тільки щодо роз’яснення поточних російських інформаційних акцій, а й на їх упередження та активну протидію.

Зокрема, пропонується застосовувати ефект несподіваності, превентивності інформаційного удару, який закладено сьогодні у концепції глобального інформаційного лідерства, яку експерти влучно назвали як «програмуюче лідерство».

Саме в рамках цієї концепцію Україна повинна настійливо формувати міжнародну повістку дня (на рівні ООН, ЄС, ОБСЄ), яка включатиме в себе формулювання найбільш актуальних проблем у найбільш зручному для нашої держави форматі. Так, наприклад, наполягання під егідою ООН виконання та реалізації мінських домовленостей врегулювання конфлікту на території України, передбачатиме певний спектр сумісних дій ряду держав, зокрема країн нормандського формату із залученням США і Великобританії під керівництвом нашої держави і в наших інтересах.

Крім того, така стратегія має містити низку програмних принципів:

випереджаюче зовнішньополітичне планування і вкидання у політичний дискурс ідей і концепцій, втілення яких у життя відповідає інтересам України;

випереджаюче формулювання основоположних цілей міжнародної повістки дня у вигідному для України ракурсі;

рішуче дистанціювання від «чужої гри» та ігнорування неприйнятних цілей інших суб'єктів світової політики;

штучне створення Україною умов, які підштовхуватимуть партнерів до інкорпорування запропонованої нашою державою повістки дня у їхні політичні програми.

**Література**

1. Інформаційна агресія Кремля оживилася – експерти ЄС [Електронний ресурс]. – Режим доступу: http://www.depo.ua/ukr/life/ informatsiyna-agresiya-kremlya-ozhivilasya---eksperti-es-06052016200500.

2. Радковець Ю. Два з половиною роки російської військової інтервенції проти України оголили вразливі місця у системі міжнародної безпеки / Ю.Радковець. – [Електронний ресурс]. – Режим доступу: https:// www.ukrinform.ua/rubric-politycs/2107122-gibridna-vijna-rosii-proti-ukraini-uroki-ta-visnovki.html.

3. Куйбіда В. Інформаційний простір як об'єкт зовнішньої і внутрішньої політико-ідеологічної агресії проти України / В.Куйбіда, І. Розпутенко. – [Електронний ресурс]. – Режим доступу: http://www.nru. org.ua/blogs/bloh-vasylia-kuibidy/2088-informatsiinyi-prostir-iak-ob-iekt-zovnish noi-i-vnutrishnoi-polityko-ideolohichnoi-ahresii-proty-ukrainy.

*УДК 004.056.53*

**Бровко В.Д.**
кандидат технічних наук
Національна академія Служби безпеки України

## ВИЗНАЧЕННЯ МОМЕНТУ РОЗЛАДКИ ІНФОРМАЦІЙНОГО ПОТОКУ

Масова комунікація у мережі Інтернет набирає дедалі більших обертів. Зокрема, ринок онлайнової реклами був єдиним рекламним ринком,

який не лише не скоротився в роки фінансової кризи 2008–2009 рр., а навіть трохи зріс. Абсолютну меншість серед найвідвідуваніших інтернет-ресурсів становлять сайти зі сталим змістом або рідко поновлювані джерела, такі, як електронні бібліотеки, енциклопедії або деякі корпоративні сторінки. Усі інші мережеві ресурси є, по суті, інформаційними потоками. Тому доцільно сформувати визначення: інформаційний потік – це система продукування й поширення повідомлень, які характеризуються певними спільними ознаками. [2].

Прогнозування виникнення інформаційних загроз є невід'ємною частиною системи захисту інформації. При правильному виявленні загрози, а також правильному її опрацюванню, вжитті запобіжних заходів знижується ризик виникнення атаки. Одним із джерел можливої інформації для виявлення загроз є інформаційний потік. Інформаційний потік являє собою сукупність усіх форм інформації, представленої у вигляді друкованих, електронних, усних носіїв, та яка має повний зміст розкриття об'єкту інформації. При аналізі інформаційного потоку важливим являється виявлення можливого інформаційного викиду інформації, яка сама по собі може бути загрозою або провокувати виникнення інформаційних загроз. Ця проблема може бути вирішена шляхом виявлення моментів розладки часового ряду, сформованого з інформаційного потоку [1].

Для дослідження доцільно використовувати таке поняття як часовий ряд – особливий тип даних, який містить інформацію про плинність значень станів або характеристик об'єкту дослідження у часі. При дослідженні часових рядів в їх структурі намагаються окремо виділити детерміновану $y_t$ та стохастичну $e_t$ складові, процедури моделювання та прогнозування яких принципово відмінні. Найчастіше при цьому спираються на адитивну модель представлення часового ряду [2].

Таким чином розв'язується задача виявлення моментів розладки в інформаційному потоці шляхом аналізу коефіцієнтів моделі авторегресії, побудованої на інтервалах часового ряду, сформованого з інформаційного потоку.

Основний акцент при цьому робиться на визначення інформаційного потоку, моделі авторегресії та поняття часового ряду з його складовими. Досліджується момент розладки та згладжування часового ряду. Також аналізуються застосування методу медіанного згладжування та виявлення аномальних даних.

**Література**

1. Аналіз данних та статистична обробка сигналів : навч.посіб / О.Є. Архіпов, С.А. Архіпова . – 2012 р.

2. Феномены современных информационных потоков : навч. посіб. / Д.В.Ландэ, А.Б. Литвин // Сети и бизнес. – 2001 р.

3. Політика і мас-медіа (переклад з нім.) : навч. посіб. / Г. Штромайєр. – К. : Вид. дім «Києво-могилянська академія». – 2008 р.

4. Непараметрический метод обнаружения моментов переключения двух случайных последовательностей// Автоматика и телемеханіка: навч. посіб. / Б.Е. Бродський, Б.С. Дарховський. –1989 р.

5. Последовательные оценки параметров стохастических динамических систем: навч. посіб. / В.В. Конєв. – Томск : Изд-во Томского університета. – 1985 р.

6. Обнаружение изменения свойств сигналов и динамических систем : навч. посіб. / М. Бассвиль, А. Банвениста. – М. : Мир. – 1989 р.

*УДК 316.485.6:351.746.1(477)*

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

## ОСОБЛИВОСТІ ЗДІЙСНЕННЯ ІНФОРМАЦІЙНО-ПІДРИВНОЇ ДІЯЛЬНОСТІ З ВИКОРИСТАННЯМ РЕЛІГІЙНИХ СТРУКТУР

Добре відомо, що інформаційно-підривна діяльність – найвищий ступінь інформаційного протиборства, який спрямований на розв'язання суспільно-політичних, ідеологічних, національних, територіальних та інших конфліктів між державами, народами, націями, класами й соціальними групами шляхом широкомасштабної реалізації засобів і методів інформаційного насильства (інформаційної зброї).

Релігійні організації завжди мали один з вирішальних важелів впливу на суспільство в інформативному імперативно-наказовому плані. Не змінилася докорінно ситуація і сьогодень. За матеріалами одного з найавторитетніших статистичних центів – Центру Разумкова, вплив релігії на населення досить високий – майже 67 % громадян вважать себе віруючими та прислухаються до позиції тієї чи іншої церкви або релігійної організації [1].

Крім того, психологами неодноразово доведено, що у випадках кризових ситуацій люди втрачають у більшості ситуацій можливість критично мислити і часто звертаються «за допомогою» або «покровительством» когось сильнішого і могутнішого [2, с. 56]. На сьогодні розгалужена релігійна мережа представлена низкою «уповноважених осіб» (гуру, батюшки, медіуми, духовні наставники і сенсеї тощо) які знають відповіді на всі життєві питання і освідомлені з вирішенням будь-яких проблем: від економічних до політичних тощо. У нашому випадку ми маємо невтішний факт: релігійні організації, зокрема Українська православна церква (далі – УПЦ), прямо чи опосередковано виявилися втягнутою у збройний конф-

лікт та на відміну від Української православної церкви Київського патріархату (далі – УПЦ КП) та інших церков, ще й виявилася по обидва боки барикад . Чому УПЦ? Тому що, по-перше, на сьогодні це найбільша і найвпливовіша релігійна організація України [3], представлена у всіх регіонах України, та яка на сході держави має набагато більшу «популярність» ніж на заході, де сильна конкуренція історично вкорінених греко- і римокатоликів, автокефалістів та УПЦ КП. По-друге, історично так склалося, що керівні центри УПЦ знаходиться у Москві (Синод Руської православної церкви (далі – РПЦ) і Патріарх Московський і всія Руси) і незалежно від оголошеної у 1992 році «широкої автономії» у господарській і адміністративній діяльності УПЦ є де-факто дочірньою церквою РПЦ на теренах України. «Не может быть в Азии двух царей как не может быть на небе двух солнц» – А.Македонський, видатний полководець і завойовник [2, с. 167].

У зв'язку з вищевикладеним, з початком АТО УПЦ виявилася зручним інструментарієм для проведення Російської Федерацією (її церковними структурами та спеціальними службами) інформаційно-підривної діяльності на тимчасово-окупованих територіях.

Наведемо тезу одного із дослідників АТО В. Кострова: «Згадаймо, як усе починалося. Спочатку було слово. Брехливе й провокаційне слово російської пропаганди. Зомбовані нею певні прошарки українського суспільства – а це тільки на Сході близько третини населення – за активного втручання Москви спочатку підтримали захоплення екстремістами адміністративних будівель у Донецьку й Луганську, а потім за вказівкою своїх «духовних наставників» вийшли на «референдуми про федералізацію» [4].

Цьому свідчать і низка фактів втручання окремих священнослужителів УПЦ на окупованих територіях у сприяння ополченцям і їхня безпосередня участь у збройному конфлікті, а головне – вони наразі передають «слово» Кремля народу України. Окремі з них здійснюють ідеологічну проросійську пропаганду і на підконтрольній Україні територіях, про що свідчить низка матеріалів СБ України. Які ми маємо наразі наслідки:

1. Майже всі підрозділи ополченців ідеологічно готові полягти за «Святу Русь» і «чистоту православ'я», що свідчить про їх непоганий бойовий дух.

2. З кожним днем населення Донбасу відвертається від ідеї об'єднання регіонів (для них яскравими прикладами, якими переповнений Інтернет, є агресивна політика «розкольників» УПЦ КП по відношенню до УПЦ).

3. Наявність інформації про двояку сутність УПЦ вже спричинила низку релігійних конфліктів на теренах нашої держави, що ніяк не сказується позитивно на суспільно-політичній єдності народу України та відродженню його духовності.

4. УПЦ КП, керуючись хитким становищем УПЦ, замість вирішення питання єдності церкви повернулася до 1990-х років: захоплення церковних будівель, побиття віруючих УПЦ і агресивна інформаційна політика щодо «церкви-конкурента» тощо.

Можемо зробити висновок, що наразі в Україні інформаційно-підривна діяльність з використанням релігійних структур ведеться з обох полюсів: з ОРДЛО та з позиції релігійних осередків на території нашої країни. Ніякого діалогу з 2014 року. Ніяких способів, апелюючи до релігійних вірувань громадян, дійсно *зупинити* збройний конфлікт і врятувати життя українців. Як протидіяти інформаційно-підривній діяльності з позиції релігійних структур на сьогодні? На наш погляд, ключ успіху залежить як від конкретних заходів керівництва держави та релігійних структур так і від пересічного «віруючого» громадянина, рівня його розвитку, уміння критично мислити та адекватно оцінювати свої дії, адже недарма зауважив І. Богослов: «Возлюбленные! Не всякому духу верьте, но испытывайте духов, от Бога ли он, потому что много лжепророков появилось в мире» [5].

**Література**

1. Український центр економічних та політичних досліджень імені Олександра Разумкова. Етноконфесійна ситуація в Україні [Електронний ресурс]. – Режим доступу : www.uceps.org.

2. Спиркин А.Г. Философия : учебник / А.Г. Спиркин. – М. : Гардарика, 1998. – 816 с.

3. Релігійнийзвіт Міністерства культури України за 2017 рік [Електронний ресурс]. – Режим доступу : www.kmu.gov.ua/control/.../article%3Fart_id%3D72645.

4. Костров В. Війна і мир на Донбасі / В. Костров. – К.: Національна безпека. Правозахист.– С. 28.

5. Библия, Новый завет, Первое соборное послание И. Богослова гл. 4, стих 1.

*УДК 94(470 + 571) : 355.425*

**Даниленко В. М.**
доктор історичних наук, професор
Національна академія СБ України

## РОСІЯ І СВІТ: ІНФОРМАЦІЙНІ ЗАГРОЗИ І ЗАСОБИ ПРОТИДІЇ

Глобальні зміни у міжнародних відносинах протягом XX – на початку XXI століття зумовлюють необхідність нового прочитання історії країн і народів і чіткого визначення їхньої ролі в історичному процесі. Тривале перебування українських земель у складі Російської імперії, в тому числі

більшовицької, цілеспрямована русифікація і колонізація мали наслідком болісний і суперечливий шлях становлення незалежної Української держави. Систематичне нав'язування тверджень про нерозривну єдність українського й російського народів і про неспроможність України існувати самостійно розраховувалось на формування внутрішніх переконань багатьох поколінь українців і становлення такого явища, як «русский мир». Тепер, коли прояснилася ситуація зі справжніми намірами сусідньої держави, варто розглянути, якими є мета, форми і методи інформаційних загроз з боку Росії для України і всього людства. Їх з'ясування дасть можливість напрацьовувати нові й удосконалювати наявні засоби протидії російському агресору, який в особі політичного керівництва РФ вступив у глибокий і затяжний конфлікт зі світовою спільнотою.

Важливою методологічною передумовою висвітлення поставлених питань є розуміння спадкоємності великодержавної політики Росії. Істеблішмент РФ узяв на озброєння тезу про доцільність возвеличення всіх, хто докладав сил для збереження і примноження надбань «єдиної і неділимої». У такому разі має настати історична відповідальність за імперську експансію й асиміляцію народів, організацію голодоморів і політичних репресій.

Для встановлення істини цінними є праці в галузі права, історії, мовознавства сучасних українських авторів В. Василенка, В. Брехуненка, М. Ковальчука, І. Патриляка, Г. Півторака, В. Сергійчука, В. Смолія та інших авторів, які ґрунтуються на документальних та історіографічних джерелах. Російська офіційна політична риторика й тотальна критика подій в Україні (від державної до культурної неспроможності) не мають належного наукового підґрунтя: праці українських науковців в РФ майже не перекладаються і не читаються, прямі наукові й культурні контакти зійшли нанівець.

Російські політики, враховуючи військову міць, людські й економічні ресурси своєї держави, не змогли змиритися з послабленням провідних позицій на міжнародній арені і втратою впливу на східноєвропейські країни та колишні радянські республіки. Договір про дружбу, співробітництво і стратегічне партнерство між Україною та Російською Федерацією був підписаний лише 31 травня 1997 р. У ньому зафіксовано, що «Високі Договірні Сторони відповідно до положень Статуту ООН і зобов'язань по Заключному акту Наради з безпеки і співробітництва в Європі поважають територіальну цілісність одна одної і підтверджують непорушність існуючих між ними кордонів». Відносини двох держав мали будуватися на основі принципів «взаємної поваги, суверенної рівності, територіальної цілісності, непорушності кордонів, мирного врегулювання спорів, незастосування сили або загрози силою, включаючи економічні та інші способи тиску, права народів вільно розпоряджатися своєю долею, невтручання у

внутрішні справи, додержання прав людини та основних свобод, співробітництва між державами, сумлінного виконання взятих міжнародних зобов'язань, а також інших загальновизнаних норм міжнародного права». Очевидним є цинічне порушення Російською Федерацією зазначених положень Договору, а для свого виправдання керівництвом РФ застосовано весь накопичений арсенал гібридної війни.

Наступ з боку Росії в інформаційній сфері супроводжується посиленням військового протистояння, ескалацією політичного та економічного напруження у дво- та багатосторонніх міжнародних відносинах. Вістря російських загроз спрямовується також проти європейських країн, США, Канади, міжнародних і громадських організацій. Використовуються такі форми і методи: 1) збір і оголошення компромату на провідних державних і громадських діячів, а за його відсутності – продукування фейкових повідомлень і троллінг конкретних осіб; 2) сприяння поширенню негативних явищ у середовищі противника – корупції, соціального невдоволення, відчуття тривоги, апатії, незахищеності; 3) розгойдування внутрішньополітичної ситуації, підтримка радикальних партій і рухів, будь-яких опозиційних проявів; 4) втручання у волевиявлення народів під час проведення референдумів і виборів; 5) постійна демонстрація військової сили в тих чи інших точках планети; 6) неповага до міжнародних організацій та їхніх посадових осіб, які виступають з критикою зовнішньої і внутрішньої політики Росії; 7) фальсифікація історії країн і народів, їхніх взаємовідносин.

Інформаційна війна, яку Росія веде проти України і світу, є складовою гібридної війни. Це фактично один з інструментів колишньої «холодної» війни, яка не припинялася від 1946 р. до кінця 1980-х років. Отже, час дії гібридної війни теж може бути тривалим, а її форми і методи надзвичайно мінливими.

Ефективність російської інформаційної агресії проти України залежить не стільки від витонченості її форм і методів, скільки від стану українського суспільства і влади. Прогрес в економіці, соціальній сфері, реальні зрушення у боротьбі з корупцією і тероризмом, інтенсивний розвиток міжнародного співробітництва і реформи як передумова євроатлантичної інтеграції – найкращі засоби протидії агресії. Принципово важливо на будь-якому напрямі внутрішньої і зовнішньої політики мати стратегію розвитку, прораховувати причинно-наслідкові зв'язки, встановлювати пріоритети, розширювати лави союзників. Чинниками позитивних результатів може бути врахування гіркого історичного досвіду, коли через внутрішні суб'єктивні обставини, чвари й надмірні амбіції лідерів політичних партій та рухів втрачалося головне. Вагомою запорукою адекватного реагування на прояви кіберзлочинності й інформаційних атак, які несуть загрозу для національної безпеки України, є високий рівень підготовки, світогляд і ерудиція майбутніх фахівців з питань інформаційної безпеки.

*УДК 342*
**Дудатьєв А.В.**
Кандидат технічних наук, доцент
Вінницький національний технічний університет

# КОНЦЕПТУАЛЬНІ ТА НАУКОВО-МЕТОДОЛОГІЧНІ ОСНОВИ ЗАХИСТУ ДЕРЖАВИ ВІД ДЕСТРУКТИВНИХ ІНФОРМАЦІЙНИХ ВПЛИВІВ

Методи проведення спеціальних інформаційних операцій використовувались в глибоку давнину при веденні численних війн. Дезінформування, проведення пропаганди з метою дезорієнтації як війська, так і населення країни-супротивника використовувалось з метою формування необхідної інформаційної моделі. Сучасні технології ведення інформаційного протиборства, які базуються на різних методах маніпулювання інформацією, використовують можливості сучасних інформаційного та кіберпростору. Ці можливості обумовлюються, в першу чергу, можливостями створеннями системи зв'язків між користувачами та різними об'єктами, що входять у глобальне інформаційне середовище. З урахуванням сучасних можливостей створення, зберігання та поширення інформації можна констатувати що сучасний інформаційний та кіберпростори складають специфічну арену для проведення спеціальних інформаційних операцій (СІО). Основними характеристиками СІО є такі:

- латентність агресивних дій;
- практична відсутність людських втрат;
- можливість одночасного проведення декількох СІО;
- необізнаність оппонента щодо специфіики проведення СІО;
- можливість поетапного охоплення населення (ефект ланцюжкової реакції);
- неможливість (складність) визначення оппонента;
- складність (неможливість) пртидії впливу;
- відсутність реваншизму.

**Метою дослідження** є побудова концептуального підходу щодо забезпечення комплексної інформаційної безпеки соціотехнічних систем (СТС).

**Основна частина**

Відповідно до сучасної термінології СІО називають кібернетичними операціями (КО) . Оскільки СІО або КО, що спрямовані на СТС розраховані на ураження різнорідних складових, то доцільно їх розбити на інформаційно-психологічні операції (ІПО), що спрямовані на соціальну складову СТС та інформаційно-кібернетичні операції (ІКО), які спрямовані безпосередньо на технічну складову СТС.

Деструктивний інформаційний вплив, який подається на вхід соціальної складової соціотехнічної системи може призвести до нестійкого стану всієї системи за рахунок впливу соціальної частини на технічну. Можливі різні комбінації взаємодії технічної і соціальної складових системи і як наслідок різні ризики потенційних деструктивних інформаційних впливів. Соціотехнічну систему можна представити:

$STS=\{SuBSTS_t, SuBSTS_s\}$,

де $SuBSTS_t$ – підсистема СТС, яка представляє технічну складову, $SuBSTS_s$ – підсистема СТС, яка представляє соціальну складову системи.

У свою чергу $SuBSTS_t$ може бути представлена такими ознаками: структура об'єкта, специфіка системи управління, характеристика інформаційно-телекомунікаційної системи (ІТС), технології, що використовують на об'єкті захисту, обладнання, яке розташовано на об'єкті тощо. $SuBSTS_s$ може бути представлена такими ознаками: мета впливу, розташування суб'єкта впливу, кваліфікація, доступ до спеціальних технологій, обладнання тощо.

Незважаючи на різні типи СІО сценарії їх реалізації практично збігаються і можуть бути представлені такими етапами:

- планування СІО;
- знаходження інформаційного приводу для проведення СІО;
- "розкрутка" інформаційного приводу або супровід СІО;
- вихід з процесу проведення СІО.

Наведені етапи реалізації СІО фактично представляють етапи проведення інформаційної війни. На рис. 1. представлено концептуальну модель системи інформаційного впливу.

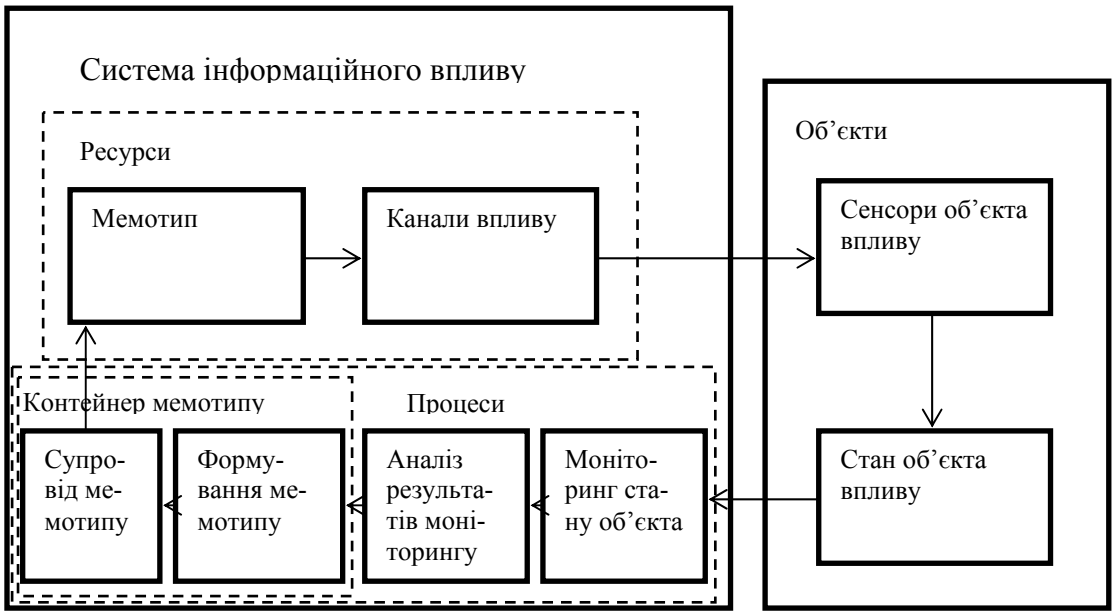



Рис. 1. Концептуальна модель системи інформаційного впливу

У доповіді запропоновано аксіоматику теорії інформаційної взаємодії типу «об'єкт–суб'єкт» та класифікацію інформаційних вірусів, що можуть бути використані для «інфікування» соціальної частини соціотехнічної системи. Представлено модель інформаційного впливу та моделі і методи протидії спеціальним кібернетичним операціям. Зокрема, запропоновано комплексний FC-метод, що дозволяє ефективно розв'язувати задачі з комплексного захисту інформації, з урахуванням специфіки етапів проектування та експлуатації КСЗІ в умовах ведення інформаційного протиборства на рівні «підприємство–регіон–держава». Представлено метод інформаційної обфускації, метою якого є заплутування соціальної частини соціотехнічної системи. Запропоновано метод мем-програмування, метою якого є оптимальне проведення інформаційно-психологічної операції. Представлено метод оцінювання інформаційної стійкості соціотехнічної системи, а також комплексний метод протидії ІПО, який використовує попереджувальні та компенсуючі меми.

*УДК 342.95:727:007.056*

**Єсімов С.С.**
кандидат юридичних наук, доцент
Львівській державний університет внутрішніх справ

## ДІЯЛЬНІСТЬ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ З ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У КОНТЕКСТІ ДІЯЛЬНОСТІ ЗАСОБІВ МАСОВОЇ ІНФОРМАЦІЇ

Інформаційна безпека відіграє значущу роль в системі забезпечення національної безпеки. Це прямо зазначено в Доктрині інформаційної безпеки України. Оптимізація системи інформаційного управління відбувається на основі технологій ефективного використання та розподілу контролю над інформаційними ресурсами. Інформаційна сфера складається з інформаційних полів різної складності, що генеруються та випромінюваних різними джерелами інформації. При цьому кожна людина, регіон існують одночасно в різних політико-інформаційних сферах. Інформаційний простір став системо утворюючим фактором життя, чим активніше ця сфера суспільних відносин розвивається, тим більше політична і інші складові безпеки держави залежатимуть від ефективного забезпечення інформаційної безпеки.

Зовнішні загрози та виклики безпеці генеруються не тільки на кордонах, а й у регіонах. Серед внутрішніх чинників, що створюють суттєві виклики та загрози в інформаційній сфері, можна виділити чутливість інвестиційної компоненти економіки до негативного інформаційного впливу.

Правові можливості громадян у галузі інформаційних відносин виражаються в системі конституційних прав: свобода думки, слова, масової інформації, право на доступ до інформації органів влади. Право на доступ до інформації органів влади порівняно зі свободами думки, слова і друку є порівняно новим правовим утворенням. У цілому воно вимагає не невтручання держави в систему інформаційного обміну в суспільстві, а прямого сприяння держави в отриманні необхідної інформації громадянами. В умовах забезпечення реалізації базових інформаційних прав громадян в ЄС виявляються риси права універсального доступу до засобів і технологій інформаційного обміну як нового суб'єктивного права індивіда.

Конституційної основою, що визначає характер правового регулювання інформаційних відносин, є принцип ідеологічної багатоманітності взаємопов'язаний з принципом державного суверенітету. Прояв принципу суверенітету в системі регулювання інформаційних відносин виражається у ціннісній оцінці національного та зарубіжного інформаційного обміну, відмінність яких обумовлено наявністю національних інтересів, що відстоюються в публічному діалозі. Визнання тези дозволяє систематизувати існуючі законодавстві механізми, що створюють умови для вироблення національних інтересів у внутрішньополітичній дискусії: організаційні обмеження інформаційної діяльності російських виробників інформації; заходи з підтримки національної політико-правової культури; розвиток традицій саморегулювання та діалогу влади і преси. У правовому регулюванні інформаційних відносин принцип суверенітету не може підміняти принцип ідеологічного плюралізму, а останній суперечив принципу суверенітету.

У системі масового інформаційного обміну правове регулювання відносин, поставлене в залежність від змісту розповсюджуваних повідомлень, є проблематичним, оскільки держава може встановлювати ідеологічні умови обміну інформацією і зумовлювати результати суспільної дискусії, тобто по суті встановлювати цензуру. Лише практичне гарантування принципу ідеологічної багатоманітності, яка отримує вираження у механізмах захисту свобод думки, слова і друку, виявляє випадок допустимості заборони розповсюдження інформації з її утримання – при зловживаннях правами індивіда в публічному інформаційному обміні. Перелік тематичних заборон, які складають зміст інституту зловживання, в законодавстві завжди чітко визначений і строго обмежений.

Завдання поліції у сфері забезпечення інформаційної безпеки конкретизовано в наказі МВС України від 19.08.2014 № 840 «Про деякі питання інформаційної безпеки України». Нормативними документами передбачено налагодження ефективної взаємодії з представниками Національної ради України з питань телебачення і радіомовлення в регіонах спрямованої на виявлення та припинення протиправної

діяльності провайдерів, фізичних і юридичних осіб, що здійснюють незаконну ретрансляцію заборонених рішеннями Окружного адміністративного суду м. Києва від 23 березня 2014 року, Національної ради України з питань телебачення і радіомовлення від 17.07.2014 № 292 і № 663 програм у місцях масового відпочинку та скупчення людей, баз відпочинку, розважальних закладів тощо.

Територіальні підрозділи поліції при виявленні ретрансляції заборонених програм повинні інформувати представників Національної ради з питань телебачення і радіомовлення в регіонах для застосування заходів адміністративної відповідальності до: провайдерів, що здійснюють заборонену ретрансляцію заборонених програм; фізичних і юридичних осіб, що здійснюють незаконну ретрансляцію заборонених програм у місцях масового відпочинку та скупченню людей або продаж продукції, що надає можливості здійснювати перегляд передач заборонених програм, або пакет програм, який містить заборонені телерадіопрограми; засобів масової інформації, що поширюють повідомлення, які розпалюють ворожнечу та сепаратисті настрої, посягають на державний суверенітет і територіальну цілісність України (Протокол спільної наради МВС і Національної ради з питань телебачення і радіомовлення від 30.08.2014 року.

Адміністративна діяльність направлена на забезпечення ліквідації загроз і ризиків у сфері інформаційної безпеки є основним чинником її структурування, формування і розглядається як діяльність, спрямована на запобігання нанесення збитку інтересам особи, суспільства і держави в інформаційній сфері.

**Література**

1. Наказ МВС України від 19.08.2014 № 840 «Про деякі питання інформаційної безпеки України».

*УДК 340.1*

**Зоренко Д.С.**
Інститут підготовки юридичних кадрів для СБ України
Національного юридичного університету ім. Я. Мудрого

## КОНЦЕПЦІЯ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ В КОНТЕКСТІ РЕФОРМУВАННЯ СБ УКРАЇНИ

З початком гібридного україно-російського конфлікту СБ України стикнулася з безпрецедентним викликом національній безпеці – використанням комунікації в якості зброї, проведенням масштабних за розмахом і

системних за методами інформаційно-психологічних операції, кампаній «брудної» пропаганди та дезінформації. Головна мета – комплексна дестабілізація ситуації в країні, підрив довіри до європейських цінностей, деморалізація й пригнічення населення, формування «п'ятої колони».

Постає закономірне питання спроможності СБУ з її громіздкими ієрархічними рівнями, подекуди застарілими підходами до організації службової діяльності, декларативним характером координації і взаємодії, плинністю кадрів ефективно протидіяти постійному інформаційному бліцкригу, не зв'язаному вимогами об'єктивності та етичності. В цьому контексті не останню роль відіграє й тяжіння органів держбезпеки до обмежувальної тактики – реагування на виключно на події за відсутності агресивно-наступального характеру планування та реалізації власних заходів.

Євроатлантичний курс розвитку України вимагає не тільки розбудови інститутів суспільства та держави на засадах західної демократії, а і запозичення дієвих механізмів їх захисту в умовах нелінійної агресії – стратегічних комунікацій. Концепція стратегічних комунікацій створена фахівцями НАТО ще на початку 2000-х років як скоординоване і належне використання комунікативних можливостей і діяльності Північноатлантичного альянсу – публічної дипломатії, зв'язків з громадськістю (цивільних), військових зв'язків з громадськістю, інформаційних та психологічних операцій – у разі необхідності для підтримки політики Альянсу, операцій і заходів та з метою просування цілей НАТО. До того ж, вказане поняття вже знайшло свою реплікацію в новій редакції Воєнної доктрини України 2015 року.

Це набуває ще більшої актуальності в світлі нещодавніх заяв вищого військово-політичного керівництва Російської Федерації щодо подальшої мілітаризації пропаганди – формування військ інформаційних операцій, одним з головними завдань яких має стати ведення кібервійни, а також створення відповідної інфраструктури підготовки фахівців.

До базових підходів організації Страткому можна віднести наступні: комплексна розробка діяльності на стратегічному, оперативному і тактичному рівнях; врахування всіх наявних можливостей та інструментів організації; системність, послідовність і регулярність запланованих заходів; скоординовані зусилля усіх залучених суб'єктів комунікації; оперативність, вчасне реагування та адаптація до змін у середовищі; створення додаткових координаційних органів або механізмів у кризових умовах; інтеграція комунікаційної складової до процесу розробки і реалізації управлінських рішень.

Стратегія національної безпеки України завданнями реформування СБУ визначає створення динамічної, укомплектованої високопрофесійними фахівцями, забезпеченої сучасними матеріальними і технічними засобами спеціальної служби, здатної ефективно захищати державний суверені-

тет, конституційний лад і територіальну цілісність України. З огляду на це, врахування основних положень стратегічних комунікацій стає необхідною умовою вказаного процесу.

В противному випадку існує досить висока ймовірність того, що оперативні підрозділи СБ України (не принижуючи їх напрацювань і здобутків) й надалі обмежуватимуться реалізацією заходів виключно на тактичному рівні, демонстрацією окремих «маленьких перемог» на певних напрямах службової діяльності за відсутності системної переваги над агресором.

Таким чином, сучасні асиметричні виклики національній безпеці нашої держави потребують аналогічних підходів до процесу реформування побудови як системи Служби безпеки України, так і підвищення результативності її функціонування. І не останню роль в цьому контексті має стати створення системи підготовки фахівців у сфері стратегічних комунікацій.

*УДК 351.746.1*

**Іванов О.Ю.**
викладач кафедри теорії та історії держави і права
Національної академії СБ України

## СПЕЦІАЛЬНІ ІНФОРМАЦІЙНІ ОПЕРАЦІЇ ЯК МЕТОД ДІЯЛЬНОСТІ РФ ІЗ ПСЕВДОЛЕГІТИМАЦІЇ АНЕКСІЇ АВТОНОМНОЇ РЕСПУБЛІКИ КРИМ

Доктрина інформаційної безпеки України від 25 лютого 2017 р. покладає на Службу безпеки України (далі – СБ України), серед іншого, повноваження з протидії проведенню проти України спеціальних інформаційних операцій, спрямованих на підрив конституційного ладу, порушення суверенітету і територіальної цілісності України, загострення суспільно-політичної та соціально-економічної ситуацій. Під спеціальними інформаційними операціями прийнято розуміти сплановані дії з впливу на свідомість та поведінку суб'єктів із відповідною метою. У нашому випадку йдеться про систематичний інформаційний вплив представників РФ на населення України з метою формування у нього ворожої позиції до влади, а також виправдання в його очах факту анексії Автономної Республіки Крим (далі – АРК).

Найпоширенішим методом проведення спеціальних інформаційних операцій є дезінформування, яке здійснюється через введення в оману відповідної категорії населення. Зокрема, російська історіографія відзначається чітко тенденційним викладом подій з історії Криму з тим, щоб довести нібито «споконвічно російський» статус півострова, а також начебто

важливе значення Росії для його соціально-економічного розвитку у різні періоди історії (зокрема, Російської імперії). При цьому окремі факти історичної дійсності якщо і не викривляються самі собою, то спотворюється об'єктивність їх оцінки. Такими фактами наповнений, наприклад, фільм «Крим: шлях на батьківщину», підготовлений до річниці анексії АРК. Він транслювався також і українськими телеканалами, що не могло не накласти відбитку на свідомість населення, особливо тієї його частини, яка не має належного рівня історичної та політичної обізнаності.

Пропаганда як метод спеціальних інформаційних операцій виступає основним засобом діяльності РФ у гібридній війні проти України. Вона полягає у розповсюдженні серед населення (як українського, так і російського, а також міжнародної спільноти) вигідних Кремлю неправдивих фактів та укоріненні їх у суспільній свідомості. Так, наприклад, доволі активно поширюються аргументи щодо нібито незаконності зміни правового статусу Кримської області у 1954 р. Доволі активно також поширюється ідея щодо того, що факт входження АРК до складу РФ є нібито результатом вольового акту кримськотатарського народу, який у такий спосіб реалізував своє право на національно-державне самовизначення. Загалом цей факт росіяни намагаються подати як такий, що нібито відповідає чинним нормам міжнародного права, а норми конституційного права України при цьому не мають першорядного значення. Відтак, пропагується ідея визнання Кремля як «добродія», котрий повернув «споконвічно російську» територію і вирішує її проблеми, котрих не зміг вирішити український уряд за доби незалежності. Не маючи належних правових аргументів для обґрунтування своїх дій, влада РФ активно вдається до пропагандистських заходів.

Своєрідним методом спеціальних інформаційних операцій РФ є також і психологічний тиск на населення АРК. Це відбувається через масові арешти кримських татар на анексованій території, а також їх переслідування та гучні судові процеси, що ведуться самопроголошеною владою. У такий спосіб населення непрямим шляхом примушується до визнання офіційної кремлівської ідеології та невисловлення критики на адресу чинної влади. Про це свідчать результати ряду соціологічних опитувань, під час яких громадяни, що проживають на окупованому півострові, бояться висловлювати своє дійсне ставлення до російської політики. За таких умов російська влада фактично сама собі забезпечує цілковиту безкарність і знищує громадянське суспільство, перетворюючи громадян на зручний інструмент для утвердження свого політичного курсу.

Кремлівська верхівка також активно займається диверсифікацією суспільної свідомості українців. Так, їх увага штучно переключається з проблематики статусу АРК на інші також штучно створені проблеми суспільно-політичного життя. Це стосується, насамперед, дестабілізації роботи Верховної Ради України, терористичних провокацій у різних обласних

центрах, агресивної політики в окупованих районах Донецької та Луганської областей і т. ін. За таких умов українці тимчасово «забувають» про кримське питання. Те ж саме стосується і світової спільноти, яка періодично змушена переключати увагу на агресивні дії РФ в інших регіонах світу. Тим часом самопроголошена окупаційна влада вживає заходів щодо інтеграції АРК до політико-правової системи РФ.

Діяльність РФ з проведення спеціальних інформаційних операцій включає також поширення чуток відповідного змісту серед населення України. Зокрема, поширення чуток має місце також і в середині самого населення України. Так, окремі громадяни, які не мають відповідного рівня історичної, політичної та правової обізнаності, сприймають за істину факти російської пропаганди, на основі чого будують власні міркування щодо політичної ситуації навколо АРК та діляться ними з іншими людьми, котрі так само відзначаються не надто високим рівнем світогляду. У такий спосіб може породжуватись як недовіра до української влади, до її спроможності належним чином врегулювати ситуацію, що склалася навколо АРК, так і віра у правильність дій органів влади РФ, а також навіть і сепаратистські тенденції.

Таким чином, проведення спеціальних інформаційних операцій може розглядатись як невід'ємний елемент гібридної війни, що розгорнута і активно ведеться РФ проти України. З огляду на очевидну протиправність анексії АРК як з точки зору міжнародного права, так і національного законодавства України РФ здійснює псевдолегітимацію своїх дій саме із застосуванням спеціальних інформаційних операцій. Відтак, наразі оперативно-службова діяльність СБ України має бути спрямована на протидію дезінформуванням, пропаганді, психологічному тиску на населення, диверсифікацією його суспільної свідомості та поширенню чуток представниками РФ з метою виправдання факту анексії АРК у суспільній свідомості.

*УДК 341.824*

**Капосльоз Г.В.**
кандидат психологічних наук,
старший науковий співробітник
Національний університет оборони України
імені Івана Черняховського

## ЕВОЛЮЦІЯ МЕХАНІЗМІВ ІНФОРМАЦІЙНОЇ ВЗАЄМОДІЇ ДЕРЖАВИ Й ГРОМАДЯН В ГАЛУЗІ БЕЗПЕКИ ТА ОБОРОНИ

Аналіз ведення локальних війн і збройних конфліктів, політичних процесів останнього десятиліття дозволяє стверджувати, що протиборство у військовій та політичній сферах дедалі частіше переміщується у віртуальний, доступний широкій аудиторії простір – інформаційний.

Науковцями, що досліджують питання інформаційної взаємодії держав, держави та громадян, силових структур та громадян, а також фахівцями, що здійснюють практичну діяльність у цих сферах широко вживаються поняття “пропаганда”, “контрпропаганда”, “інформаційно-психологічний вплив”, “інформаційно-психологічна протидія”, “цивільно-військове співробітництво”, а останнім часом (10-15 років) – “стратегічні комунікації” [1, 2, 3]. Проте, у переважній більшості публікацій, та спецкурсів, не дано порівняльної характеристики механізмів, що забезпечують функціонування феноменів, які могли б бути описані термінами (словами та знаками), що виражають істотні і необхідні характеристики вище перелічених та інших подібних понять.

Метою даної публікації, є визначення ключових тез, що дозволять диференціювати механізми інформаційної взаємодії держав(и) й громадян в галузі безпеки та оборони на різних етапах розвитку теорії та практики.

Дані тези подано у порівняльній таблиці.

Таблиця 1

**Порівняльна таблиця механізмів інформаційної взаємодії держав(и) й громадян в галузі безпеки та оборони**

| Класи характеристик | Технології інформаційної взаємодії держав(и) й громадян в галузі безпеки й оборони та їх характеристики | | | | |
|---|---|---|---|---|---|
| | Пропаганда | Контрпропаганда | Інформаційно-психологічний вплив | Цивільно-військові відносини | Стратегічні комунікації |
| Предмет | ідеологія | ідеї, інформаційні конструкти | процес прийняття рішень | психіка людини та міжособистісні стосунки | відносини між державою та громадянами |
| Мета | вплив на суспільну думку на користь певної спільної справи чи громадської позиції | дискредитація пропаганди | вплив як на свідомість та підсвідомість людей, так і на ту інформацію, на підставі якої приймаються рішення | створення сприятливих умов для військової місії | просування національних інтересів |
| Суб'єкт | спеціальні державні політичні органи та їх представники | спеціальні державні органи та їх представники | органи психологічних операцій | військове командування, та підрозділи | органи державної влади та військового управління |
| Об'єкт | маси | соціальні групи | уряди, організації, групи, і індивідууми | населення в зоні дій військ (сил) | населення країни |
| Мішень впливу | емоції, погляди, думки й дії визначеної, за ознакою приналежності, цільової аудиторії | емоції, погляди, думки й дії визначеної, за результатами ретельного вивчення, цільової аудиторії, а також суб'єкти ворожої пропаганди | погляди, думки, ціннісні орієнтації, настрої, установки, мотиви, стереотипи поведінки людини; групові норми, масові настрої, суспільна свідомість в цілому | психологічні характеристики людини та соціально-психологічні характеристики групи | Довіра громадян до дій влади |

Продовження таблиці 1

| Класи характеристик | Технології інформаційної взаємодії держав(и) й громадян в галузі безпеки й оборони та їх характеристики | | | | |
|---|---|---|---|---|---|
| | Пропаганда | Контрпропаганда | Інформаційно-психологічний вплив | Цивільно-військові відносини | Стратегічні комунікації |
| Способи | контрольована передача односторонніх повідомлень, що поширюють світогляд, теорії, твердження, факти, аргументи, погрози, чутки | прищеплення мислення, що орієнтовано на факти; ізоляція дивергентних (здатних продукувати ідеї) груп | планові дії з передачі відібраної інформації і індикаторів (результатів силового впливу) | організація взаємодії (наради, конференції, круглі столи, зустрічі з лідерами); координація взаємодії з гуманітарними організаціями | синхронізація дій, образів і слів для досягнення бажаного ефекту, врахування інтересів громадян |
| Засоби | взаємодія безпосередня (зустрічі, мітинги) або через канали мас-медіа (листівки, плакати, періодична література, радіо, телебачення, Інтернет тощо) | взаємодія безпосередня (зустрічі, мітинги, арешти) або через канали мас-медіа (листівки, плакати, періодична література, радіо, телебачення, Інтернет тощо) | сили та засоби частин ІПсО та спеціальних підрозділів, медіа-ресурс міжнародного, державного та регіонального рівнів | інформаційні, фінансові, матеріальні ресурси | соціологічні, особистісні, фінансові та матеріальні ресурси |
| Методи | отруєння джерела, багатократне повторення, апелювання до авторитету, апелювання до страху, апеляція до народу, брехня, фальшива дилема, прості люди, когнітивний дисонанс, культ особи, демонізація ворога | капкан, перенос несхвалення або негативного образу, юридична безпека, суспільне несхвалення, імітаційна дезінформація, спростування, ігнорування | маніпулювання, навіювання, дезінформація, обмеження джерел інформації, дестабілізація (провокування сутичок), утруднення прийняття рішень (тиск) | планування, рекомендації, інформування | 80% реальних дій і лише на 20% слів. |

**Література**

1. Баровська А.В. Стратегічні комунікації: досвід НАТО / А. В. Баровська // Стратегічні пріоритети. – № 1 (34). – 2015. − С. 147-152.

2. Попова Т. Стратегічні комунікації у США: 80% реальних дій і лише 20% слів / Тетяна Попова [Електронний ресурс]. Опубліковано 13 жовтня 2017 року. – Режим доступу : http://detector.media/infospace/article/130925/2017-10-13-strategichni-komunikatsii-u-ssha-80-realnikh-dii-i-lishe-20-sliv.

3. Tykhomyrova E.B. Стратегічні комунікації ЄС: інституціональний вимір / Євгенія Борисівна Тихомирова // Науковий журнал "Політичне життя", 2016. – № 4. – С. 103-112.

*УДК: 316.255.01*

**Кожедуб О.В.**
кандидат соціологічних наук, доцент,
Військовий інститут Київського національного
університету імені Тараса Шевченка

## МЕРЕЖНІ ВІЙНИ ЯК РІЗНОВИД ІНФОРМАЦІЙНИХ ВІЙН

Сучасне суспільство, за класифікацією Д. Белла, характеризується як постіндустріальне, або як інформаційне, якому притаманні: інформаційний виробничий ресурс, характер виробничої діяльності характеризується обробкою інформаційних даних, характер технологій є переважно наукомістким, а тип взаємодії характеризується як "людина-людина" [2]. Такі характерні ознаки інформаційного суспільства визначили характер війни [7].

Вперше термін "інформаційна війна" вперше був використаний американським експертом Т. Рона в 1976 р., який наголосив, що інформація стає все більш вразливою ціллю не лише в воєнний час, але й у мирний.

Для інформаційної війни характерні: створення спеціалізованих мобільних підрозділів у різних видах військ, перетворення інформації на інструмент ведення війни, освоєння космічного простору, комп'ютеризація управління на всіх рівнях. При цьому суб'єктами війни стають цивілізації, чиє протистояння пов'язане з фундаментальною інфраструктурою суспільства [3].

Сьогодні, коли українська держава стала активною учасницею не лише традиційних бойових дій, а й інформаційних баталій, увага наукового світу сконцентрована на пошуку дієвих засобів ведення інформаційних операцій.

Як слушно зазначає М. Куц, можливість інформаційного впливу виникла з розвитком технологій та комунікацій, появою інформаційного суспільства та розвитком *глобалізаційних процесів*. Глобалізація є всесвітнім

за масштабом процесом, головною ознакою якого є обширність, широкомасштабність проявів.

Основними наслідками цього процесу виступають розподіл праці, розвиток міждержавних комунікацій, міграція в масштабах усієї планети капіталу, людських та виробничих ресурсів, стандартизація законодавства, економічних та технічних процесів, а також наближення культур різних країн. Це об'єктивний процес, якому притаманний системний характер, тобто він охоплює всі сфери життя суспільства. Глобалізацію часом репрезентують як причинну теорію, тобто певні різновиди глобальних процесів спричиняють певні результати; іноді це ціла низка концепцій, які пояснюють, як слід розуміти глобальну систему; іноді це різновид ідеології [4].

Зазначимо, що сьогодні найшвидшим способом передачі інформації є її передача за допомогою всесвітньої мережі Інтернет, що актуалізує проблематику такого різновиду інформаційних війн як *мережні війни*, які здійснюються у просторі Інтернету.

Інформаційна війна є війною інформаційного суспільства, вона зводить до мінімуму людські втрати. Інформаційним війнам притаманний дистанційний характер. Під час таких війн не використовується зброя масового знищення, натомість відбувається контроль потоків інформації, за допомогою яких змінюється, коректується та впроваджується та чи інша модель мислення та сприйняття у широкі маси. Слід зазначити, що інформація для такої війни може бути як метою, так і зброєю.

Безумовно, виникнення такого нового типу війни пов'язаний із процесом глобалізації, який дає змогу розповсюджувати на великій швидкості та на широкі масштаби ту чи іншу інформацію. *Мережні війни* є специфічним видом інформаційних війн. Використання Інтернету в інтересах війни може як спричиняти позитивні, нешкідливі наслідки, так і руйнувати та завдавати тяжких збитків комп'ютерним технологіям, системам та людям, країнам. Використання хакерських технологій та прийомів підривного характеру задля завдання тяжкої (іноді навіть матеріальної) шкоди несе той негативний відбиток мережної війни, з яким намагається боротися кожна країна окремо та світова спільнота в цілому. Мережні війни поступово витісняють традиційні війни, адже подальший розвиток комунікаційних технологій та технічного прогресу загалом лише сприяє переходу від затратної та чисельної за жертвами війни до мережної війни, яка є набагато вигіднішою та легшою [5].

Одним з об'єктом мережної війни є масова та індивідуальна свідомість. Виокремлюють такі складові впливу на масову та індивідуальну свідомість: дезінформування, лобіювання, маніпулювання, пропаганда, управління кризами, шантаж [6]. Інформаційний вплив в умовах мережних війн містить спотворення фактів або нав'язування аудиторії емоційно-

го сприйняття, яке вигідне агресору. Як правило, дезінформація яка використовується веде до появи почуття страху у населення, що є дієвим фактором зміни моделі поведінки [1].

**Література**

1. Балаев Р.С. Сетевые войны как доминирующий фактор формирования социальных страхов и "экзистенциального вакуума" в современном обществе / Р.С. Балаев // Вестник Адыгейского государственного университета. – 2015. –№ 2 (158). – С. 19-23.

2. Белл Д. Грядущее постиндустриальное общество. Опыт социального прогнозирования: [пер. с англ.] / Даниел Белл. – М. : Academia, 1999. – 956 с.

3. Денисенко І.Д. Сучасні війни: нові підходи та інтерпретації / І.Д. Денисенко // Вісн. Харк. нац. ун-ту ім. В. Н. Каразіна. Серія: Питання політології. – Х., 2008. – № 810. – Вип. 12. – С. 212-218.

4. Куц Г.М. Ідентичність соціальна та індивідуальна: політологічна експлікація / Г.М. Куц // Сучасне суспільство: політичні науки, соціологічні науки, культурологічні науки : зб. наук. пр. – Х., 2013. – Вип. 1 (3). – С. 48-67.

5. Куц М.Ю. Мережні війни: сутність та основні характеристики / М.Ю. Куц // Вісник Національного університету "Юридична академія України імені Ярослава Мудрого". Серія: Філософія, філософія права, політологія, соціологія. – 2015. – № 2(25) – С. 277-286.

6. Манойло А.В. Государственная информационная політика в особых условиях. – М.: МИФИ, 2003.

7. Требін М. П. Інформаційне суспільство: війни нової епохи / М. П. Требін // Віче. – 2002. – № 4. – С. 64–68.

*УДК 323.173*

**Косілова О.І.**
кандидат політичних наук, доцент
Академія Служби безпеки України

## СЕПАРАТИЗМ В УКРАЇНІ: ІНОФОРМАЦІЙНА ТА СОЦІАЛЬНО-ПОЛІТИЧНА СКЛАДОВА

Сепаратизм як ідеологічний, суспільно-політичний, етнічний рух є однією з найбільш гострих загроз національній та політичній безпеці держави, що набуває особливої актуальності у XXI столітті у зв'язку з геополітичними змінами в світі та перерозподілом сфер впливу між новими наддержавами. У сучасних умовах сепаратизм становить безпосередню загрозу національній безпеці України у зв'язку з гібридною війною, що здійснюється Російською Федерацією на південно-східному фронті.

На думку українських дослідників О. О. Резнікової, А. О. Місюри, С. В. Дрьомова, К. Є. Войтовського, сепаратизм − явище, що містить загрозу національній безпеці. Він формується під впливом різних чинників, у т.ч. тих, що пов'язані з процесами трансформації суспільства. Конфлікти найчастіше спалахують тоді, коли загальне соціально-економічне становище в країні різко змінюється на гірше та (або) коли настає політична нестабільність [1, с. 37]. На політичній складовій сепаратистського руху акцентує Р. Ключник: «…виникнення сепаратистського руху можливе за наявності двох умов: дискримінації етнічної спільноти з боку державної влади та формування активної політичної еліти, здатної очолити цей рух» [2, с. 121]. При чому дискримінація може бути як політична так і економічна. Політична дискримінація означає, що дана етнічна одиниця позбавлена політичних прав, на відміну від домінуючої більшості. Економічна дискримінація призводить до ситуації «внутрішньої колонії», коли певна частина території перетворюється на своєрідного економічного донора.

Велику роль у розгортання сепаратистських процесів в Україні відіграла цілеспрямована ідеологічна та інформаційна діяльність Російської Федерації та її агентів щодо підриву національної єдності та легітимності Української держави. Зокрема, одним із важливих факторів, що спричинив появу сепаратистських настроїв у Східному регіоні та в Автономній Республіці Крим є інформаційний вплив Російської Федерації на фоні слабкого рівня економічного розвитку та дотаційності регіону. Як вважає О. Карпец, до причин виникнення сепаратизму на Сході України, належить також соціально-класова складова, яку умисно замовчують. Значна кількість населення неконтрольованої частини Донбасу, принаймні на початку конфлікту, вважала, що виступає проти панівної в Україні разючої соціальної несправедливості, проти політичної та майнової нерівності, нарешті, проти експлуататорського класу, за якесь справедливе, без експлуатації людини людиною, суспільство, яке, на їхню думку, має бути встановлено у «Новоросії» [3]. Таким чином, приєднання до Російської Федерації вбачалася частиною населення Донецької та Луганської областей як шлях до покращення матеріального достатку та асоціювалося з поверненням до колишнього СРСР.

Порівнюючи чинники появи сепаратизму в Україні з тенденціями в інших державах, українські дослідники наголошують, що сепаратизм на Сході України має низку особливостей.

По-перше, він не є результатом внутрішньодержавного конфлікту на міжетнічному, міжконфесійному або іншому ґрунті. Протягом всієї історії незалежної України на цій території не спостерігалися системні організовані сепаратистські рухи з визнаними лідерами та широкою підтримкою з боку населення, а також відсутні райони компактного проживання представників окремих народів, етнічної або конфесійної групи.

По-друге, ідеологічні основи такого сепаратизму були розроблені за межами України у вигляді проекту «Русский мир». Організаційне і фінансове забезпечення діяльності квазідержавних утворень «ДНР» і «ЛНР» та-

кож здійснюється переважно з території Росії за постійного контролю з боку кураторів від уряду РФ і ФСБ. Безпосередню участь у бойових діях на території Донбасу беруть регулярні підрозділи ЗС РФ, що відповідно до міжнародного права розцінюється як неспровокована збройна агресія РФ проти України [4, с. 7].

Підводячи підсумки, слід зазначити, що подолання сепаратизму в Україні має здійснюватися з використанням всіх видів методів, враховуючи особливості регіонів (насильницькими, ненасильницькими та превентивними), але перевагу слід надавати все ж таки ненасильницьким, політичним методам. Зважаючи на особливості сепаратизму в Україні, його «гібридний характер», доцільним також є посилення інформаційної, ідеологічної (виховання патріотично-свідомої молоді, культивування української мови та культури) та пропагандистської роботи на територіях, на яких фіксуються ознаки сепаратизму та потенційно-небезпечних територіях. Запобігання поширенню та подолання сепаратизму в Україні на сучасному етапі значною мірою залежить від забезпечення легітимності державної влади, визнання законності застосування нею сили до населення у разі необхідності. Легітимність державної влади є міцною за умов формування правової держави та забезпечення політичної безпеки.

**Література**

1. Міжнародний досвід боротьби з сепаратизмом: висновки для України : аналіт. доп. / О. О. Резнікова, А. О. Місюра, С. В. Дрьомов, К. Є. Войтовський. – К. : НІСД, 2016. – 46 с.

2. Ключник Р. Сепаратизм як світова мегатенденція сучасності/Р. Ключник // Політичний менеджмент. – 2011. – № 6. – С. 120–128.

3. Карпец А. Сепаратизм в Україні та його соціальні причини http://eizvestia.com/uk/politika-ukr/full/706-separatizm-v-ukraini-ta-jogo-socialni-prichini).

4. Резнікова О. О., Дрьомов С. В. Деякі законодавчі аспекти протидії сепаратизму в Україні // Стратегічні пріоритети, 2016. – №3(40). – С. 18-25.

*УДК 35.077*

**Котляренко О.П.**
кандидат юридичних наук, полковник юстиції
Національний університет оборони України
імені Івана Черняховського

## РОЗВИТОК СТРАТЕГІЧНИХ КОМУНІКАЦІЙ У ВОЄННІЙ СФЕРІ

Застосування Російською Федерацією технологій гібридної війни проти України перетворило інформаційну сферу на ключову арену протиборства. Саме проти України Російська Федерація використовує найновіші інформаційні технології впливу на свідомість громадян, спрямовані на

розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України [1].

З розвитком сучасних інформаційних технологій, зростання ролі інтернет-видань та соціальних мереж, інформаційна складова стає повноцінною зброєю. Поширення ворогом неправдивої інформації через засоби масової інформації набувають все більшого впливу на думку громадськості, противник все частіше робить ставку саме на порушення комунікації як внутрішньої, так і зовнішньої, що може мати не менш руйнівні наслідки, ніж збройна агресія. Моніторинг та аналіз інформаційного простору допомагають своєчасно виявити, розпізнати, охарактеризувати, класифікувати виникаючі загрози та попередити їх негативний вплив. Узгоджене та своєчасне застосування стратегічних комунікацій має вирішальне значення у протистоянні загрозам в інформаційному просторі, стає джерелом активного розповсюдження інформації у засобах масової інформації та реагування на поширення неправдивої інформації.

У Воєнній доктрині України, затвердженій Указом Президента України від 24 вересня 2015 року № 555, визначено: «стратегічні комунікації – це скоординоване і належне використання комунікативних можливостей держави – публічної дипломатії, зв'язків з громадськістю, військових зв'язків, інформаційних та психологічних операцій, заходів, спрямованих на просування цілей держави». Серед основних напрямків практичної діяльності, які охоплюються сферою стратегічних комунікацій, слід також згадати інформаційні заходи під час реалізації проектів цивільно-військового співробітництва, розвідувальне забезпечення реалізації стратегічних комунікацій, документування подій, діяльність у кіберпросторі і соціальних мережах, безпека операцій, залучення ключових лідерів та багато іншого.

Не випадково у Воєнній доктрині України чітко закріплено, що Україна розглядає посилення розвідувальної діяльності в інтересах підготовки та проведення Україною стратегічних комунікацій, контрпропагандистських заходів та інформаційно-психологічних операцій, як основу кризового реагування на воєнні загрози та недопущення ескалації воєнних конфліктів. Водночас передбачено, що забезпечення інформаційної складової воєнної безпеки здійснюватиметься шляхом запровадження ефективної системи заходів стратегічних комунікацій у діяльність органів сектору безпеки.

Причому стратегічні комунікації доцільно розглядати в двох аспектах: 1) як напрям державної політики; 2) як напрям підготовки відповідних фахівців (страткомівців). Тому потрібні організаційні структури, які забезпечать набуття Збройними Силами України (ЗС України), іншими складовими сектору безпеки і оборони необхідних оперативних спроможностей, у т.ч. наукових та освітніх.

Для виконання цих завдань слід мати законодавчу базу, яка б дала поштовх створенню інституційних структур. Необхідну основу ми знаходимо в Дорожній карті Партнерства у сфері стратегічних комунікацій між РНБО України та Міжнародним секретаріатом НАТО, яка підписана 22 вересня 2015 року [2]. У документі, зокрема, декларується «сприяння розвитку в Україні культури стратегічних комунікацій на інституційному рівні». На пріоритетності стратегічних комунікацій у воєнній сфері наголошується в ряді інших документів.

Концепція стратегічних комунікацій Міністерства оборони України та ЗС України визначає, що основними цілями розвитку стратегічних комунікацій є: формування довіри українського суспільства до воєнної політики держави, підтримка ним реформ у воєнній сфері та курсу з набуття Україною членства в НАТО; скоординованість дій державних органів та інших учасників стратегічних комунікацій під час об'єктивного інформування суспільства з питань, що стосуються оборони держави, підготовки і застосування ЗС України [3].

Звернемо увагу, що у цій Концепції проведений розподіл функцій між основними суб'єктами стратегічних комунікацій, зокрема зазначено: загальну координацію здійснює помічник Міністра оборони України (прессекретар) через Відділ координації стратегічних комунікацій та моніторингу, який в свою чергу, спрямовує, координує та синхронізує загальні зусилля з комунікації всіх суб'єктів системи; демонстрація дій військ здійснюється командуваннями видів та окремих родів військ (сил) ЗС України; внутрішня комунікація реалізується Головним управлінням морально-психологічного забезпечення ЗС України; оперативне планування та управління веденням інформаційних операцій здійснюють Головне оперативне управління Генерального штабу ЗС України та Об'єднаний оперативний штаб ЗС України; розвідувальне забезпечення проведення інформаційних заходів здійснюється Головним управлінням розвідки Міністерства оборони України; психологічні операції відносяться до компетенції Командування Сил спеціальних операцій ЗС України; проведення операцій (дій) в кіберпросторі сьогодні відноситься до функцій військ зв'язку ЗС України; заходи цивільно-військового співробітництва проводяться під керівництвом Управління цивільно-військового співробітництва ЗС України.

Практика доводить, що нові виклики національній безпеці обумовлюють нагальну необхідність пошуку інструментарію, за допомогою якого стане можливою організація узгодженої взаємодії ЗС України з іншими військовими формуваннями та державними органами. Дієвим, адекватним та комплексним інструментарієм такої взаємодії виступає система стратегічних комунікацій, яка дає можливість, залишаючись у межах демократичних практик і принципів, організувати ефективну відсіч деструктивним інформаційним кампаніям агресора.

**Література**

1. Доктрина інформаційної безпеки України, затверджена Указом Президента України від 25 лютого 2017 року № 47. URL: http://zakon2.rada.gov.ua/laws/show/47/2017.

2. Дорожня карта Партнерства у сфері стратегічних комунікацій між Радою національної безпеки України та Міжнародним секретаріатом НАТО. URL: http://mfa.gov.ua/mediafiles/sites/nato/files/Roadmap_Ukr.pdf.

3. Концепція стратегічних комунікацій Міністерства оборони України та Збройних Сил України, затверджена наказом Міноборони від 22 листопада 2017 року № 47. URL: www.mil.gov.ua/content/mou_orders/612_nm_2017.pdf.

*УДК 323:351+316.77*

**Крисяк П.В.**
Воєнно-дипломатична академія
імені Євгенія Березняка

# ІНФОРМАЦІЙНО-ПРОПАГАНДИСТСЬКИЙ ВПЛИВ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ НА НАСЕЛЕННЯ ІНОЗЕМНИХ КРАЇН (НА ПРИКЛАДІ РОБОТИ «ФАБРИКИ ТРОЛІВ»)

Гібридний метод агресії, який застосовує Російська Федерація не лише до України, але й до демократичних держав загалом, поступово знищує зрозумілий нам світовий порядок. Системна дискредитація міжнародного права, поновлення проблеми кордонів, перетворення міграційних процесів на зброю, знищення довіри до медійних систем, новий після «холодної війни» виток пропаганди – лише невелика частина тих процесів, які формуються та підтримуються Російською Федерацією.

Незважаючи на, здавалося б, масштабні викриття російської пропаганди як окремими авторами, так і цілими колективами дослідників, незважаючи на те, що постійно приймаються рішення про «протидію» російській пропаганді, ми продовжуємо стикатися з цим феноменом практично в тих же масштабах, що і раніше. Спроби протидіяти, на кшталт історії з не допуском журналістів Sputnik і RT на зустрічі керівників ЄС чи керівників держав-членів ЄС, носять епізодичний характер.

В той же час, як зазначає Д.Дубов: «…видима частина «айсберга російської пропаганди» (Sputnik, RT, кібератаки і використання соціальних мереж) куди менша від тієї планомірної і масштабної «підводної частини», яка майже не привертає уваги громадськості: робота з експертною думкою, робота з іноземної молоддю, відновлення мережі організацій прикриття, розгортання «культурних центрів» в західних країнах, залучення в свої компанії західних же артистів, художників і режисерів» [1].

З огляду на викладене дослідження так званої «підводної частини айсберга російської пропаганди» є актуальною темою.

Одним з елементів «гібридної війни», яку протягом останніх років російські спеціальні служби ведуть проти України та її партнерів – країн західної демократії, є діяльність так званих «фабрик тролів».

Специфіка роботи російських спеціальних служб полягає в тому, що за допомогою «фабрик тролів», що фінансуються і контролюються урядом РФ, вони намагаються сформувати в інформаційному полі країн Європи політичні «групи підтримки», які б просували альтернативну проросійську думку.

Зокрема, колишній працівник так званої «фабрики тролів» у РФ Марат Міндріянов відкрито розповів про особливості її функціонування. Публікація наробила галасу на тлі нещодавніх заяв прокуратури США про російське втручання в американські вибори. Він працював у «фабриці тролів» з листопада 2014 року по лютий 2015. В інтерв'ю він розповів – її працівники з фейкових акаунтів масово поширювали пропаганду у соцмережах [2].

В мережі Інтернет останніми днями активно обговорюється обвинувачення, висунуте спеціальним прокурором Мюллером, яке сфокусоване лише на аспекті Russiagate – втручанні Росії в американську виборчу кампанію та політичне життя шляхом розповсюдження пропаганди та фейкових даних через соціальні мережі та інші Інтернет-ресурси, а також шляхом організації в США провокаційних демонстрацій та мітингів з ціллю посіяти розбрід між різними соціальними, релігійними та етнічними групами населення, а також з ціллю здійснення підтримки одним кандидатам в президенти та шельмування інших кандидатів в президенти [3].

В обвинувальному висновку детально описується організаційна структура створеної у 2013 році фабрики тролів «Internet Research Agency», широко відомої як «ольгінська фабрика тролів», яка активно працює з часу свого заснування. 12 з 13-ти обвинувачених громадян Росії є співробітниками цієї фабрики, а 13-ий – Євгеній Пригожин, який обвинувачується у фінансуванні діяльності цієї ферми тролів.

Таким чином, можемо констатувати, що війна в інформаційному просторі тільки набирає обертів, а значить є сенс вивчати тактику та стратегію супротивника, щоб наносити випереджувальні удари.

Ми повинні визнати, що знаходимося в самому розпалі нової «холодної війни», де інформаційна складова стала ще більш значущою, ніж у попередній.

**Література**

1. Дубов Д. Инструменты российской пропаганды: старые песни на новый лад. URL: http://www.russkiivopros.com/index.php?pag=one&id= 740&kat=5&csl=83. (дата звернення 12.02.2018).

2. Російська «фабрика тролів»: Колишній працівник розкрив подробиці його роботи. URL: https://24tv.ua/mizhnarodni_novini_tag1121. (дата звернення 23.02.2018)

3. Спеціальний відділ фабрики тролів РФ для підривних пропагандистських операцій в США. URL: https://www.obozrevatel.com/ukr/ my/politics/spetsialnij-viddil-fabriki-troliv-rf-dlya-pidrivnih-propagandistskih-operatsij-v-ssha.htm. (дата звернення 26.02.2018).

*УДК 004.89: 004.912*

**Кубявка М.Б.**
кандидат технічних наук
Військовий інститут КНУ ім. Тараса Шевченка
**Кубявка Л.Б.**
кандидат технічних наук
факультет інформаційних технологій
КНУ ім. Тараса Шевченка

## ПРО ВПЛИВ, ЯКИЙ ЗМІНЮЄ І ПОВІДОМЛЕННЯ, І ЙОГО ЗМІСТ

Ще з часів К.Шеннона відомо, що впливи можуть бути двох основних типів:

– вплив безпосередньо на повідомлення, на їхню форму, механізми передачі, збереження, обробку тощо;

– вплив на зміст повідомлень.

Сьогодні можна говорити ще про один вплив, який змінює і повідомлення, і його зміст. Це несиловий (інформаційний) вплив на джерело повідомлення з метою вироблення у нього реакції, що відповідає цілям впливу. Саме такий вплив може бути реалізований із застосуванням теорії несилової взаємодії, яка дає досить чіткий математичний інструментарій для визначення найбільш ефективних способів інформаційного впливу [1].

В поняттях теорії несилової взаємодії представлено атрибути «м'якої сили». Основним таким поняттям є поняття інтроформації. Під інтроформацією розуміється внутрішня організація взаємодіючих об'єктів, яка формує їх відношення до дійсності і проявляється у їх діях. Щоб досягти потрібного впливу необхідно спочатку змінити відношення до дійсності у цільової аудиторії (об'єкта впливу). А це досягається зміною їх інтроформації. В свою чергу для зміни інтроформації необхідно щоб на контрагента здійснювались інформаційні (несилові) впливи.

Як слідує з теорії будь-який несиловий вплив призводить до змін у внутрішньому стані об'єкта впливу, що, в свою чергу, призводить до змін в його поведінці.

Так, саме змінюючи відношення об'єкта впливу (цільової аудиторії) до отриманої інформації за рахунок певних інформаційних методик певною мірою можна досягти бажаного ефекту. Не зважаючи на бажання ініціатора, а лише зважаючи на деякі виключення (специфіку) відносно якої здійснюється цей (цільовий) вплив.

Найбільш розповсюдженим запитанням, яке виникає при пошуку такого рішення є, а яким чином це здійснити.

Саме спираючись на математичний апарат теорії несилової взаємодії та основні її аксіоматичні твердження було розроблено інформаційну технологію супроводження несилового впливу, яка визначає, яку інформацію і кому та в якому обсязі краще надати, яка формує необхідне відношення до певних знань у цільової аудиторії не з позицій максимального її інформування, а з позиції потрібної інформаційної дії на неї [2].

**Література**

1. Тесля Ю.Н. Введение в информатику Природы / Юрий Тесля. – К. : Маклаут, 2010. – 256 с.

2. Кубявка М.Б. Моделі та методи управління інформаційним супроводженням в умовах гібридної війни : автореф. дис... канд. техн. наук: 05.13.06 / М.Б.Кубявка. – К., 2017. – 24 с.

*УДК 316.34*

**Кухарська Н.П.**
кандидат фізико-математичних наук, доцент
Львівський державний університет безпеки життєдіяльності

## ПРОБЛЕМА ОСОБИСТІСНОЇ ІДЕНТИФІКАЦІЇ В ІНТЕРНЕТ-СЕРЕДОВИЩІ

Останнім часом ми все частіше пов'язуємо свою професійну діяльність, освіту, дозвілля з мережею Інтернет. Нині для сотень мільйонів людей соціальні мережі стали повсякденним обов'язковим елементом життя. Людство перетнуло межу і перейшло від моделі двох світів – реального і віртуального – до світу змішаної реальності. Поєднання непоєднуваного стало частиною життя сучасної людини.

Ще у 1990 році віртуальна реальність розглядалась як деякий штучний всесвіт, замкнений всередині комп'ютера. З того часу проходить лише шість років і соціолог Мануель Кастельс у своїй тритомній праці "Інформаційна епоха: економіка, суспільство і культура" (1996-1998 рр.) [1-3] вже говорить про зародження нової культури "реальної віртуальності".

Сьогодні процес конвергенції реального і віртуального набирає темпу. Ми стаємо свідками зародження епохи інтернету речей. Від смартфо-

нів ми стрімко рухаємося до розумного будинку, розумного міста, розумної країни і, зрештою, розумної планети.

В умовах поширення мобільних засобів комунікації і мережі Інтернет, які дають можливість бути на зв'язку 24 години на добу 7 днів на тиждень, стираються кордони між особистим, сімейним і робочим часом. Порушується послідовність соціальних практик.

Віртуальна реальність змінює поведінку людей, а, отже, і їх самих. У соцмережах ми може придумати собі цілком нові "амплуа", нове життя. І ніхто, і ніщо нас у цьому не обмежує. Ми живемо у світі усюдисущих аватарів, намагаємось знайти відповідь на питання "Хто Я?" і "заводимо" по кілька аккаунтів у різних соціальних мережах. Наші цифрові двійники загострюють і без того складну проблему людської ідентичності.

Соціальні мережі – це свого роду meeting point для її користувачів, гарне місце для розмов про себе та інших, самопрезентування, вироблення і демонстрації своєї позиції чи позиції тієї групи, від імені якої виступає користувач. Тут можна виражати свої емоції, сперечатися і погоджуватися, тут здобувають прихильників і супротивників.

Мережа Інтернет, соціальні мережі, як комунікаційні середовища володіють специфічними властивостями, що використовуються їх користувачами сповна. А саме:

•Властивість анонімності Інтернет-комунікацій сприяє психологічній розкутості їх учасників, спонукає до більшої свободи у висловлюваннях та поступках, дає змогу користувачам "втекти від власного тіла", керувати враженнями оточуючих про себе, конструювати свій образ на свій вибір, програвати нереалізовані у реальному житті ролі та сценарії і при цьому не зважати на усталені у суспільстві норми. Анонімність Інтернет-комунікацій має кілька граней, наприклад, можна висловлювати почуття, можна приховувати їх, а можна висловлювати почуття, які людина на даний момент і не відчуває.

•Своєрідність протікання в Інтернет-середовищі процесів міжособистісного сприйняття: територіальна доступність, фізична привабливість, стать, вік, соціальний статус співрозмовника не відіграють ніякого значення, спілкування будується на основі подібності поглядів, переконань і цінностей.

•Добровільність контактів і завжди існуюча можливість у будь-який момент перервати зв'язок і назавжди зникнути в Мережі, що не має кордонів, дозволяє людям бути більш відвертими і розкутими, ніж у реальності.

Непомірне захоплення Інтернетом, доведено наукою, посилює соціальну ізоляцію індивіда, і, відповідно, відчуття самотності. Залежність від онлайн-спілкування провокує виникнення "самотності в натовпі".

Слід задуматися: чи варто заміщувати оф-лайн-відносини віртуальними? Чи така заміна є повноцінною? Незважаючи на те, що віртуальне

спілкування має багато плюсів, переваги живого спілкування більш вагомі. Віртуальна не замінить реальну комунікацію. Користувачам соціальних мереж слід припинити, надмірно захоплюючись пропонованими Інтернетом можливостями, відкладати реальне життя на потім, потрібно жити тут і зараз.

**Література**

1. Castells Manuel The Information Age: Economy, Society and Culture / Castells Manuel. – Oxford: Blackwell. – . – Vol. I: The Rise of the Network Society. – 1996. – 556 pp.

2. Castells Manuel The Information Age: Economy, Society and Culture / Castells Manuel. – Oxford: Blackwell. – . – Vol. II: The Power of Identity. – 1997. – 460 pp.

3. Castells Manuel The Information Age: Economy, Society and Culture / Castells Manuel. – Oxford: Blackwell. – . – Vol. III: End of Millennium. – 1998. – 448 pp.

4. Кухарська Н. П. Загрози безпеці дітей у соціальних мережах / Н. П. Кухарська, В. М. Кухарський // Безпека інформації. – 2014. – Т. 20, № 2. – С. 169-175.

*УДК 004.415.2*

**Лоза В.М.**
кандидат технічних наук
**Лалетін С.П.**
**Дяченко І.М.**
Військовий інститут Київського національного
університету імені Тараса Шевченка

## ВИЗНАЧЕННЯ ТОНАЛЬНОСТІ ТЕКСТОВОЇ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ МЕТОДУ ШТУЧНИХ НЕЙРОННИХ МЕРЕЖ В ЗАДАЧІ ВИЯВЛЕННЯ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ ВПЛИВІВ

Основною метою аналізу тональності є знаходження думок у тексті і виявлення їх властивостей. Які саме властивості будуть досліджуватися залежить вже від поставленого завдання. Тональність тексту визначається трьома факторами: суб'єкт тональності (автор, тобто кому належить це думка), об'єкт тональності і його властивості (сутність, щодо якої висловлюється автор), власне тональна оцінка (емоційна позиція автора щодо згаданої теми).

На відміну від пропагандистського впливу, інформаційно-психологічний вплив здійснюється, головним чином, на емоційну сферу свідомості. Інформаційно-психологічний вплив на емоційну сферу здійснюється на основі некритичного сприйняття інформації особистістю. Тобто, на відміну від пропагандистського впливу, він базується на відносно

низькому рівні критичності й свідомості психіки індивіда (при цьому його установки не змінюються). Зниження рівня усвідомленості є однією з умов ефективності даного впливу. У процесі прийняття інформації функціонує тільки сприйняття й запам'ятовування, діяльність мислення «випадає» або дуже послабляється.

Проаналізувавши основні аспекти текстової інформації, та аспектів її можливого користування – приходимо до висновку, що на основі різноманітних підходів можна проводити детальний аналіз інформації, створювати системи для масового інформування населення, та застосовувати їх в комплексному використанні для повсякденних цілей та у спеціальних завдань спеціалізованих галузей. В умовах великого поширення інформації серед населення та зокрема у засобах масової інформації, необхідно правильно її аналізувати. Для того, щоб робити це безпомилково, необхідно використовувати програмні засоби, як такі, які забезпечують максимальну точність навіть при великій кількості інформації яку потрібно проаналізувати.

У сучасних системах автоматичного визначення емоційної оцінки тексту найчастіше використовується одномірний емотивний простір: позитив чи негатив (добре чи погано). Однак відомі успішні випадки використання і багатовимірних просторів. Приклади тональних оцінок: позитивна, негативна, нейтральна. Під «нейтральна» мається на увазі, що текст не містить емоційного забарвлення. Також можуть існувати й інші тональні оцінки.

Найбільшого поширення для виконання поставленої задачі набули лексемний метод, наївний класифікатор Баєса, метод опорних векторів, метод максимальної ентропії, логістична регресія та штучні нейронні мережі. Недоліком методу опорних векторів є те, що від здійснює бінарну класифікацію, яка дозволяє розділити дані на дві категорії: дані без інформаційно-психологічних впливів та дані з інформаційно-психологічними впливами. Основний недолік наївного класифікатора Баєса – неможливість врахування залежності результату від комбінації ознак (слів). Спільним недоліком лексемного методу, наївного класифікатора Баєса та методу максимальної ентропії є необхідність складання словників, що вимагає тісної співпраці з лінгвістами.

Проведені дослідження методів автоматичного аналізу тональності текстової інформації показало, що найбільш придатним для виявлення у текстовій інформації інформаційно-психологічних впливів є нейронні мережі, оскільки вони не потребують складання словників, обов'язкової попередньої лінгвістичної обробки текстів, можуть застосовуватись до різних типів даних та здатні здійснювати класифікацію за декількома категоріями, що дозволяє виявляти різні типи інформаційно-психологічного впливу.

Штучні нейронні мережі (Artificial Neural Network) – це адаптивна система, яка складається з групи з'єднаних штучних нейронів. Система може бути навчена для зміни її внутрішніх станів, відображення зв'язків документів та їх категорій. Для ефективного проведення класифікації текстів необхідно визначити раціональну структуру і топологію нейронної мере-

жі. Основні топології класифікуючих нейронних мереж – це одно- і багатошаровий персептрон, нейромережевий Гаусів класифікатор, мережа Кохонена, мережа вбудованого розповсюдження, каскадна мережа. Всі вищевказані топології мають високу точність в обробці одночасно лінійних і нелінійних прикладів, але прийняття рішень щодо класифікації важко формалізуються у зв'язку з природою організації нейронної мережі та представляють нетривіальну задачу з урахуванням масштабованості з обмеженими обчислювальними ресурсами.

Перевагами застосовуваного методу нейронних мереж є: можливість рішення задач при невідомих закономірностях, стійкість до шумів у вихідних даних, здатність до навчання. Алгоритми навчання штучних нейронних мереж поділяються на алгоритми навчання з учителем та без учителя. Навчання нейронної мережі в першу чергу полягає в заміні вагових коефіцієнтів синаптичних зв'язків між нейронами. Для аналізу тональності текстових даних, доцільно застосовувати глибоке навчання рекурентних нейронних мереж, яке не викликає складнощів із перенавчанням, на відміну від згороточних та повнозв'язних зв'язків між нейронами. Однак при навчанні нейронних мереж часто виникає проблема перенавчання (overfitting). Перенавчання виникає в разі занадто довгого навчання, недостатньої кількості навчальних прикладів або переускладненої структури нейронної мережі. Один з варіантів боротьби з перенавчанням мережі – поділ навчальної вибірки на дві множини (навчальну і тестову). На навчальній множині відбувається навчання нейронної мережі. На тестовій множині здійснюється перевірка побудованої моделі.

**Література**

1. Галушкин А. И. Теория нейронных сетей. – М.: ИПРЖР, 2000. – 416 с.

2. Круглов В. В., Борисов В. В. Искусственные нейронные сети. Теория и практика. 2-е изд. – М.: Горячая линия–Телеком, 2002. – 382 с.

3. Lakkaraju H., Socher R., Manning C. Aspect Specific Sentiment Analysis using Hierarchical Deep Learning // NIPS Workshop on Deep Learning and Representation Learning. – 2014.

*УДК 35:001.8:303.833*

**Марутян Р.Р.**
кандидат історичних наук, доцент
Національна академія державного управління
при Президентові України

## СТРАТЕГІЧНІ КОМУНІКАЦІЇ: ПОНЯТТЯ, ЦІЛІ, ЗАВДАННЯ

Концепція «стратегічної комунікації» (strategic communication, stratcom – СК) з'являється в США на початку XXI століття. 16 березня 2010 року у доповіді Білого Дому Конгресу США «Національні рамки

стратегічних комунікацій» визначаються основні цілі, завдання і організаційні форми СК США. У діючої стратегічній концепції НАТО, що була затверджена на саміті в Лісабоні в листопаді 2010 року приводиться наступне визначення стратегічних комунікацій: «...скоординоване і належне використання комунікативних можливостей НАТО: публічної дипломатії, зв'язків з громадськістю, PR-служби ЗС, інформаційних і психологічних операцій для підтримки політики альянсу і заходів, направлених на просування цілей НАТО» [5].

У Воєнній доктрині України, «стратегічні комунікації» визначаються як скоординоване і 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].

Російська історіографія з цього питання стверджує, що стратегічна комунікація – це проектування державою в свідомість національних і зарубіжних цільових аудиторій певних стратегічних цінностей, інтересів і цілей шляхом адекватної синхронізації різносторонньої діяльності у всіх сферах суспільного життя з її професійним комунікаційним супроводом» [2].

За К. Халлаханом СК – це, перш за все, «спосіб переконати інших людей прийняти ваші ідеї, політику або дії. Ціллю СК є: переконати союзників і друзів залишитися з вами; переконати нейтралів зайняти вашу сторону (або, принаймні, залишитися нейтральними); переконати противників, що у вас є сили і воля для домінування» [4].

Ще наочніше операційні цілі стратегічної комунікації були прописані в документі, складеному співробітниками Міжвидового командування збройних сил США: «Стратегічна комунікація є системою довготривалих і узгоджених дій, що реалізовується на стратегічному, оперативному і тактичному рівнях, яка дозволяє виявити цільові аудиторії, визначити ефективні канали дії на них для того, щоб забезпечити необхідну стійку поведінку цих аудиторій» [3].

Стратегічна комунікація здійснюється в трьох основних формах: зв'язки з громадськістю, публічна дипломатія і інформаційні операції. При цьому, всі складові повинні діяти синхронно, але при цьому мають свої особливості.

Так, зв'язки з громадськістю орієнтовані, перш за все, на інформування зовнішнього реципієнта і повинні в значній мірі відповідати його базовим світоглядним установкам, іншими словами, говорити з ним на одній мові понять і символів.

Істотним доповненням зв'язків з громадськістю повинна стати публічна дипломатія, що включає «зусилля по прямій взаємодії з громадянами, громадськими діячами, журналістами і іншими лідерами громадської думки за межами країни. Публічна дипломатія доповнює традиційну міждер-

жавну дипломатію, в якій переважає офіційна взаємодія професійних дипломатів. Неформальний характер публічної дипломатії значно спрощує процес взаємодії з громадянами іншої держави та формує позитивне відношення до політики і національних інтересів країни, спонукає до дій в їх підтримку.

Третьою формою стратегічної комунікації є інформаційні операції, під якими розуміють «інтегроване використання радіоелектронної війни, комп'ютерних мережевих операцій, психологічних операцій, маніпулювання у військових цілях і оперативної безпеки, включаючи їх супутні і прикладні аспекти, з метою вплинути, зруйнувати, зіпсувати або перехопити процес людського або автоматизованого ухвалення рішення противником» [2].

Стратегічна комунікація покликана забезпечити політику держави за межами національних кордонів. Основним об'єктом дії є певна цільова аудиторія - політична (економічна, наукова, культурна тощо) еліта тієї держави, відносно якої робляться відповідні дії.

Результатом дії є формування в цільової аудиторії такої системи стійких уявлень про дії іншої держави, які б повністю виправдовували дані дії. Тим самим забезпечується лояльність політичної еліти держави, на яку направлена дана дія, а, отже, і формування дієвої системи геополітичного контролю над заданою територією.

**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. Пашенцев Е.Н. Стратегическая коммуникация США: «Имперское перенапряжение сил» // Мир и политика [Электронный ресурс]. URL: http:// ch.bief2015.com/1317-strategicheskaya-kommunikaciya-ssha-imperskoeperenapryazhenie-sil.html.

3. Commander's Handbook for Strategic Communication and Communication Strategy Version 3.0. US Joint Forces Command Joint Warfighting Center. 24 June 2010 [Электронный ресурс]. URL: http://www.dtic.mil/doctrine/doctrine/jwfc/sc_ hbk10.pdf (дата обращения : 11.06.2016 г.).

4. Hallahan K., Holtzhausen D., Van Ruler B., Vercic D., Siramsh K. Defining Strategic Communication // International Journal of Strategic Communication. – 2007. № 1. –P. 3–35.

5. National Framework for Strategic Communication. The White House, Washington. 2010 // FAS – Federation of American Scientists [Official Site]. URL: https://fas.org/man/eprint/pubdip.pdf (accessed: 07.02.2017).

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

# ЩОДО ПРОТИДІЇ ВИКОРИСТАННЮ ІНТЕРНЕТ-РЕСУРСІВ ДЛЯ ПОШИРЕННЯ АНТИУКРАЇНСЬКОЇ ІНФОРМАЦІЇ

Указом Президента України від 15.05.2017 № 133/2017 (далі – Указ № 133/2017) введено в дію рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)», яким російські соцмережі «Вконтакте» та «Одноклассники» і інформаційні сервіси («Mail.ru» і «Yandex») внесені до санкційного списку [1].

Такий захід фактично став протидією актуальним на сьогодні загрозі національним інтересам в інформаційній сфері, якими на державному рівні визнаються:

– здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу Збройних Сил України та інших військових формувань, провокування екстремістських проявів, підживлення панічних настроїв, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні;

– поширення закликів до радикальних дій, пропаганда автономістських концепцій співіснування регіонів в Україні [2].

Зазначений Указ № 133/2017 створив правові передумови для протидії використанню інтернет-ресурсів для поширення антиукраїнської інформації, що порушує чинне законодавство України та спрямоване на розпалювання ворожнечі, закликає до повалення існуючого ладу, пропагує насильство тощо. Його прийняття в цілому підтримано переважною більшістю лідерів громадської думки та експертів. Із зареєстрованих в Реєстрі операторів, провайдерів телекомунікацій НКРЗІ в Україні понад 6 тис. юридичних осіб, що надають послуги доступу до Інтернет, переважна більшість припинила доступ своїх клієнтів до заборонених ресурсів.

Більшість громадян України також відмовилась від користування російськими соціальними мережами. Значний вплив на це має висвітлення результатів протидії СБ України інформаційній агресії РФ, що підкріплювались прикладами викриття деструктивних груп у соцмережах, їх використання спецслужбами РФ для підбурювання населення до участі в масових акціях протесту, збирання розвідувальної інформації тощо на шкоду національній безпеці України.

За оцінками закордонних експертів, протягом першого місяця дії санкцій відвідування українськими користувачами заборонених російських Інтернет-ресурсів знизилось на третину, загальний обсяг їх трафіку впав на 10%, фіксується стабільна динаміка до зменшення чисельності користувачів російських Інтернет-сервісів в Україні, що в сукупності послаблює вплив країни-агресора на українську аудиторію. Спостерігається зростання міграції патріотично налаштованих користувачів до інших соціальних мереж, насамперед, до «Facebook», а також до вітчизняних соціальних мереж «Ц.укр», «UkrOpen», «Hurtom.com», «ukrface.com.ua», «Ukrainians». Так, за результатами експертних досліджень серед Інтернет-користувачів (за даними SimilarWeb, TNS KantarCMeter [3, 4]), станом на кінець травня 2017 року активна українська аудиторія російських соціальних мереж «ВКонтакте» та «Одноклассники», а також порталу Mail.ru та пошуковикаYandex орієнтовно зменшилася на 5% (втрата понад 1 млн. користувачів соцмереж та 50% користувачів сервісів Mail.ru та Yandex). Водночас, аналіз добової відвідуваності ресурсу «ВКонтакте» станом на той же період часу вказує на скорочення української аудиторії на 3,35 млн. користувачів (18,1%). Охоплення українською аудиторією мережі «Одноклассники» зменшилося на 1,67 млн. відвідувачів (29,6%). On-Line присутність користувачів з України в російських соцмережах зменшилась на 30% (втрата 300 000 on-Line користувачів) та має сталу тенденцію до зниження, що яскраво демонструє соціальний тренд на відмову від користування російськими соцмережами.

Однак, існують також непоодинокі факти використання громадянами України і іншими учасниками антиукраїнських спільнот програмних засобів для подолання блокування. Цьому сприяє розгортання в РФ медійної кампанії з популяризації методів обходу блокування російських сервісів на антиукраїнських загальнодоступних ресурсах мережі Інтернет. Так, приміром, використання VPN-режиму Інтернет браузеру Opera призвело до суттєвого збільшення аудиторії сайту Opera.com (за тиждень зросла з 1% до 12%). Також (за даними Liveinternet [5]), з часу введення санкцій на 2 млн. осіб зросла чисельність користувачів, які відвідують російські Інтернет-ресурси з IP-адрес VPN-сервісів країн Германії, США и Нідерландів.

У якості висновку зазначимо, що для задоволення вже сформованих потреб громадян України у соціальних інформаційних сервісах мають пропонуватися вітчизняні соціальні мережі «Ц.укр», «UkrOpen», «Hurtom.com», «ukrface.com.ua», «Ukrainians». Існує необхідність державної підтримки зазначених вітчизняних сервісів для пропагування національних інтересів в інформаційній сфері.

**Література**

1. Указ Президента України від 15.05.2017 № 133/2017 «Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» // Офіційний вісник України. – 2017. – № 41. – Ст. 1276.

2. Указ Президента України від 25 лютого 2017 року № 47/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» // Офіційний вісник України. – 2017. – № 20. – С. 8.
3. www.similarweb.com.
4. https//tns-ua.com.
5. www.Liveinternet.ru.

*УДК 341.824*
**Міхєєв Ю. І.**
кандидат технічних наук
Житомирський військовий інститут ім. С. П. Корольова

## АВТОМАТИЗАЦІЯ ОЦІНЮВАННЯ ПРОПАГАНДИ ДЕРЖАВИ-АГРЕСОРА

Українське суспільство попри збройну агресію і нині знаходиться під впливом російської пропаганди, що стала одним з дієвих інструментів ведення гібридної війни проти нашої країни. Так, за допомогою пропаганди Росія виправдовує та прикриває присутність на території України своїх збройних сил. З іншого боку, російські засоби масової інформації всіляко намагаються демонізувати в очах російського та світового суспільства керівництво України. Аналіз перебігу подій, які відбувалися у 2014 році у Криму, свідчить, що тривалою була також і пропагандистська підготовка до початку російської агресії в Україні, спрямована на дестабілізацію ситуації у країні за рахунок посилення недовіри нашого суспільства до керівництва держави, що поєднувалося з формуванням позитивного ставлення до Росії [1, 2]. У таких умовах розкрити та зірвати наміри противника можливо лише шляхом системного аналізу пропагандистських матеріалів, які він розповсюджує у засобах масової комунікації.

У цілому оцінювання пропаганди передбачає вивчення джерела, змісту, цільової аудиторії, середовища та наслідків пропагандистського впливу, спрямованого проти ворожої, нейтральної або дружньої аудиторії. Для цього можуть бути використані різні підходи, які ґрунтуються на технологіях контент-аналізу текстових повідомлень [3–6]. Основним проблемним питанням в умовах обмежених часових та людських ресурсів залишається завдання з автоматизації обробки та оцінювання текстових повідомлень, які розповсюджуються на сторінках новинних сайтів та соціальних мереж Інтернету.

У доповіді розкриваються основні завдання з автоматизації оцінювання пропаганди держави-агресора. Для розробки показників з оцінювання текстових повідомлень, які розповсюджуються у мережі Інтернет пропонується використати SCAME-метод, суть якого полягає у виконанні завдань з аналізу: джерела пропагандистських повідомлень; змісту повідомлень; цільових аудиторій, на які спрямований вплив; середовищ розпо-

всюдження пропагандистських впливів; бажаних для противника наслідків реалізації пропагандистських впливів [6].

Передбачається, що програмна реалізація процесу збирання та оцінювання пропаганди дозволить оперативно отримувати данні про: чисельність аудиторії, на яку впливають; витрати противника на інформаційно-психологічні заходи; ефективність психологічних акцій, залучених учасників до діяльності, пов'язаної із розробленням та розповсюдженням пропаганди. Це позитивно відобразиться на організації відповідних заходів з протидії негативним психологічним впливам та у цілому підвищить ефективність діяльності аналітичних підрозділів Збройних Сил України.

**Література**

1. Хоружий Г. Ф. Війна Росії проти України російська пропаганда як складова "гібридної війни" / Г. Ф. Хоружий // Освіта регіону. Політологія Психологія Комунікації. – 2016. – № 4: Український науковий журнал. – С. 6–15.

2. Левченко О. В. Еволюція гібридної війни Російської Федерації проти України / О. В. Левченко // Наука і оборона. – 2017. – № 2. – С. 11–16.

3. Додонов А. Г. Виявлення категорій і їх взаємозв'язків у рамках технології контент-моніторингу / А. Г. Додонов, Д. В. Ланде // Вісник державної служби України. – 2006. – № 4. – С. 45–52.

4. Берко А. Ю. Система контент-моніторингу новинних інтернет-ресурсів / А. Ю. Берко, Я. П. Кісь, В. І. Суховерський // Вісник Національного університету "Львівська політехніка". – 2011. – № 699: Інформаційні системи та мережі. – С. 13–21.

5. Pysarchuk O. Statistical Analysis of the Thematic Content on the Internet for Predicting the Development of Information Treats / O. Pysarchuk, O. Lagodnyi, Y. Mikhieiev. International Electronic Scientific Journal. Traektoria Nauki = Path of Science. – Vol 3, No 8. – P. 3011–3019 [Electronic resource]. – Mode of access: http://pathofscience.org/index.php/ps/article/view/376. – ISSN 2413-9009.

6. Field Manual 33-1-1 – Psychological Operations Techniques and Procedures [Electronic resource]. – Mode of access: http://www.enlistment.us/field-manuals/fm-33-1-1-psychological-operations-techniques-and-procedures.shtml.

УДК 355.35

**Мокляк С.П.**
кандидат технічних наук, професор
Воєнно-дипломатична академія імені Євгенія Березняка

## АНАЛІЗ ІСНУЮЧОЇ ПРАКТИКИ ПІДГОТОВКИ ТА ВЕДЕННЯ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА У СФЕРІ ВІЙСЬКОВО-ТЕХНІЧНОГО СПІВРОБІТНИЦТВА УКРАЇНИ

Активна позиція України на ринку продукції військового призначення виводить сферу ВТС на рівень найбільш прибуткових та найважливіших напрямків зовнішньополітичної та зовнішньоекономічної діяльності нашої

держави. В той же час, саме експортна спрямованість військово-технічного співробітництва України спричиняє постійну протидію з боку конкурентних країни та транснаціональних корпорацій [1].

Подібні дії створюють пряму загрозу національній безпеці України, оскільки протидія ВТС як одному з елементів воєнно-економічної безпеки нашої держави в той же час шкодить і політичному іміджу нашої держави.

Одним з найбільш дієвих засобів протидії успішній реалізації Україною ВТС з іншими країнами є проведення проти неї інформаційних операцій, які здійснюються за класичними методиками та алгоритмами, однак мають певні особливості.

Насамперед, це стосується широкого використання ЗМІ на міжнародному та національному рівні. Специфіка інформаційних матеріалів щодо ВТС надає змогу організаторам інформаційних операцій використовувати ЗМІ «втемну». Це пояснюється тим, що, як правило, журналісти не можуть отримати повну інформацію з цих питань. Більш того, часто вони не володіють всім необхідним масивом інформації і специфічними знаннями в цій сфері. В результаті інформаційна операція може ґрунтуватись на непідтвердженій або повністю сфальсифікованій інформації, однак ЗМІ будуть вимушені користуватися цими даними до отримання коментарів з урядових та експертних джерел.

Також однією зі специфічних рис подібних інформаційних операцій є закритість даних стосовно ВТС. З одного боку це спрощує завдання організаторам операцій – перевірити їхню інформацію буде важко, оскільки офіційні структури можуть утриматись від коментарів через «грифованість» даних. З іншого боку, реагування представників уряду на інформаційні повідомлення у цій сфері буде завжди затримуватись, у зв’язку з існуючою процедурою узгодження та перевірки даних в державних органах.

Виходячи з того, що ВТС з іноземними державами має два аспекти: воєнно-політичний та воєнно-економічний, в залежності від мети основні завдання інформаційної протиборства у сфері ВТС можуть бути воєнно-політичного та/або воєнно-економічного характеру [2,3].

Воєнно-політичними завданнями інформаційного протиборства у сфері ВТС можуть бути:

дискредитація країни-конкурента на міжнародній арені, як надійного суб’єкта військово-технічного співробітництва;

дискредитація країни-конкурента на міжнародній арен, що реалізує ВТС з певними країнами в обхід міжнародних санкцій;

дискредитація воєнно-політичного керівництва країни-конкурента;

створення передумов для подальшого інформаційного тиску на країну-конкурент у вирішенні двосторонніх політичних проблемних питань тощо.

Воєнно-економічними завданнями інформаційного протиборства у сфері ВТС можуть бути:

дискредитація спеціальних експортерів країни-конкурента;

дискредитація підприємств ОПК країни-конкурента, які виробляють аналогічні типи ОВТ;

дискредитація певних зразків ОВТ, які створюють конкуренцію на ринках ТВППВ українській продукції;

створення інформаційних передумов для недопущення подальшого експорту певних зразків ОВТ країною-конкурентом на перспективні ринки збуту;

створення інформаційних передумов для подальшого тиску на країну-конкурент в ході проведення передконтрактної підготовки;

створення інформаційних приводів для припинення військово-технічного співробітництва з певними країнами тощо.

В цілому слід констатувати, що незважаючи на наявність низки суттєвих негативних факторів, які пов'язані із широким проведенням проти України інформаційних операцій (акцій) у сфері ВТС, наша країна залишається одним з ключових суб'єктів у вказаній сфері, що викликає занепокоєння та відповідно жорстку протидію з боку країн-конкурентів.

Аналіз змісту на адресу України звинувачень у несанкціонованій торгівлі озброєнням та військовою технікою показує, що вони пов'язані з перерозподілом світового ринку озброєнь і намаганням традиційних постачальників не допустити на нього потенційних конкурентів, часто безпідставно дискредитуючи їх.

У зв'язку з цим найважливішим чинником сприяння збереженню та зміцненню позицій країни на світовому ринку озброєнь має бути підвищення ефективності інформаційного супроводження на державному рівні реалізації завдань військово-технічного співробітництва та, у випадку необхідності, ефективної протидії деструктивному інформаційному впливу з боку інших держав.

**Література**

1. Горбулін В. П. Входження ОПК України в європейський оборонно-промисловий простір / В. П. Горбулін, В. С. Шеховцов, А.І.Шевцов // Стратегічні пріоритети. – 2015. – № 1(34). – С. 5–10.

2. Свергунов О. О. Управління експортною політикою у сфері військово-технічного співробітництва в умовах криз: світовий досвід та Україна / О. О. Свергунов // Стратегічні пріоритети. – 2014. – № 3. – С. 166–176.

3. Свергунов О.О. Стратегічне управління імпортною політикою у сфері військово-технічного співробітництва в умовах криз: світовий досвід та Україна / О.О. Свергунов // Стратегічні пріоритети. – 2015. - № 1 (34). – с. 26-33.

*УДК 621.396.967*
**Нікіфоров М.М.**
кандидат військових наук
**Жогіна Л.В.**
**Доброгурська О.Б.**
**Нікіфорова О.М.**
Військовий інститут Київського національного
університету імені Тараса Шевченка

# ОБҐРУНТУВАННЯ ВИБОРУ РАЦІОНАЛЬНОГО АЛГОРИТМУ АНАЛІЗУ ТОНАЛЬНОСТІ РІЗНОМОВНОЇ ТЕКСТОВОЇ ІНФОРМАЦІЇ ДЛЯ ЗАДАЧІ МОНІТОРИНГУ ІНФОРМАЦІЙНОГО ПРОСТОРУ

У забезпеченні результату політичного аналізу й прогнозування вирішальну роль відіграє оптимізація методів, які становлять арсенал наукового напряму. Однією з характерних тенденцій, яка склалася в сучасних умовах, не тільки в Україні, а й у світі, – це випереджальний розвиток форм, способів, технологій і методики впливу на свідомість (підсвідомість), психологію й психічний стан людини в порівнянні з організацією протидії негативним, деструктивним психологічним впливам, інформаційно-психологічним захистом особистості й суспільства в цілому.

Проведено обґрунтування вибору раціонального алгоритму аналізу тональності різномовної текстової інформації для задачі моніторингу інформаційного простору, та обґрунтуємо вибір характеристик, які будемо вважати визначальними для вибору алгоритму:

1. Першою та найголовнішою характеристикою буде наявність фази навчання. Це необхідно, аби забезпечити можливість врахувати всі нові або непомічені раніше особливості задачі. Якщо це не передбачити, то з появою нових чинників, кожного разу треба буде змінювати наявний чи обирати інші алгоритми. Так наприклад, розвиток технологій, який може мати досить не передбачений (інноваційний) характер, може змінити вплив певних типів даних.

2. Іншим прикладом може стати зміна політичного становища, що звичайно, змінює ставлення людей до тих чи інших подій (нажаль, таких прикладів в нас більш ніж достатньо). Тож, другою важливою характеристикою буде те, що навчання повинно відбуватися під контролем людини, аби вловлювати зміну людського ставлення до тих, чи інших подій. До того ж, машинне навчання з вчителем є більш розповсюдженим для аналізу текстів, в той час як навчання без вчителя є більш природним для навчання в біологічних чи фізичних системах, де немає впливу людського чинника в аналізі результату.

3. Третьою характеристикою є те, що цей метод повинен мати теоретичне обґрунтування. Це потрібно, аби мати можливість використовувати результати цього алгоритму (хоча б з певною похибкою) для інших досліджень. Ця характеристика суттєво звужує вибір раціонального алгоритму для задачі моніторингу, відкинувши всілякі евристики.

4. Напевно, останньою важливою характеристикою буде швидкість роботи, бо таку іншу важливу характеристику, як точність, можна поліпшити за рахунок навчання.

З проведеного обґрунтованого вибору раціонального алгоритму аналізу тональності різномовної текстової інформації для задачі моніторингу інформаційного простору ми обрали комбінований метод, який полягає в застосуванні двох потужних методів:

1) методу опорних векторів (support vector machine, SVM);

2) методу ключових слів.

Під час реалізації комбінованого методу, спочатку знаходимо результат за допомогою методу опорних векторів:

1. Розраховуємо за допомогою підходу TF-IDF вагу для кожного слова в словнику

2. Формуємо векторну модель для подальшого навчання SVM-класифікатора.

3. Будуємо гіперплощини, що класифікують слова відповідно до двох класів.

4. Обчислюємо гіпотезу.

Потім знаходимо результат за допомогою методу ключових слів:

1. Для кожного слова обчислюємо релевантну частоту (Relevance Frequency, RF).

2. Для кожного класу: обираємо підмножину слів з частотою більше за граничне значення цього класу.

3. Отримали список підмножин пар слів та їх частот, які відповідають кожному класу.

4. Кожному класу ставимо у відповідність суму частот по всім словам з відповідної підмножини.

5. Обираємо клас з найбільшою сумою частот, який буде гіпотезою.

Після виконання обох методів комбінуємо їх результати за певною стратегією. Сутність використання комбінованого методу полягає у постійному навчанні програми, а саме в аналізі текстової інформації на базі стартової вибірки та фінальне порівняння результатів роботи алгоритмів з відомими правильними результатами. Оцінки, які використовують, для порівняння результатів можна також використати для порівняння різних методів.

Точність і якість системи аналізу тональності тексту оцінюється тим, наскільки добре вона узгоджується з думкою людини щодо емоційної оцінки

досліджуваного тексту. Для цього можуть використовуватися такі метрики як точність та повнота. Отже, програма, яка визначає тональність тексту за допомогою комбінованого методу з точністю 70%, робить це майже так само добре, як і людина. Цей результат може повністю влаштовувати нас, так як специфіка завдання полягає у відсутності точної відповіді.

Визначено, що комбінований метод автоматичного визначення тональності тексту, що об'єднує результати двох потужних класифікаторів (SVM та на основі ключових слів), дає можливість досягти підвищення якості класифікації в порівнянні не лише з цими класифікаторами, а й з найкращими результатами інших підходів.

**Література**

1. Терехов А.В. Информатика: учеб. пособ. / А.В. Терехов, В. Н. Чернышов. – Тамбов : Изд-во Тамб. гос. техн. ун-та, 2007. – Т. 35. – С. 54-55.

2. L. Lytvynenko "Construction of premorphological level of analisys for multilanguage texts" // – USA. The advanced science journal, volume 2013 issue 5. – С. 28-32.

3. O. Nikolaievskyi "Components of lingware for automatic morphological analysis in knowledge-oriented machine translation system" // – USA. The advanced science journal, volume 2013 issue 5. – С. 32-36.

*УДК 681.518.5*

**Охрамович М.М.**
кандидат технічних наук,
старший науковий співробітник
Військовий інституту Київського національного
університету імені Тараса Шевченка
**Шевченко В.В.**
Військовий інституту Київського національного
університету імені Тараса Шевченка
**Кравченко О.І.**
Військовий інституту Київського національного
університету імені Тараса Шевченка

## ОСОБЛИВОСТІ МОНІТОРИНГУ РАДІО ПРОСТОРУ НА БАЗІ SDR ТЕХНОЛОГІЇ

Принцип роботи SDR (*Software Defined Radio (SDR)*) ґрунтується на оцифруванні прийнятого радіосигналу і подальшій обробці його вже в цифровій формі.

Радіопередавач або радіоприймач, який використовує технологію SDR, має можливість за допомогою програмного забезпечення встанов-

лювати або змінювати робочі радіочастотні параметри, зокрема, діапазон частот, тип модуляції або вихідну потужність, за винятком зміни робочих параметрів, що застосовуються в ході звичайної попередньо визначеної роботи з попередніми установками радіопристрою, згідно з тією чи іншою специфікації або системи. SDR виконує значну частину цифрової обробки сигналів на звичайному персональному комп'ютері або за допомогою програмуємо логічної інтегральної схеми (ПЛІС). Метою такої схеми є радіоприймач або радіопередавач довільних радіосистем, змінюваний шляхом програмної переконфігурації. Технологія SDR передбачає адаптацію до спектру протоколів, так що в результаті можуть взаємодіяти різні моделі радіостанцій і мережі. Це важливо, оскільки підрозділи, що представляють різні країни, все частіше працюють у великомасштабних і багатонаціональних операціях, наприклад, Міжнародні сили сприяння безпеці (ISAF – International Security Assistance Force) в Афганістані. Наявність радіостанції для взаємодії важлива не лише для силових структур і для цивільних відомств. Інтерфейс, який застосовується у радіостанціях також покращується. Операторові не потрібно мати спеціальної освіти або проходити додаткове навчання, щоб користуватися пристроєм. Ключовою перевагою SDR є взаємодія між засобами радіозв'язку попередніх поколінь і сучасними системами. Військовим системам зв'язку завжди була властива консервативність і оновлення парку засобів радіозв'язку в Збройних Силах та інших силових структурах, навіть у розвиненіших країнах ніколи не порівняється по своїх темпах з ринком сучасних мобільних телефонів і інших комунікаційних засобів. Це очевидно, адже жодного прибутку, окрім підвищення боєздатності, оснащення підрозділів сучаснішими радіозасобами не приносить. Тому важливо, щоб новостворені і старі системи могли працювати сумісно. Технологія прямого цифрового перетворення і прямого цифрового синтезу (DDC/DUC), з діапазонними фільтрами, дозволяє отримати максимально високі характеристики приймального тракту. Велике навантаження по кінцевій обробці сигналів припадає на комп'ютер, тому він повинен високо продуктивним. Наприклад, станція може виступати як ретранслятор чи брати участь в створенні безпровідних мереж передачі даних під час руху.

Ще однією перевагою SDR є можливість здобуття багатьох функцій і сервісів в одному компактному корпусі. Одна система тепер може зробити роботу, для якої раніше було б потрібно декілька радіостанцій. Наприклад, дані про військовослужбовців, що мають sdr-радіостанцію і вбудовані системи глобального позиціювання (GPS – Global Positioning Systems) можуть транслюватися у мережу інформацію, так що всі кореспонденти мережі, або, наприклад, лише командир, можуть знати, і навіть бачити на реальній карті місцевості (при підключенні планшета або комп'ютера) де вони знаходяться. Значна перевага SDR полягає в можливості оперативної

модернізації конструкції передавача, оскільки вона може бути пристосована до нових технологічних можливостей і сервісів просто через зміну програмного забезпечення. Сучасній армії потрібні компактні, легкі і швидкодіючі пристрої, що в той же час адаптовані із старими вузько смуговими системами. SDR використовує вбудовуванні комп'ютерні технології, і спирається на досягнення в області цифрової обробки сигналів (*DSP – digital signal processing*), напів-програмованих вентильних матрицях (*FGPA – field-programmable gate arrays*), розробках в області генерації програмного коду.

Напрямки розвитку SDR. З розвитком технологій, засобу зв'язку стають значно меншими по розміру. Наприклад, SDR-системи можуть бути вбудовані в пристрої на зап'ясті або в надшоломний дисплей. Дослідники вивчають, яким чином пристрої можуть бути зв'язані один з одним на полі бою, так щоб люди могли мати доступ до мережі і оперативно отримати корисні дані. Майбутні мережі зможуть відображувати в режимі реального часу свої сили і сили противника, а також надавати інші ситуаційні дані. Частково це вже реалізовано, наприклад, в мережах зв'язку, побудованих на устаткуванні *Harris Falcon III* з використанням програмного забезпечення (ПЗ) *Falcon Command*. Інший напрям – використання сенсорів (датчиків) ядерного, біологічного і хімічного контролю, або реєстрації наявності артилерійських ударів і бомбардування з повітря, що дуже актуально сьогодні в умовах локального збройного конфлікту. Наступним кроком після SDR може бути створення радіостанції з інтелектуальним управлінням, яка автоматично дасть змогу встановлювати зв'язок у реальному часі. Підхід до побудови інтелектуальних радіосистем, що отримав назву когнітивне радіо, є передовою технологією, що дозволяє забезпечити раціональне використання радіочастотного спектру. Проте впровадження вказаної технології у військових засобах зв'язку вимагає додаткових досліджень, які враховують специфічні особливості роботи радіозасобів в складній електромагнітній обстановці, а також в умовах активної радіопротидії противника.

**Література**

1. Пампуха І.В., Бурий С.В., Пусан В.В. Аналіз сучасних автоматизованих систем моніторингу радіо простору на базі SDR технологій для ведення завдань радіоелектронної розвідки / Збірник наукових праць Військового інституту Київського національного університету ім. Тараса Шевченка. – К., 2017. – № 56. – С. 40-46.

2. J. Mitola ii, Z. Zvonar Software Radio technologies. New York: ieee press, 2001.

3. Форум sdr (www.sdrforum.org).

*УДК 327:325*
**Партоленко І.В.**
провідний науковий співробітник
відділу наукових досліджень Інституту СЗРУ

# ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНІ ВПЛИВИ В КОНТЕКСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

В умовах формування глобального інформаційного суспільства в даний час Україна активно переживає трансформацію політичного світогляду.

Однією з головних особливостей сьогодення є постійне зростання темпів створення інформації. Цей процес у цілому позитивний, однак нині людство зустрілось, на перший погляд, з парадоксальною ситуацією, коли в умовах формування глобального інформаційного суспільства знижується загальний рівень його інформованості, а найважливішим наслідком є поширення практики застосування інформаційно-психологічних впливів для досягнення односторонніх переваг у міжособистісних, міжгрупових та міждержавних відносинах.

Сучасні інформаційно-психологічні впливи стали невід'ємною частиною політики будь-якої держави. Стає очевидним, що дана проблема набуває все більшої актуальності та потребує наукового осмислення й обґрунтування. Особливо актуалізується проблема політологічного дослідження сутності інформаційних-психологічних впливів.

Аналіз тенденцій у міжнародному інформаційному просторі довкола України дає підстави стверджувати, що наша країна стала об'єктом інформаційно-психологічних впливів, які є свідченням спроби встановити контроль над усіма сферами існування української держави та суспільства. Ведеться не лише інформаційна, а й психологічна війна Російської Федерації проти України, яка зумовлена її стремлінням будь-якою ціною утримати Україну в зоні своїх стратегічних інтересів.

Змушені також відзначити, що у цих складних геополітичних та глобалізаційних умовах, коли державний суверенітет знаходиться під загрозою впливів з боку російських спецслужб, йде постійне застосування стратегічної пропаганди (створення негативних інформаційних умов сприйняття політики держави або "київської влади"), що суттєво впливає на зовнішню та внутрішню аудиторію України.

Використання терміну "стратегічна пропаганда" стоїть поряд з традиційними термінами "інформаційна війна" та "психологічна боротьба", які зумовлені своїм прикладним характером та зростанням ролі психологічних операцій у сучасних війнах, розширенням використання інформаційної зброї, створеної на базі новітніх технологій і методів психологічного впливу. Проте головною роллю інформаційно-психологічних впливів є

атака на соціаосистему, що, зрештою, спричиняє прийняття нею завідома неправильних та неадекватних рішень [3].

М. А. Дмитренко стверджує, що за весь час незалежності політичні й бізнесові кола Росії крок за кроком відвойовували все нові “плацдарми” на українських теренах, відіграють важливу роль в українському політикумі, економіці, промисловості, кредитно-фінансовій сфері тощо [2].

Виходячи з цього, більшість зарубіжних і вітчизняних науковців, а також суспільно-політичних діячів дійшли спільного висновку, що інформаційно-психологічні операції набувають значення одного з найважливіших інструментів у вирішенні сучасних, а тим більш майбутніх конфліктів [1].

На підтвердження вищезазначеної тези також є слушним наведення прикладу того, що військові структури інформаційно-психологічних операцій української армії виявилися не готовими, із об’єктивних і суб’єктивних причин до сучасних конфліктів на теренах своєї держави.

Згідно з доктриною інформаційної безпеки України, затвердженої Указом Президента України від 8 липня 2009 року N 514/2009 для забезпечення інформаційної безпеки України у зовнішньополітичній сфері держава мала гарантувати своєчасне виявлення та нейтралізацію зовнішніх загроз національному інформаційному суверенітету тощо [4].

Але недооцінка важливості проведення інформаційно-психологічних впливів в рамках здійснення Україною інформаційних операцій, спрямованих на підтримку її національних інтересів і державної політики за кордоном, як показують останні події, завдає державі величезних економічних, політичних, іміджевих збитків.

Саме розбалансованість системи захисту національної безпеки в секторі протидії інформаційній експансії є вагомою причиною невдач ще на початку воєнних дій на сході України, та під час анексії Криму. Жодну війну нині не можна виграти без переваг на інформаційному фронті.

Отже, результати проведеного дослідження свідчать, що Україна знаходиться під сильним інформаційно-психологічним впливом найпотужнішого світового суб’єкта інформаційних відносин російської влади, яка веде війну не лише за територію, а й за світогляд, думки і душі людей.

У цьому контексті нагальною є потреба розробки комплексної системи протидії інформаційної агресії, операціям інформаційної війни та вироблення стратегії інформаційної політики держави.

**Література**

1. Литвиненко О.В. Інформаційні впливи та операції. Теоретико-аналітичні нариси. / О.В. Литвиненко. – К., 2003. – 240 с.

2. Дмитренко. М. Зовнішньополітичні впливи як пріоритети діяльності держави / М.А.Дмитренко. – К.: 2013. – 146 с.

3. Манойло А. В. Государственная информацыонная политика в особых условиях. [Электронный ресурс] / А. В. Манойло. – 2003. – Режим доступа: http:// www/evartist.narod.ru.

4. Указ Президента України «Про Доктрину інформаційної безпеки України» від 8 липня 2009 року № 514/2009.

*УДК: 328. 325*

**Петряєв О.С.**
викладач Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»
аспірант Національного Інституту стратегічних досліджень

# ІСЛАМСЬКИЙ МІГРАЦІЙНИЙ ЧИННИК ЯК СТРАТЕГІЧНИЙ ВИКЛИК ЦІННІСНО-СМИСЛОВІЙ БЕЗПЕЦІ ЄВРОПЕЙСЬКИХ КРАЇН

У грудні 2010 року туніський громадянин Мухамед Буазізі здійснив акт публічного самоспалення, протестуючи таким чином проти корупції і свавілля влади, що стало символічним початком «Жасминової революції» в Тунісі, а згодом - низки таких самих, але більш кривавих революцій в інших країнах ісламу, починаючи від країн Північної Африки (Магребу) й закінчуючи країнами Леванту (Ліван та Сирія) і Аравійського півострову. У деяких з цих країн (Сирія, Ємен) ці революції трансформувалися в довготривалі громадські війни за інтенсивної іноземної участі.

Водночас відбулися й контрреволюційні процеси: повалення президентів і корумпованої політичної еліти в Тунісі і Єгипті закінчилося, наприклад, наступним відновленням приблизно таких самих «постреволюційних» політичних режимів.

В цілому, зазначені революційні процеси слід розуміти як намагання політичних еліт модернізувати арабсько-ісламський світ. Політичні реформи зачепили навіть такий оплот ісламського консерватизму як Саудівська Аравія, де була проведена масштабна антикорупційна компанія та змінено порядок успадкування королівського престолу.

Революції і громадянські війни створили хаос, яким вміло скористалися ісламські радикали. Під час диктаторського правління ісламістам-радикалам доводилося перебувати в політичній тіні. Арабська весна дала їм шанс на здобуття влади, а довготривалі конфлікти в Іраку та Сирії навіть творили підґрунтя для радикальних ісламістів взяти під контроль великі території Месопотамії, і створити власну Ісламську Державу Іраку і Леванту (ІДІЛ), певну подобу Ісламського Халіфату. Хоча ІДІЛ було про-

голошено ще в 2006 р., будувати цю державу екстремісти розпочали тільки в 2014 р., причому пропагандистський апарат Ісламського Халіфату активізував інформаційну рекрутингову діяльність не тільки на Близькому Сході, але і в країнах Європи, результатом чого стала ціла низка терактів, вчинених європейськими мусульманами, значна частина яких навіть не належали до ІДІЛ.

Іншою загрозою й викликом для країн «Старого Світу» стали неконтрольовані міграційні процеси. Значною мірою поясненням причини виникнення цієї загрози є той факт, що у Лівії, яка в часи перебування при владі диктаторського режиму Муамара Каддафі, була своєрідним антиміграційним щитом, станом на 2018 р. так і не було відновлено повноцінну державність. Країна de facto розпалася на дві відносно самостійних частини, - Тріполітанію та Кіренаїку.

За 3,5 роки (починаючи від 2014 р. й до середини 2017 рр.) 600 000 мігрантів здійснили «прорив» до Європи (власне, до Італії) через лівійський неконтрольований владою середземноморський перехід. Для 12 тисяч цей перехід виявився смертельним [1].

Другий етап зростання міграційного виклику розпочався в 2015 р., коли до Європи масово почали мігрувати сирійські біженці, які до того, втікаючи від терору ІДІЛ, були зосереджені переважно в таборах на території Турецької республіки.

Разом з мусульманськими біженцями до Європи приходить культура ісламу. Араби та інші мусульмани компактно розселяючись переважно в європейських мегаполісах, вибудовують культурно-цивілізаційні анклави (гетто), де існують власні школи, продуктові магазини з халяльними їстивними продуктами, мечеті, навчальні заклади (медресе) тощо.

Західноєвропейські суспільства та держави, зорієнтовані головно на ліберально-демократичні цінності (секуляризм і свобода віросповідання, толерантність, політична коректність, гендерна рівність, вільний перетин кордонів тощо) у ставленні до міграційної проблеми наштовхнулися на спротив східноєвропейських суспільств та держав.

Типовим прикладом нетерпимого ставлення до мігрантів є Угорщина, очолювана Віктором Орбаном. Виступаючи 18 лютого 2018 р. в Угорському Парламенті з традиційним Посланням «Про стан нації», Віктор Орбан у суто алармічному стилі висвітлював міграційні проблеми «Старого Світу»: «Якщо справи підуть й надалі подібним трибом – наша культура, наша ідентичність, наша нація, саме в тому вигляді, в якому ми їх знаємо, загинуть. Наші найгірші побоювання стануть реальністю. Захід впаде. Європа опиниться під [ісламською] окупацією. Це підтверджує тезу, що цивілізації не вбивають, вони вчиняють акт самогубства. Й помиляються ті, хто думає, що це станеться ще не скоро. Прогнози вказують на те, що це розпочнеться вже всередині даного століття. Тобто нинішні 50-літні стануть у свої 80 свідками цих подій» [2].

Саме цими побоюваннями втрати європейської ідентичності пояснюється розходження в міграційно-адаптаційній політиці країн Західної й Центральної Європи всередині ЄС.

Ще однією загрозою «деєвропеїзації» створюють ті жителі європейських країн, які під впливом ісламської радикальної пропаганди поїхали воювати в Сирію або Ірак. Чимало з цих найманців з Європи є етнічними європейцями, які прийняли іслам у його войовничій (джихадистській) версії й, повертаючись до Європи, готові воювати з релігійно-ідеологічними переконаннями європейського типу, що становить безпосередню загрозу для європейської цивілізації та безпеки й може призвести до нового спалаху в Європі релігійних війн, які дошкуляли «Старому Світу» аж до відомої дати укладення Вестфальського миру (1648 р.).

На цьому тлі в академічних та безпекових колах Європи й Північної Америки загострилися дискусії стосовно ключового поняття «європеїзація», під якою, згідно одного з академічних визначень, слід розуміти «процес включення до логіки внутрішнього (національного та субнаціонального) дискурсу, політичних структур та державної політики формальних та неформальних правил, процедур, політичних парадигм, стилів, «способів виготовлення речей» («ways of doing things») та спільні вірування та норми, які вперше визначені в процесах політики ЄС»[3].

**Висновок.**

Пришвидшена ісламізація Європи під впливом радикалізації самого ісламу та пожвавлення міграційних процесів, спричинених війнами та революціями в країнах Близького Сходу, перетворюється на безпосередню загрозу західним цінностям і традиційній для країн Заходу ліберально-демократичній ідеології. З одного боку, в країнах Західної Європи починають набирати популярність європейські праві партії (деякі з них сповідують навіть нацистську расистську ідеологію), які виступають проти не тільки мігрантів-мусульман, але й проти європейських, ліберально налаштованих урядів.

Ще більший спротив ліберально орієнтованій, диригованій з Брюсселю, європейській міграційній політиці чинять націоналістично зорієнтовані лідери країн Східної й Центральної Європи, які відтак проводять внутрішню і зовнішню політику, відмінну від рішень офіційного Брюсселя. І справа тут не тільки в тому, що ці країни не бажають приймати у себе мусульман-мігрантів, витрачаючи на них частину бюджету. Значною мірою така позиція пояснюється законними побоюваннями втрати європейської ідентичності, «європейськості», які лідери цих країн (переважно католицьких та православних) пов’язують з традиційними християнськими цінностями.

**Література**

1. Hayden, Sally. New mafia-led militia may be stopping refugees from leaving Libya for Italy // The Independent. 22 August 2017 [Електронний ресурс]. –Режим доступу: http://www.independent.co.uk/news/world/africa/mafia-refugees-libya-italy-stop-leave-militia-mediterranean-crossing-sabratha-migrant-boats-a7906666.html.

2. Речь Виктора Орбана об итогах года. 18 февраля 2018 г. [Електронний ресурс]. Режим доступу: http://www.kormany.hu/en/the-prime-minister/the-prime-minister-s-speeches/viktor-orban-s-state-of-the-nation-address-ru.

3. Europeanisation //Wikipedia. [Електронний ресурс]. Режим доступу: https://en.wikipedia.org/wiki/Europeanisation.

4. Bodissey, B. The Islamization of Europe: The Evidence. [Електронний ресурс]. URL: http://gatesofvienna.net/2018/02/the-islamization-of-europe-the-evidence/ (Дата звернення 02.03.2018).

*УДК 342*

**Печериця С. В.**
кандидат юридичних наук,
старший науковий співробітник
Національна академія СБ України

## ЗВ'ЯЗОК ІЗ ЗАСОБАМИ МАСОВОЇ ІНФОРМАЦІЇ ПІД ЧАС ПРОВЕДЕННЯ АНТИТЕРОРИСТИЧНОЇ ОПЕРАЦІЇ

В умовах агресії Російської Федерації одну з найбільших загроз національній безпеці становить антиукраїнська інформаційна кампанія, яка здійснюється за наступними напрямками: розпалювання протестних настроїв у суспільстві; підрив обороноздатності нашої держави *(використання «брудних» інформаційних технологій проти керівництва оборони, правоохоронних та органів спеціального призначення тощо)*; протидія євроінтеграційному курсу України та мінімізація міжнародної підтримки; легалізація самопроголошених утворень «ДНР/ЛНР» та анексії Криму; використання ресурсів Інтернет *(Інтернет-сайтів, соціальних мереж)* для здійснення деструктивного впливу на свідомість їх користувачів, поширення неправдивої та перекрученої інформації, пропаганда терористичної діяльності, а також координація діяльності терористичних угрупувань.

Фактично пропагандистська робота Російської Федерації в Україні спрямована на: підтримку сепаратистських та терористичних рухів у південно-східних регіонах України та Прикарпатті; дискредитацію чинної української влади, шляхом звинувачення у фашизмі, дискримінації російськомовного населення, невиконанні умов Мінських домовленостей, насильства над громадянами, боротьбою зі свободою слова, нездатності вирішувати проблеми населення соціально-економічного характеру; ескалацію розколу серед українського суспільства на національному, мовному, релігійному та політичному підґрунті; інспірування протестних рухів серед різних верств населення України, зокрема, учасників Антитерористичної операції та їх родичів, а також створення негативного іміджу нашої

держави на міжнародній арені, поширюючи серед іноземної аудиторії інформації, яка у викривленому вигляді відображає результати реалізації внутрішньої та зовнішньої політики органами вітчизняної влади.

Зокрема, агресивна політика Російської Федерації по відношенню до України, свідчить про значну активізацію діяльності інформаційних структур РФ, направлених на підтримку проросійської орієнтації російськомовного населення України, пропагування ідеї інтеграції нашої країни до пострадянського простору, підтримку відверто сепаратистських настроїв, лобіювання інтересів т.зв. «Л/ДНР».

Останнім часом скоєння терористичних актів, зокрема із взяттям заручників є досить частою подією у світових новинах. Скоюючи такий злочин терористи сподіваються на виконання їх політичних, матеріальних або інших вимог в обмін на життя та здоров'я заручників або цілісність важливих об'єктів життєзабезпечення та суспільної безпеки. Міжнародні екстремістські й терористичні організації у своїй діяльності сьогодні не тільки висувають вимоги державі й суспільству, але й прагнуть до залякування суспільної думки, поширення атмосфери тривоги й непевності, навіювання панічних настроїв та демонстрації слабкості влади. І в цьому побіжними помічниками їм часто стають сучасні ЗМІ. Прагнучи підвищити свою популярність, вони найчастіше стають ретрансляторами терористичних ідей, не уявляючи до кінця можливих наслідків своїх публікацій і їхнього патогенного впливу на масову аудиторію. ЗМІ не завжди в змозі відслідковувати рівень небезпеки переданої ними інформації для аудиторії. Здійснюючи свою діяльність, вони можуть заважати роботі спеціальних державних служб у момент здійснення терактів. У погоні за сенсацією журналісти часто безвідповідально наражають на небезпеку як себе, так і заручників. При висвітленні терористичних актів ЗМІ, не завжди усвідомлюючи реальне положення справ, найчастіше провокують суспільну думку про саботування політики держави, спрямованої на зниження рівня загроз від тероризму. «Незалежні журналісти» (наприклад, непрофесійні фрілансери або автори блогів) не володіють об'єктивним і збалансованим підходом до висвітлення подій, привносять в інформаційне поле дезінформацію, що провокує соціальні й психологічні травми.

Без інформаційного забезпечення ЗМІ сучасний тероризм неможливий, оскільки йому необхідні канали передачі інформації, адже одна із цілей терористів - залякування, що повинне вести до підпорядкування й установлення контролю. Деякі фахівці називають діяльність терористів і їхніх захисників не інакше як PR-кампанією. Більше того, відомі факти, коли арабських терористів консультували випускники факультетів по піару американських вузів. Зрозуміло, реклама, який «обдаровують» бойовиків збалансовані ЗМІ, завжди носить негативний характер. Однак ексклюзивні інтерв'ю терористам вигідні, хоча з моральної точки зору сумнівні:

адже, наприклад, маніякові-убивці або грабіжникові ефір давати не стануть. Тероризм чинить руйнівний ефект на стандарти журналістики. Журналісти в екстремальних ситуаціях, часом, губляться, що вкрай негативно позначається на якості їхньої роботи.

Так, 24 квітня п.р. знімальна група Київського офісу телеканалу у складі А.Стельмаха та О.Палямара була затримана співробітниками СБ України за спробу за допомогою квадрокоптера здійснити фото- та відеофіксацію військової бази в с. Оржів Рівненського району Рівненської області, яка є режимним об'єктом. За вказаним фактом було відкрито кримінальне провадження за ознаками злочину, передбаченого ч. 1 ст. 14 та ст. 113 ККУ («готування до вчинення диверсії»). На даний час, проводяться слідчі дії.

У зв'язку з цим постає необхідність розробки документів, які б регламентували поводження журналістів в екстремальних ситуаціях а також методичні рекомендації по зв'язку із представниками засобів масової інформацій під час вчинення терористичного акту або проведення антитерористичної операції. Важливо й те, щоб правила й норми в журналістиці виходили від самих журналістів, як і розуміння їх необхідності. Водночас необхідно витримати певний баланс між дотриманням правил та свободи слова.

*УДК 3%!.86(477)*

**Пилипчук В.Г.**
доктор юридичних наук, професор, член-кореспондент Національної академії правових наук України,
директор НДІ інформатики і права НАПрН України

## ІНФОРМАЦІЙНА СФЕРА ЯК СКЛАДОВА ГІБРИДНОЇ ВІЙНИ

Протягом останніх років поняття «**гібридна війна**» набуло значного поширення і вийшло за межі російсько-українського конфлікту, а низка держав світу фактично стали учасниками цього протистояння з використанням *політичної, інформаційної, економічної, енергетичної, воєнної* та інших складових.

Як свідчить аналіз, однією із першопричин зазначеного на пострадянському просторі було формування т.зв. *«поясу безпеки РФ»* – створення *«керованих зон конфліктів»* на території колишніх союзних республік, які стали на шлях розбудови суверенних держав та почали виходити зі сфери впливу РФ.

Зокрема, ще на початку 90-х років XX століття за участі російських військ чи воєнної підтримки РФ розпочалися довготривалі військово-

політичні та інші конфлікти на території **Таджикистану**, **Азербайджану**, **Вірменії**, **Грузії**, **Молдови** та **України**. Також спостерігалися неодноразові спроби втручання РФ у внутрішні справи **Литви**, **Латвії** та **Естонії**, які змогли убезпечити свої народи завдяки набуттю членства у ЄС і НАТО.

У контексті зазначеного заслуговують на увагу *можливі сценарії розвитку подій на пострадянському просторі*, надані вченими Національного інституту стратегічних досліджень [1], зокрема:

1) «*сценарій хаосу»* – виникнення суцільної зони конфліктів на пострадянському просторі;

2) *«імперський сценарій»* – створення регіональної пострадянської імперії з можливим повторенням відомих негативних історичних наслідків;

3) *«сценарій розколу»* – виникнення на пострадянському просторі східноєвропейського демократичного та євразійського імперського сегментів.

За нашими оцінками, активні спроби реалізації другого сценарію розпочалися ще 20 – 25 років тому (остання спроба була зроблена у 2014 р. шляхом підписання договору про Євразійський союз). Однак, події останніх 10-15 років в Україні та інших державах-членах ГУАМ свідчать про стійку тенденцію до розбудови східноєвропейського демократичного простору, який внаслідок «гібридного протистояння» може поширитись на увесь пострадянський простір.

Цьому може сприяти і фактичне створення коаліції країн-членів ЄС, НАТО та інших держав світу, спрямованої проти імперської політики та порушення РФ норм міжнародного права.

Одним із ключових чинників гібридної війни в сучасних умовах залишається інформаційна сфера. Тому для ефективного забезпечення інформаційної безпеки вкрай актуальними є проблеми протидії *інформаційним війнам, кібератакам та негативному інформаційно-психологічному впливу* на шкоду людині, суспільству і державі.

За результатами проведених наукових досліджень [2–5 та ін.], нині першочергової уваги потребують такі *ключові загрози національній та міжнародній безпеці в інформаційній сфері*:

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

*– в інформаційному просторі спостерігається тенденція до поширення інформаційної агресії і насилля, маніпуляції свідомістю людини та суспільства, періодично проводяться інформаційно-психологічні операції;*

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

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

Рівень сучасних викликів і загроз в інформаційній сфері наочно підтверджує справедливість і виключну значимість положень ст. 17 Конституції України про те, що *забезпечення інформаційної безпеки є однією з основних функцій держави* і справою всього Українського народу.

З урахуванням зазначеного, аналізу і прогнозування сучасних глобальних процесів в інформаційній сфері, першочергової уваги, системного наукового, організаційного і правового опрацювання та обговорення потребують такі **основні проблеми інформаційної безпеки**:

*1. Організації захисту прав, свобод і безпеки людини в інформаційній сфері,* насамперед, щодо:

1) реформування *національної системи захисту персональних даних* відповідно до "*Пакету захисту даних*" *ЄС*, що набуває чинності у травні 2018 р., і впроваджує такі *базові принципи* роботи з персональними даними: *законність, справедливість, прозорість, цільове обмеження, зведення до мінімуму даних, точність, обмеження терміну зберігання, цілісність і конфіденційність*;

2) врахування прецедентної судової практики США та інших країн-членів ЄС і НАТО стосовно визначення *«деліктів проти приватності»* (privacy torts):

*– втручання в усамітненість (intrusion upon seclusion) – вторгнення в «особистий простір» індивіда;*

*– публічне розголошення інтимних фактів (publication of private facts);*

*– спотворене представлення особи перед громадськістю (false light);*

*– використання чужого імені або образу в корисливих цілях (appropriation);*

3) опрацювання проблем захисту приватності та інформаційної безпеки людини в умовах впровадження новітніх інформаційних технологій: *штучного інтелекту, Інтернет-речей, «хмарних» технологій, Великих Даних* тощо.

*2. Інституційного розвитку та організаційно-правового забезпечення системи інформаційної безпеки,* зокрема:

1) удосконалення *державної інформаційної політики, політики національної безпеки в інформаційній сфері* та організація її належного *законодавчого забезпечення*. (Наприклад, у проекті Закону «Про національну безпеку України» (реєстр. № 8068 від 28.02.2018) питання інформаційної безпеки взагалі не згадуються);

2) розвиток *національної системи кібернетичної безпеки*, згідно з прийнятими нормативно-правовими актами і стандартами країн-членів

НАТО, насамперед, щодо захисту *об'єктів критичної інфраструктури, державних реєстрів і баз даних*;

3) опрацювання питання щодо *переведення сформованої системи протидії інформаційній агресії* проти України в режим *«активної інформаційної оборони»*, насамперед, щодо тимчасово окупованих територій та інших напрямів захисту національних інтересів України.

*3. Формування системи стратегічних комунікацій* відповідно до стандартів країн-членів НАТО, як складової системи національної безпеки і оборони, а саме:

1) розроблення *моделі національної системи стратегічних комунікацій*, визначення суб'єктів цієї системи, їх основних завдань, функцій, повноважень, взаємодії та організації міжнародного співробітництва;

2) опрацювання правових, організаційних, технічних та інших питань протидії *використанню мереж соціальних комунікацій на шкоду людині, суспільству і державі.* (Наприклад, масовий збір даних користувачів Фейсбук та їх застосування для впливу на суспільство в ході виборів у США та подібні події в Індії; тотальний контроль над мережами соціальних комунікацій в РФ та інших державах; зловживання державних службовців у Фейсбук та інших мережах тощо);

3) визначення *кваліфікаційних вимог до персоналу* підрозділів стратегічних комунікацій, *організація* його *підготовки*, перепідготовки та підвищення кваліфікації.

**Література**

1. Власюк О.С. Кремлівська агресія проти України: роздуми в контексті війни : моногр. / О.С. Власюк, С.В. Кононенко. – К. : НІСД, 2017. – С. 194-197.

2. Дзьобань О.П. Інформаційне насилля та безпека: світоглядно-правові аспекти: монографія / Дзьобань О.П., Пилипчук В.Г. (За заг. ред. проф. В.Пилипчука). – Харків: Майдан, 2011. – 244 с.

3. Пилипчук В.Г. Становлення і розвиток правових основ та системи захисту персональних даних в Україні: монографія / В.Г. Пилипчук, В.М. Брижко, О.А. Баранов, К.С. Мельник; за ред. В.М. Брижка, В.Г. Пилипчука. – К.: ТОВ "Видавничий дім "АртЕк", 2017. – 226 с.

4. Пилипчук В.Г. Реформування і розвиток Служби безпеки в контексті євроінтеграції України: Науково-методичний посібник / В.Г Пилипчук, О.Ф. Бєлов, С.С. Кудінов. – К. : Нац. акад. СБУ, 2017. – 260 с.

5. Пилипчук В.Г. Глобальні виклики і загрози національній безпеці в інформаційній сфері / Пилипчук В.Г., Дзьобань О.П. // Вісник Національної академії правових наук України. – Харків : «Право». – № 3(78). – 2014. – С. 43-52.

*УДК 323:351/343:341*
**Покровська А.В.**
державний експерт відділу зв'язків із ЗМІ
служби забезпечення доступу до публічної інформації
Апарату РНБО України

# КОГНІТИВНА СТІЙКІСТЬ В КОНТЕКСТІ ПРОТИДІЇ ТЕРОРИСТИЧНІЙ ЗАГРОЗІ

Сучасні прояви тероризму дозволяють говорити про те, що це явище сьогодні відіграє потужну інформаційно-пропагандистську роль, головною метою тероризму стає маніпулювання громадською свідомістю шляхом залякування населення, поширення паніки та істерії, примушення влади йти на поступки та виконувати вимоги терористів. Поширення страху, що виникає від загрози тероризму, формування певних образів терористів у ЗМІ, обґрунтування необхідності боротьби з тероризмом силовими методами створює певне уявлення про тероризм у свідомості людей. Таким чином, боротьба з тероризмом здійснюється не лише в кінетичному, але головним чином – в інформаційному та когнітивному просторах, що вимагає розвитку когнітивної стійкості до загрози тероризму серед населення.

Ідея виділення когнітивного виміру в інформаційній безпеці не є новою. Як зазначає Г. Почепцов, аналізуючи і узагальнюючи концепції західних авторів, сучасна інформаційна війна має чотири виміри – фізичний, соціальний, інформаційний та когнітивний. Когнітивний вимір стосується сприйняття, цінностей, переконань та схем інтерпретації, на основі яких людина приймає рішення; в когнітивному вимірі наративи стають основною зброєю конфліктуючих сторін [1]. Незважаючи на те, що під час війни проникнення в когнітивний простір можливе через кібернетичні та електромагнітні заходи [2], він все одно часто залишається без уваги.

У своїй доповіді перед Комітетом з питань збройних сил Сенату США «Інформація як зброя: необхідність когнітивної безпеки» [3] провідний дослідник RAND Ренд Вальцман аналізує російські інформаційні війни та пропагандистські кампанії та стверджує, що необхідно розробити нову концепцію когнітивної безпеки. Вальцман визначає її як «нову сферу, де в майбутньому дослідники, уряди, соціальні платформи та приватні актори будуть залучені до постійної гонки озброєнь з метою впливу та захисту від впливу великих груп користувачів онлайн» [3, с. 7]. Враховуючи те, що російський підхід до інформаційної та когнітивної війни досить агресивний (за визначенням Центру розвитку наукової політичної думки та ідеології, «когнітивна війна – це введення в інтелектуальне середовище країни ворога фальшивих наукових теорій, парадигм, концепцій, страте-

гій, що впливають на владу, послаблюючи значущі захисні національні потенціали» [4]), необхідність відповідних контрзаходів є нагальною.

Когнітивна безпека або COGSEC відрізняється від інформаційної безпеки, яка фокусується на процесі створення та відправки певних повідомлень для впливу на аудиторію, а також від комп'ютерної безпеки, де головним є запобігання фізичним атакам та збоям у комп'ютерних системах. За словами Вальцмана, COGSEC спрямована на «експлуатацію когнітивних упереджень у великих суспільних групах» та «соціальний вплив як самоціль» [3, с. 7]. Автор пропонує створити спеціальний неприбутковий міжнародний центр когнітивної безпеки в тісному співробітництві між «урядом, промисловістю, науковцями, аналітичними центрами та громадськими організаціями на міжнародному рівні» [3, с. 7]. По суті, ідея Вальцмана про такий центр нещодавно була частково реалізована під час створення Європейського центру передового досвіду боротьби з гібридними загрозами в Гельсінкі в липні 2017 р., який об'єднав 12 країн-членів НАТО та ЄС та почав діяти 6 вересня 2017 р.; серед пріоритетів Центру – протидія гібридним терористичним загрозам [5].

Беручи до уваги загальне поняття стійкості як «здатності матеріалів, людей або біотопів протистояти різким змінам або стресам, а також здатність до відновлення та повернення до попереднього нормального стану» [6], можна розуміти когнітивну стійкість у вузькому розумінні – як такий стан, коли розум може ідентифікувати та відбивати помилкове або спотворене уявлення про реальність; у більш широкому сенсі, наприклад, на державному рівні, можна розуміти це як умову забезпечення спроможності громадян чинити опір дезінформації та спотворенням, що надходять як зсередини, так і ззовні.

Застосовуючи концепцію когнітивної стійкості до контртероризму, можна сказати, що вона передбачає формування чіткого розуміння громадянами терористичної загрози та засобів протидії та запобігання їй, з одночасним забезпеченням того, що з цією загрозою та можливими наслідками терористичних атак поводяться раціонально, не нагнітаючи страх, тривогу та істерію. Як зазначають Баккер та Де Граф, «терористи, які нападають на стійке суспільство, матимуть значно менший вплив та не досягнуть своїх цілей» [6]. Суспільство має зрозуміти, що тероризм став новою «нормальністю». Незалежно від того, наскільки досконалі та широкомасштабні заходи безпеки застосовуються країнами, терористи знайдуть лазівки та адаптуються до нових реалій; навіть після того, як ІДІЛ буде остаточно переможена, з'являться нові форми терористичних мереж. У будь-якому випадку це не повинно пригнічувати суспільство, а навпаки – спонукати його до об'єднання та розробки системної відповіді, яка спрацює лише за умови тісної співпраці між урядом, приватним сектором та громадянами.

**Література**

1. Почепцов Г. Когнитивное пространство и информационные войны / Георгий Почепцов // Media Sapiens. – 2017. URL: http://osvita.mediasapiens.ua/trends/1411978127/kognitivnoe_prostranstvo_i_informatsionnye_voyny/.
2. Duggan P. Tactical CEMA in Cognitive Spaces / Patrick Duggan // Small Wars Journal. – 2017. URL: http://smallwarsjournal.com/jrnl/art/tactical-cema-in-cognitive-spaces.
3. Waltzman R. The Weaponization of Information: The Need for Cognitive Security / Rand Waltzman // RAND Corporation. – 2017. – URL: https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT473/RAND_CT473.pdf.
4. Рущенко І. П. Когнітивна безпека: погляди з Вашингтону, Москви і Києва / І. П. Рущенко, Н. В. Зубар // Оборонний вісник. – 2017. – URL: https://maidan.org.ua/wp-content/uploads/2017/09/CogSecComparison.pdf.
5. The European Centre of Excellence for Countering Hybrid Threats. – 2017. – URL: https://www.hybridcoe.fi/hybrid-threats/.
6. Bakker E. Towards a Theory of Fear Management in the Counterterrorism Domain: A Stocktaking Approach / E. Bakker, B. de Graaf // International Centre for Counter-Terrorism (ICCT) – The Hague. – 2014. – URL: https://www.icct.nl/download/file/ICCT-Bakker-de-Graaf-Towards-A-Theory-of-Fear-Management-in-CT-January-2014.pdf.

*УДК 342.95*

**Прозоров А.Ю.**
старший викладач
Національна Академія СБ України

## ПРАВОВЕ РЕГУЛЮВАННЯ ПРОТИДІЇ ПОШИРЕННЮ НЕГАТИВНОГО КОНТЕНТУ ЕКСТРЕМІСТСЬКОГО ХАРАКТЕРУ В ІНФОРМАЦІЙНОМУ ПРОСТОРІ

Мережа Інтернет на сьогоднішній день є одним з ефективних інструментів пропаганди терористичної та екстремістської діяльності, його специфіка полягає в тому, що велика частина щоденних користувачів онлайн-ресурсів становлять молоді люди. Правові норми, спрямовані на протидію поширенню матеріалів екстремістського характеру, законодавчо закріплені у таких країнах як Франція, Великобританія, Іспанія, Німеччина, Чехія, Словаччина, Словенія, Польща, Литва, Казахстан, Білорусь та інші. Екстреміз́м (від фр. extremisme, лат. extremus – крайній) – прихильність крайнім поглядам і, особливо, методам, діям, заходам у політиці [1]. Основи захисту суспільства від поширення екстремізму закладені у ст. 14 Конвенції про захист прав людини і основоположних свобод від 4 листопада 1950

року, в якої визначено, що користування правами та свободами, визнаними в цій Конвенції, має бути забезпечене без дискримінації за будь-якою ознакою – статі, раси, кольору шкіри, мови, релігії, політичних чи інших переконань, національного чи соціального походження, належності до національних меншин, майнового стану, народження, або за іншою ознакою [2]. З метою боротьби з молодіжним екстремізмом Уряд Великобританії в 2006 році видав спеціальну директиву по боротьбі з пропагандою і поширенням екстремізму в університетах і коледжах країни [3]. У листопаді 2010 року влада Великобританії акцентували свою увагу на боротьбі з активною діяльністю екстремістів в Інтернеті [4]. Відповідно до статті 108 Кримінального кодексу Болгарії людина, яка проповідує фашистську або іншу антидемократичну ідеологію чи насильницьку зміну суспільного і державного ладу, встановленого Конституцією Республіки Болгарія, підлягає кримінальній відповідальності [5].

Закон Республіки Казахстан «Про протидію екстремізму» передбачає поняття «екстремістських дій» – безпосередня реалізація дій в екстремістських цілях, включаючи публічні заклики до вчинення таких дій, пропаганда, агітація і публічна демонстрація символіки екстремістських організацій. У зв'язку з тим, що засоби масової інформації є джерелами поширення інформації для необмеженого кола осіб, законодавець допускає можливість поширення через засоби масової інформації екстремістських матеріалів. Згідно п. 7 ст. 1 закону під такими матеріалами розуміються будь-які призначені для оприлюднення або поширення документи або інформація на інших носіях, що закликають до здійснення екстремістських дій або обґрунтовують або виправдовують необхідність їх здійснення. У зв'язку з цим, з метою профілактики екстремізму уповноважений орган із засобів масової інформації відповідно до п. 2 ст. 6 закону проводить моніторинг продукції засобів масової інформації на предмет недопущення в них пропаганди і виправдання екстремізму, дотримання ними законодавства Республіки Казахстан [6]. Відповідно до ст. 17.11 Кодексу Республіки Білорусь про адміністративні правопорушення адміністративним правопорушенням є «виготовлення і (або) розповсюдження, а так само зберігання з метою поширення екстремістських матеріалів, якщо в цих діяннях немає складу злочину» [7].

В Кримінальному Кодексі України відсутні злочини, в диспозиціях яких було б пряме згадування екстремізму, але передбачені злочини, які вчиняються на підґрунті ненависті та нетерпимості або злочини терористичної спрямованості. На думку В. І. Боярова, до екстремістських можна віднести наступні групи злочинів, передбачені у КК України: 1) кримінально-карані діяння, які посягають на основи та безпеку політичного устрою (ст.ст. 109, 110, 111, 110-2, 113 КК України); (2) злочини терористичного характеру (ст.ст. 112, 258, 258-1, 258-2, 258-3, 258-4, 258-5, 260, 261,

278, 442, 443, 444 КК України) та (3) злочини (екстремістської спрямованості), які вчиняються з мотивів ненависті або ворожнечі стосовно осіб, які належать до певної етнічної, расової, релігійної, політичної та іншої соціальної групи (п. 14 ч. 2 ст. 115, ч. 2 ст. 121, ч. 2 ст. 122, ч. 2 ст. 126, ч. 2 ст. 127, ч. 2 ст. 129, ст. 161 та ст. 300 КК України) [8].

Відповідно до Доктрини інформаційної безпеки України актуальною загрозою національним інтересам та національній безпеці України в інформаційній сфері є: здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу Збройних Сил України та інших військових формувань, провокування екстремістських проявів, підживлення панічних настроїв, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні [9].

При цьому, в чинному законодавстві України відсутня адміністративна та кримінальна відповідальність за проведення вищезгаданої діяльності в частині провокування екстремістських проявів. З метою усунення та нейтралізації зазначених у Доктрині інформаційної безпеки України загроз національній безпеці України, вважаємо за доцільне удосконалити законодавче регулювання інформаційної сфери в частині введення адміністративної відповідальності за поширення в ЗМІ культу насильства та жорстокості, а також нерівності за ознаками статевої, расової, національної чи релігійної приналежності, якщо в цих діяннях немає складу злочину.

**Література**

1. Сайт Вікіпедія, сторінка екстремізм. – [Електронний ресурс]. – Режим доступу: // https://uk.wikipedia.org/wiki/Екстремізм.

2. «Конвенція про захист прав людини і основоположних свобод» від 04.11.1950 року, ратифіковано Законом України № 475/97-ВР від 17.07.97 – [Електронний ресурс]. – Режим доступу: // http://zakon2.rada.gov.ua/laws/show/995_004.

3. Виступ 14 листопада 2007 р. в Парламенті Великобританії прем'єр-міністра Гордона Брауна, prime minister Gordon Brown's Commons statement on anti-terrorism measures // BBC News. 2007. – [Електронний ресурс]. – Режим доступу: // http://news.bbc.co.uk/2/hi/uk_news/politics/7094620.stm.

4. Сайт поліції графства Суррей, Великобританія, сторінка "Prevent Violent Extremism" – [Електронний ресурс]. – Режим доступу: // http://www.surrey.police.uk/safety/prevent.asp

5. Болгарський правовий портал Lex.bg [Електронний ресурс]. – Режим доступу: // http://lex.bg/laws/ldoc/1589654529.

6. Закон «Про протидію екстремізму», підписаний Президентом Республіки Казахстан 18 лютого 2005 року № 31-III, «Юрист» – [Електронний ресурс]. – Режим доступу: //https://online.zakon.kz/Document/?doc_id=30004865#sdoc_params=text%.

7. Кодекс Республіки Білорусь про адміністративні правопорушення від 21 квітня 2003 р. № 194-З, Навигатор в мире права «Эталон online» – [Електронний ресурс]. – Режим доступу: // http://etalonline.by/?type=text&regnum=Hk0300194#load_text_none_1_

8. В.І. Бояров Криміналістична класифікація кримінально-караних проявів екстремізму Вісник Академії адвокатури України том 12 число 2(33) 2015, с. 210-216.

9. Указ Президента України № 47/2017 від 25 лютого 2017 року Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» / Офіційний вісник Президента України від 03.03.2017 – 2017 р., № 5, стор. 15, стаття 102.

*УДК 342.951:004*

**Радейко Р.І.**
кандидат юридичних наук
Навчально-науковий інститут права та психології
Національного університету «Львівська політехніка»

## БЛОКУВАННЯ ІНТЕРНЕТ-КОНТЕНТУ В МЕХАНІЗМІ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Швейцарський Центр з досліджень безпеки при Федеральній вищій технічній школі, у червні 2017 р. опублікував дослідження, присвячене кібернетичній та інформаційній війні в українському конфлікті [5]. Автори дослідження зазначають, що хоча й російська кібердіяльність стала широко помітною лише під час виборчої кампанії в США у 2016 р., насправді Росія постійно нарощувала та вдосконалювала свій потенціал у цій сфері протягом останніх десяти років. Перша демонстрація пов'язана кібератаками в Естонії в 2007 р. і продовжилася з російсько-грузинською війною в 2008 р. В українському конфлікті Росія продемонструвала свою здатність поєднувати кібер-можливості з електронними війнами, розвідкою і кінетичними можливостями [5, с. 4].

Важко не погодитися з тим, що значна кількість українського населення послуговується російськими соціальними мережами, використовує електронні пошти російських провайдерів та інші її інтернет-ресурси, що дає змогу російській владі «перехоплювати та читати – або ж слухати – усі діалоги, які ведуться на цих платформах» [5, с. 13].

З метою «формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни» [3], 25 лютого 2017 р. Президентом України Указом №47/2017 введено в дію рішення Ради національної безпеки і оборони України від 29 грудня 2016 року

«Про Доктрину інформаційної безпеки України» [3]. У цьому документі визначено, що для забезпечення інформаційної безпеки, слід законодавчого врегулювати не лише механізму блокування, але й виявлення, фіксації та видалення з українського сегмента мережі Інтернет, інформації, яка загрожує життю, здоров'ю громадян України, пропагує війну, національну та релігійну ворожнечу, зміну конституційного ладу насильницьким шляхом або порушення територіальної цілісності України, загрожує державному суверенітету, пропагує комуністичний та/або націонал-соціалістичний (нацистський) тоталітарні режими та їхню символіку [3].

15 травня 2017 р. Президент України підписав указ щодо застосування персональних спеціальних економічні та інші обмежувальні заходи (санкції), зокрема, до ТОВ «Мэйл.РУ ГРУП», ТОВ «Вконтакте», ТОВ «Вконтакті», ТОВ «Мейл.РУ Україна» у вигляді заборони Інтернет-провайдерам надання послуг з доступу користувачам мережі Інтернет до ресурсів сервісів «Mail.ru» та соціально-орієнтованих ресурсів «Вконтакте» та «Одноклассники» [2]. Однак в цьому Указі не було визначено причин та механізму блокування доступу до цих інтернет-сервісів, що зумовило неоднозначні оцінки експертів та широкої громадськості. Проте блокування даних інтернет-сервісів, слід розглядати крізь призму забезпечення безпеки, а не обмеження свободи слова. Особливої значущості ця теза набуває в контексті зміни політики соціально мережі Facebook після виявлення створення Росією фейковий акаунтів, для поширення у соцмережі політичної реклами під час останніх виборів президента США [4].

На початку червня 2017 р. один з громадян України оскаржив даний Указ Президента України [2] в частині блокування доступу до інтернет-ресурсів. Позивач зазначив, що оскаржуваний Указ у зазначеній частині прийнятий всупереч вимогам Закону України «Про санкції», порушує права на свободу вираження поглядів у відповідності зі статтею 10 Конвенції про захист прав людини та основоположних свобод, а також порушує право позивача на свободу доступу до інформації. Однак, ВАС України відмовив у задоволенні позовних вимоги через відсутність правових підстав, мотивував свою позицію тим, що у даному випадку спірним є не користування мережею в цілому, а лише заборона Інтернет-провайдерам на певний період здійснювати надання послуг з доступу користувачам мережі Інтернет до ресурсів певних сервісів, яка, у свою чергу, не створює перешкод для користування будь-якими іншими сервісами. Крім цього, на думку суддів ВАС України, спірним Указом позивача не обмежено у виборі форм і джерел одержання інформації. Окремі перешкоди, які можуть виникнути в процесі використання заблокованих інтернет–ресурсів, не обмежують права громадян на використання цих ресурсів, а спричинені виключно необхідністю створення негативних наслідків для осіб, щодо яких застосовано спеціальні економічні та інші обмежувальні заходи (санкції) [1].

Отже, при законодавчому врегулюванні цього питання в Україні слід закріпити процедуру формування списків веб-сайтів з детальним описом і

обґрунтуванням необхідності блокування кожного конкретного сайту. Будь-яке рішення про те, який контент необхідно блокувати, повинен приймати компетентний судовий орган або орган, який не перебуває ні під яким політичним, комерційним або іншим впливом.

**Література**

1. Постанова Вищого адміністративного суду України від 14 червня 2017 р. у справі № 800/198/17. URL: http://reyestr.court.gov.ua/Review/67196698.

2. Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року « Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)»: Указ Президента України від 15 травня 2017 р. № 133/2017 // Офіційний вісник України, 2017. – № 41. – Ст. 1276.

3. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25 лютого 2017 р. № 47/2017 // Офіційний вісник України, 2017. – № 20. – Ст. 554.

4. Цукерберг: Facebook виявив докази активності РФ в соцмережі і змінить алгоритми. URL: https://hromadske.ua/posts/tsukerberh-facebook-vyiavyv-dokazy-aktyvnosti-rf-v-sotsmerezhi-i-zminyt-alhorytmy.

5. Cyber and Information warfare in the Ukrainian conflict Zürich, Center for Security Studies (CSS), ETH Zürich, June 2017. URL: http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-01.pdf.

*УДК 355.40: 356.35*

**Сніцаренко П.М.**
доктор технічних наук,
старший науковий співробітник
**Саричев Ю.О.**
кандидат технічних наук,
старший науковий співробітник
**Ткаченко В.А.**
кандидат військових наук
**Грицюк В.В.**
Національний університет оборони України
імені Івана Черняховського

## ПІДСИСТЕМА МОНІТОРИНГУ ІНФОРМАЦІЙНОГО ПРОСТОРУ ЯК НЕОБХІДНА СКЛАДОВА СИСТЕМИ ПРОТИДІЇ НЕГАТИВНОМУ ІНФОРМАЦІЙНОМУ ВПЛИВУ НА ОСОБОВИЙ СКЛАД ВІЙСЬК (СИЛ)

Протидія негативному інформаційно-психологічному впливу – невід'ємна складова забезпечення інформаційної безпеки України, у тому

числі у воєнній сфері. Як визначено в статті за участю авторів [1], найбільш ефективна протидія такому впливу реалізується за кібернетичним принципом управління, де об'єктом управління є рівень морально-психологічного стану особового складу Збройних Сил України (далі – ЗС України). Однією з важливих складових в контурі такого управління має бути процес своєчасного і достовірного виявлення та оцінки рівня негативного інформаційно-психологічного впливу на визначену цільову аудиторію (в нашому випадку ЗС України). Таким чином, випливає проблемна потреба в створенні та постійному підтриманні дієздатності підсистеми для здійснення такого моніторингу.

Аналіз показує, що на сьогодні теорія протидії такому впливу обмежена на рівні концептуально-декларативних положень, а тому для практики є недосконалою. У ній бракує чітких формальних методів і методик для кількісних оцінок певних аспектів цієї сфери, у тому числі щодо виявлення та оцінки рівня негативного інформаційно-психологічного впливу на особовий склад ЗС України. З цієї причини його кількісна оцінка не проводиться, а оцінка морально-психологічного стану ЗС України, який є наслідком і такого впливу, здійснюється за якісними показниками на основі результатів моніторингу у військових частинах та підрозділах відповідно діючих інструкцій [2], тобто постфактум до наслідків різних впливів. Зазначене означає, що реально підсистема виявлення та оцінки рівня негативного інформаційно-психологічного впливу на особовий склад ЗС України відсутня, а це унеможливлює проведення, зокрема, випереджувальних заходів протидії для стабілізації морально-психологічного стану військ (сил), що вкрай необхідно.

Методологічний підхід до створення підсистеми моніторингу інформаційного простору для виявлення та оцінки рівня негативного інформаційно-психологічного впливу на особовий склад ЗС України базується на основі відповідної верифікованої методики, за допомогою якої визначаються необхідні кількісні показники [1]. Ця методика забезпечує можливість своєчасно та кількісно оцінити рівень такого негативного впливу на особовий склад ЗС України, а також тенденцію до зміни, що якраз і дозволяє реалізувати кібернетичну модель системи протидії негативному інформаційно-психологічному впливу на особовий склад військ (сил) та випереджено реагувати на розвиток негативного інформаційного процесу.

Виходячи із зазначеного, створення умов для випереджувальних стабілізаційних заходів потребує виконання таких вимог:

запровадити в системі протидії практику реагування на основі кількісних критеріїв оцінювання рівня негативного інформаційно-психологічного впливу;

застосувати в системі протидії підсистему моніторингу інформаційного простору на основі методики виявлення та оцінювання у кількісному

вимірі рівня негативного інформаційно-психологічного впливу на особовий склад військ (сил) з його квантуванням за ступенем значення для морально-психологічного стану ЗС України;

кожному квантовому рівню інформаційно-психологічного впливу на особовий склад військ (сил) має відповідати певна сукупність компенсаційних заходів протидії з метою стабілізації морально-психологічного стану визначеної цільової аудиторії, загалом ЗС України;

забезпечити контроль рівня морально-психологічного стану ЗС України шляхом моніторингових процедур безпосередньо у військах.

Підсистема моніторингу інформаційних процесів в інформаційному просторі держави для реалізації методики виявлення та оцінки рівня негативного інформаційно-психологічного впливу на особовий склад військ (сил) в загальній системі протидії може бути створена як трьохрівнева (рис. 1).

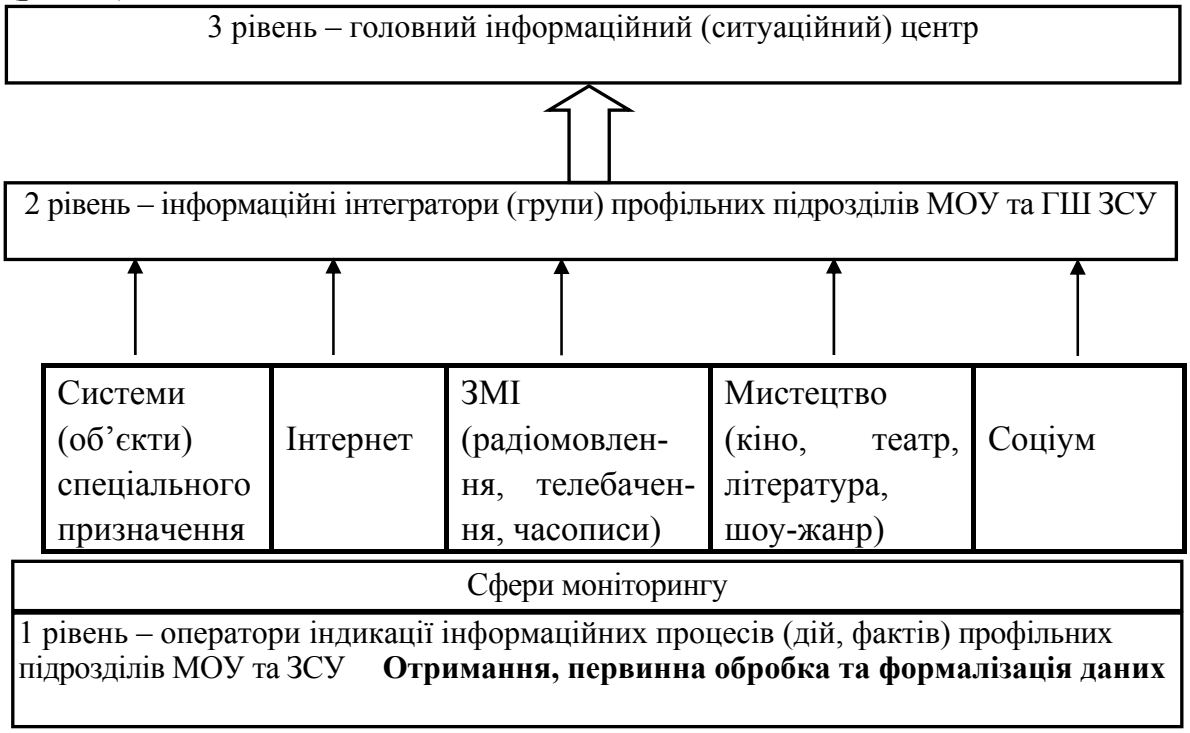



Рис. 1. Загальна структура трьохрівневої підсистеми моніторингу інформаційних процесів в інформаційному просторі держави

В цій підсистемі моніторингу:

1-й рівень – операторний (виявлення, первинна класифікація та індикація деструктивних інформаційних процесів за визначеними джерелами можливого впливу);

2-й рівень – узагальнення даних першого рівня за класифікаційними ознаками, вагова обробка отриманих формалізованих повідомлень;

3-й рівень – виявлення факту негативного інформаційно-психологічного впливу та оцінки його рівня за формалізованою інформацією другого рівня.

**Література**

1. Методичні основи виявлення та оцінки негативного інформаційно-психологічного впливу на особовий склад військ (сил) / П.М. Сніцаренко, Ю. О. Саричев, Ю.І.Михєєв, М.В.Праута // Наука і оборона. – № 3-4. – 2017. – С. 18-25.
2. Інструкція про порядок оцінки морально-психологічного стану в Міністерстві оборони України та Збройних Силах України (затверджено наказом МО України від 21.05.2013 № 335, зі змінами, внесеними наказом МО України від 17.12.2015 № 728, зареєстровано в Мін'юсті України 11.01.2016 № 29/28159).

*УДК: 316.255.01*

**Соколіна О.В.**
кандидат філософських наук
Військовий інститут Київського національного
університету імені Тараса Шевченка

# ДО ПИТАННЯ ГІБРИДНОЇ ВІЙНИ

Тема війни займає одне з центральних місць в життєдіяльності людства. Добро, зло, людяність, героїзм – це ті поняття, зміст яких був сформований війною. Сьогодні суспільство перейшло на новий етап розвитку – постіндустріальну епоху, якій властиві нові типи техноценозу та економіки. Для сучасного суспільства характерна зростаюча роль віртуальності, можливість обробляти великі й динамічні масиви інформації, виникнення нових соціальних технологій управління масами, індивідуальною поведінкою та бізнесом.

Сучасні події в Україні сприяли популяризації у засобах масової інформації теми *гібридної війни*, яка підіймає цілу низку питань, відповіді на які повинні допомогти зрозуміти, чому ведеться така війна. Адже вона технічна та інформаційно-психологічна тільки за формою, а за змістом – метафізична, тісно пов'язана із самою сутністю людини.

Основною метою гібридних війн є інформаційно-психологічний вплив на населення, а вже потім – економічно-політичні (торгівельні, газові, дипломатичні) протистояння. Зазначимо, що силові операції, які здійснюються паралельно інформаційно-психологічному впливу, мають на меті не стільки завоювати чи втримати територію, скільки вчинити хаос, спровокувати неперервний конфлікт та постійне генерування провокацій і таких військових дій, які будуть однобічно та гіпертрофовано висвітлюватися у зомбі-ЗМІ.

Треба зауважити, що гібридна війна планується не під стратегію фронтальної війни, а під стратегію інформаційної війни, де відбувається побудова альтернативної зомбі-реальності, всередині якої є можливим пере-

творення супротивника на ворога (того, хто приречений на фізичне знищення) і нелюдь (того, хто не має права вважатися людиною).

На думку Ф. Хофмана гібридній війні властиві п’ять елементів: модальність проти структури, одночасність, злиття, комплексність, злочинність [3]. Гібридну війну відрізняє від усіх інших видів війн те, що їй властиве одне правило – жодних правил.

Основним завданням гібридної війни є ідентоцид, тобто трансформація національної, державної та громадянської ідентичності країни-суперника до такого стану, коли про неї можна сказати одне – нелюдь і ворог. Суть ідентоциду – переконання більшості народу своєї країни, а в ідеалі і частини народу супротивника у злих намірах супротивника щодо своїх.

Усі сучасні медійні технології активно застосовуються в гібридній війні, і в першу чергу телебачення, тому що воно не потребує розумової діяльності для сприйняття інформації. Одним із новітніх атрибутів поширення інформації стала цифрова конвергенція, коли взаємопроникнення і злиття цифрової обчислюваної техніки й систем передачі даних відбувається на основі первинного оцифровування різнорідних інформаційних повідомлень (текстових, графічних, аудіовізуальних тощо). Одночасно знижуються витрати на обробку і доставку інформації та збільшуються і вдосконалюються функціональні можливості всього комплексу інформаційно-комунікаційних систем. Це дає можливість розширити аудиторію, стимулювати її інтерес, провокувати на відповідну реакцію [2].

Проте, є помилкою зводити гібридну війну тільки до її інформаційної складової, можливостей обробляти гігантські масиви даних, вибудовувати безструктурні суб’єкти. Така війна має свої особливі ознаки, а саме: це війна між різними рівнями цивілізаційного розвитку, де використовуються не тільки і не стільки воєнні засоби, а й легальні інструменти управління, демократії, культури, ЗМІ, освіти, що не відокремлює їх від повсякденного життя і робить ефективним засобом маніпулювання. Якщо раніше суб’єкти воєнних дій були цивілізаційно-порівняльними, використовували відносно однакові засоби, то сьогодні ведеться війна за рахунок розрізнення в цивілізаційному рівні розвитку. Гібридна війна ведеться і проти ворогів, і проти друзів, вона тотальна. Мислення та поведінка перепрограмовуються зовні таким чином, що люди самі руйнують свою державу та владу зсередини, відбувається саморуйнування. Інформаційні та соціальні технології легко проникають крізь структурні форми будь-якого походження і функціонування (державні кордони, влада) і засновані на поєднанні хаосу та впорядкування. Створюється ефект “примарного суб’єкта”, який є ефектом взаємодії двох аспектів свідомості – рефлексивної та захищеної від рефлексії [1].

Гібридна війна – це дія задля акумуляції та спрямованого застосування соціальної енергії. Але якщо в попередніх війнах мотивом до акумуля-

ції енергії були матеріальна зацікавленість, ідеологія, необхідність захисту держави, то у війні нового типу використовується енергія захоплення, що втілюється в сакральну енергію, яка конвертується в різні соціальні форми.

Гібридна війна є комплексним явищем. Про це яскраво свідчать фактори, які визначають її існування. Серед них можна назвати такі, як розвиток цивілізації, демократія, особисті свободи, світогляд та спосіб життя людей [2].

**Література**

1. Денисов А. "Призрачные" субъекты в управлении современным военным и политическим конфликтом / А. Денисов // Государственная служба. – 2010 – № 2 (64). – С. 67-70.

2. Дорошкевич А. Гібридна війна в інформаційному суспільстві / А. Дорошкевич // Вісник Національного університету "Юридична академія імені Ярослава Мудрого". Серія: Філософія – 2015. – № 2 (25). – С. 21-28.

3. Hoffman F. Future Threats and Strategic Thinking / Hoffman F. // Infinity Journal, No Fall 2011. – P. 17.

*УДК 316.485.26'64(477)*

**Соловйов С. Г.**
кандидат наук із соціальних комунікацій, доцент
Національна академія державного управління
при Президентові України

## НЕВЕРБАЛЬНІ НАРАТИВИ У СТРАТЕГІЧНИХ КОМУНІКАЦІЯХ

Комунікативна взаємодія органів публічної влади та інституцій громадянського суспільства реалізується через офіційні канали, визначені нормативно-правовими актами. Серед таких каналів – публікації в пресі та на інтернет-ресурсах, виступи, особисті прийоми, листування тощо. Загалом позиція сторін фіксується у вербальній формі.

Стратегічні комунікації мають інше співвідношення вербальності/невербальності, яке виражається пропорцією 20:80. Тобто більш вагомим є не текст, а образ, згенерований змінами у фізичному просторі. Про те, що дії у фізичному просторі містять інформаційну складову, зауважено, наприклад, у доповіді Міністерства оборони США [1].

Розглядаючи діяльність стратегічних комунікацій як таку, що спрямована на утвердження стратегічного наративу (мета-розповіді) в цільових аудиторіях, [2], важливо розглянути властивості невербального інструментарію.

Серед прикладів реалізації стратегічних комунікацій, наведених у [3], можна вирізнити і вербальну, і невербальну форми: приведення військ до

певного стану готовності або рух до певного географічного району; публікації про Великобританію, підготовані Британською Радою; Голос Америки та BBC World Service; британське антитерористичне законодавство; перша сторінка газети The Sun (британського таблоїда); рішення замінити Трайдент (заміна керівництвом США першого покоління ракет другим поколінням); обезголовлювання Аль-Каїдою заручників у помаранчевих комбінезонах.

Оскільки наведені тут невербальні форми визнаються практично реалізованими, то логічно передбачити подальше їх застосування і розвиток. Такі дії, як відкрита передислокація військ чи заміна зброї на досконалішу – це повідомлення супротивнику про наміри виконати певні дії. Це наратив, спрямований на досягнення стратегічної мети, яка може трактуватися як зміна поведінки ворога. Питання про те, чому в даному разі не застосовується вербальна форма (переговори, заяви) може мати таку відповідь: вербальна форма чітко фіксує позиції сторін, залишаючи мало можливостей для маневру.

До невербальних форм стратегічного наративу відносяться дії, зображення, які несуть символічне навантаження і достатньо повно розпізнаються цільовою аудиторією. До таких форм можна віднести пам'ятники, виставки, рішення про перейменування топонімів, нагородження визначних діячів, заснування нових інституцій.

Приклади в українській практиці: пам'ятники жертвам Голодомору в Україні, а також Національний музей «Меморіал жертв Голодомору» (наратив історичної пам'яті); виставка військової техніки із зони АТО (наратив захисту Вітчизни від агресії Росії), перейменування Кіровограда в Кропивницький (наратив історичної пам'яті, протистояння російським впливам), перейменування частини вулиці Інститутської в Києві на Алею Героїв Небесної Сотні (наратив історичної пам'яті, розвитку держави), заснування НАБУ, НАЗК, Міністерства у справах тимчасово окупованих територій (наративи боротьби з корупцією, протистояння агресії Росії, розвитку держави).

Невербальний наратив може містити і вербальний компонент, проте останній не фігурує як самодостатній. Наприклад, у пам'ятнику головним є власне фізична реалізація, задіяні образи, але він сприймається разом із текстовим поясненням щодо історичного значення відображуваної події.

Іншою формою втілення невербальних наративів є дії ключових учасників стратегічних комунікацій (посадових осіб). Це можуть бути поведінкова реакція на певні події, участь у виборах як кандидат, зустрічі із зацікавленими сторонами, започаткування важливого будівництва, підписання/непідписання закону, відвідування інших держав.

Властивості невербальних наративів описуються кількома позиціями. По-перше, невербальні наративи, діючи в комплексі з вербальними, ство-

рюють синергетичний ефект. По-друге, їхній вплив на аудиторію демонструє ефект «м'якої сили», оминаючи фільтри сприйняття аудиторії. По-третє, невербальний наратив може повторюватися (наприклад, у формі мистецької акції), або тривати (у вигляді музею) як завгодно довго, чого не завжди можна добитися застосуванням вербальних наративів.

**Література**

1. US Department of Defense : Report on Strategic Communication [Електронний ресурс]. – Режим доступу: http://www.au.af.mil/au/awc/awcgate/dod/dod_report_strategic_communication_11feb10.pdf.

2. Вступне слово директора Національного інституту стратегічних досліджень академіка НАН України В. П. Горбуліна // Стратегічні пріоритети, 2016. – № 4(41). – С. 6.

3. Cdr S A Tatham MPhil RN. Strategic Communication: A Primer, Advanced Research and Assessment Group, Defence Academy of the UK, England, 2008.

*УДК 159.9.072.42*

**Ступницька О.І.**
Військовий інститут КНУ імені Тараса Шевченка

## ПСИХОЛОГІЧНІ АСПЕКТИ ВЗАЄМОДІЇ У ВІРТУАЛЬНИХ СОЦІАЛЬНИХ МЕРЕЖАХ, ІНТЕРНЕТ ЗАЛЕЖНІСТЬ ТА ЇЇ СИМПТОМИ

Одним з основних методів інформаційного впливу на суспільство в теперішній час являється Інтернет-простір, під впливом якого формується лінія поведінки індивідуума.

У XXI столітті інформаційний простір наряді з природним, соціальним, культурним і т. п. відіграє все більш значну роль в діяльності і в повсякденному житті сучасної людини. Інформаційний простір, часто іменований «атмосферним», неоднорідний. З недавнього часу в ньому прийнято виділяти середовище Інтернету чи так званого «кіберпростору». Для останнього характерні своєрідні хронотопи, в рамках яких здійснюється психологічний аналіз поведінки індивідуума, певні специфічні аспекти, і тому представляють інтерес для психологічного аналізу – форми людської поведінки.

Такого роду поведінка в середовищі («середова поведінка») не обмежується пошуком, обробкою і передачею інформації, придбанням трансляції знань. У кіберпросторі, як в елементі інформаційного простору існує цілий конгломерат людських діяльностей, основу яких складають пізнавальна, ігрова та комунікативна діяльність. Специфічні особливості проті-

кання діяльності в Інтернет-просторі як в елементі інформаційного середовища, являється предметом досліджень спеціалістів-гуманітаріїв, в тому числі і психологів.

Не виключаючи значимості традиційних досліджень; і лабораторних, і екологічних, присвячених проблематиці систем «людина-машина» чи систем «людина-комп'ютер», все більш виразно прокладає собі шлях нова область досліджень, пов'язаних з вивченням діяльності людини, опосередкованими взаємопов'язаними глобальними комп'ютерними мережами, тобто Інтернетом і World-Wide-Web (WWW). Саме це викликає дуже глобальну проблему Інтернет-адикції.

Пояснюється це тим що за останні роки Інтернет і WWW перетворились на надзвичайно суттєвий фактор індивідуального та суспільного розвитку, зробивши кіберпростір привабливим для десятки мільйонів людей, особливо молоді. Це й зумовило мету нашої роботи – визначити психологічні особливості взаємодії індивідуума в кіберпросторі та виявлення Інтернет-залежності.

Взаємодію у віртуальній соціальні мережі можна інтерпретувати як організацію спільної діяльності віртуальної спільноти, що має на меті акумулювання інформації, її упорядкування, колективний доступ, обмін інформацією та обговорення на основі соціального сприйняття, взаєморозуміння, емоційного ставлення та підтримки між користувачами. У результаті спільної діяльності відбувається перетворення певних об'єктів, що мають для членів віртуальної спільноти предметно-практичну, пізнавальну та іншу цінність, та створення нових віртуальних об'єктів.

Віртуальні соціальні мережі є важливим агентом вторинної соціалізації особистості. Особливості взаємодії у віртуальних соціальних мережах як спільної діяльності користувачів досить сильно позначаються на розвитку їх особистості, проявляючись не лише у віртуальному просторі, але й у реальному житті. Тому серед перспективних напрямів дослідження можна виокремити вивчення впливу особистісних характеристик учасників на конструктивність мережевої взаємодії, динаміку розвитку мереж, психологічних чинників формування відносин довіри і взаємної підтримки серед користувачів віртуальних соціальних мереж тощо. А також були виділені психологічні та фізичні ознаки Інтернет-залежності, що як правило виникає при надмірному зловживанні віртуальними соцмережами та не нормованого часу сидіння за комп'ютером. Психологічна залежність виражається в наступному: ейфорія або просто гарне самопочуття при проводженні часу за комп'ютером; неможливість зупинитися і припинити проведення часу в мережі Інтернет; збільшення часу, яку людина проводить за комп'ютером (у всесвітній павутині); людина починає брехати про свою діяльність не тільки роботодавцю, вчителеві, командиру, але й членам сім'ї; при неможливості перебувати за комп'ютером людина відчуває

депресію, відчуття порожнечі і роздратування; людина віддає перевагу комп'ютеру, а не сім'ї і друзям; залежність від Інтернету супроводжується проблемками в навчанні або на роботі.

Фізичні симптоми: сухість в очах; головні болі; біль у спині; зміна режиму сну; розлади сну; недотримання особистої гігієни; пропуск прийомів їжі; об'їдання за комп'ютером; синдром карпального каналу, тобто тунельне ураження нервових клітин у руці (це пов'язано з перенапругою м'язів).

Таким чином, скоро слід очікувати появи такого діагнозу як «Інтернет-адикція». Лікування цього захворювання дуже важливе, так як до впливу «всесвітньої павутини» схильне сьогодні більша частина населення, особливо молодь. Найпильнішу увагу варто приділяти дітям та підліткам з іще не зміцнілою психікою і не здатних самостійно впоратися з таким впливом.

**Література**

1. Горошко Е.И. Коммуникативное пространство Интернета как объект социокультурного анализа / Е.И.Горошко // Вісник Одеського національного університету. Сер. «Соціологія і політичні науки». – Одеса, 2010. – Т. 15. – Вип. 14. – С. 130-136.

2. Лучинкина А.И. Психология человека в Интернете / А.И.Лучинкина. – К. : Информационные системы, 2012. – 200 с.

3. Интернет-зависимое поведение=Internet-addictive behavior: (обзор): (eview) / В.Л.Малигин [и др. ] // Журнал неврологии и психоатрии имени С.С.Корсакова. – 2011. – Т. 111. – № 8. – С. 86-92.

4. Burt R.S/Brokerage and Closure: An Introduction to Social Capital / R.S.Burt .- New York: Oxford University Press.2007.

*УДК 340.12*

**Тугарова О.К.**
кандидат юридичних наук, доцент
Національна академія СБ України

## НЕДОСКОНАЛІСТЬ ПРАВОВОГО РЕГУЛЮВАННЯ РЕКЛАМИ ЯК ДЕСТРУКТИВНИЙ ФАКТОР ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Закон України «Про основи національної безпеки» серед загроз в інформаційній сфері окремо виділяє намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації [1]. Останні події, які відбуваються в Україні і світі, засвідчили, що розповсюдження необ'єктивної і неповної інформації є не лише деструктивним фактором інформаційно-психологічної безпеки кон-

кретної особи, а і суттєво впливає на формування рівня свідомості окремих соціальних груп у заданому конкретному напрямку.

Найбільший вплив на суспільну свідомість відіграють засоби масової інформації і, зокрема, реклама. Вона формує переконання і переваги, моделює готові форми поведінки в різних ситуаціях, у значній мірі визначає образ і стиль життя. Водночас, отримана через рекламу інформація, часто сприймається суспільством як догма, через що реклама спричиняє стереотипізацію мислення, а відтак – є сугестивним фактором впливу на людську поведінку.

Сучасна реклама є складним і багатогранним явищем, яке необхідно досліджувати як у психологічній, так і правовій площині. Психологічний прояв реклами, передбачає цілеспрямований вплив на свідомість споживача з метою формування установки на придбання певного товару або послуг. Проте, відтворення зазначеної установки не виключає можливості настання для вітчизняного споживача певних негативних наслідків (про що, до речі, у рекламі і не згадується). На підтвердження сказаного можна навести приклади рекламних роликів щодо створення образу успішної людини: якщо хочеш бути впевненим у собі – купуй квартиру в престижному районі міста, якщо хочеш бути щасливим – бери кредит у банку. Щоправда, рекламодавець не інформує споживача, якими будуть правові наслідки у випадку несвоєчасного виконання зобов'язання, і як у подальшому банк псує життя тим позичальникам, які не можуть сплатити кошти за умови зростання курсу валюти та відсутності заробітної плати [2].

Схожа ситуація спостерігається у сфері реклами лікарських засобів: за даними Міністерства охорони здоров'я України (МОЗ України) та Національної ради України з питань телебачення і радіомовлення – реклама лікарських засобів, медичної техніки, методів профілактики і реабілітації, а також реклама харчових продуктів для спеціального дієтичного споживання, функціональних харчових продуктів та дієтичних добавок на рівні 29 % від загального обсягу реклами. Нині це найбільший сегмент рекламного ринку на телебаченні України. Проте, тексти реклами лікарських засобів не погоджуються в МОЗ України і часом, на думку державних органів, вони можуть мати нав'язливий характер, стимулювати людей до самолікування, або ж містять недостатньо інформації. І хоча правомірність трансляції реклами лікарських засобів, медичних виробів та методів профілактики, діагностики, лікування і реабілітації регулюється Законом України «Про рекламу» [3], відповідно до ст. 26 цього ж Закону, МОЗ України не включено до переліку державних органів, які уповноважені здійснювати контроль за рекламою. Відсутність одного компетентного органу та узгоджених дій між усіма зацікавленими державними органами робить випадки зловживань скоріше правилом, аніж винятком [4].

Ще однією проблемою правового характеру у сфері рекламної діяльності є реклама і пропаганда наркотиків. Відповідно до Закону України «Про

наркотичні засоби, психотропні речовини і прекурсори» [5], реклама наркотиків та психотропних речовин на території України може поширюватися виключно у спеціалізованих друкованих виданнях чи будь-яких інших засобах інформації, спеціально призначених для медичних, фармацевтичних, наукових працівників у сфері охорони здоров'я (ст. 35 Закону).

Останнім часом ряд українських телеканалів та Інтернет-видань підняли питання щодо поширення в українських містах граффіті, що рекламують наркотичні та психотропні препарати. Написи на фасадах житлових будинків, спорудах біля шкіл стали покажчиком адрес, де можна купити наркотики. Зазвичай трафаретна реклама, залишена на стінах будинків, містить назву сайту і назву пропонованих речовин: «сіль», «гаш», «ЛСД». На боротьбу з наркографітті стали звичайні люди, небайдужі городяни взялися зафарбовувати небезпечну рекламу. Утім, на сьогоднішній день, – за словами представників правоохоронних органів, – телеграм-канали, які відкрито рекламуються, неможливо заблокувати. Тому що сервери розташовані за кордоном і вони під дуже серйозним конфіденційним захистом [6]. Вбачається, що вирішенню означеної проблеми повинні сприяти міжнародні договори України із зарубіжними країнами, а також окремою нормою повинна бути введена заборона незаконного рекламування та пропаганди наркотичних засобів як в Законі України «Про рекламу», так і в Кримінальному кодексі України.

**Література**

1. Про основи національної безпеки: Закон України від 19 червня 2003 року //Відомості Верховної Ради України (ВВР), 2003. – № 39. – Ст. 351.

2. Литвиненко С. Соціальна реклама «за» чи «проти» наркотиків? [Електронний ресурс] / С.Литвиненко. – Режим доступу до джерела http://lagoda.org/uk/fest/articles/105-socreklama-narkotikov (дата звернення: 03.03.2018).

3. Про рекламу: Закон України від 3 липня 1996 року // ВВР України, 1996. – № 39. – Ст. 181

4. Реклама лікарських засобів: органи влади мають намір посилити контроль [Електронний ресурс]. – Режим доступу до джерела https://www.apteka.ua (дата звернення: 05.03.2018).

5. Про наркотичні засоби, психотропні речовини і прекурсори: Закон України від 15 лютого 1995 року // ВВР України, 1995. – № 10. – Ст. 60.

6. Города Украины заполонили наркограффити [Електронний ресурс]. – Режим доступу: https://www.segodnya.ua (дата звернення: 05.03.2018).

*УДК 342/354*
**Хаба Р.С.**
Департамент захисту
національної державності СБ України

# ДЕСТРУКТИВНІ ІНФОРМАЦІЙНІ ВПЛИВИ В СУЧАСНИХ РЕАЛІЯХ

Головним стратегічним завданням інформаційної безпеки України є створення потужного національного інформаційного простору, як головного аспекту присутності держави в світовому інформаційному просторі. Крім того, таке завдання включає створення системи протидії інформаційним загрозам та захист власного інформаційного простору, інформаційної інфраструктури та інформаційних ресурсів держави.

Одним із найбільш проблемних питань в системі забезпечення національної безпеки України є протидія інформаційно-психологічній війні, яка набула систематичного, добре спланованого і довготривалого у часі характеру з боку країни-агресора.

Саме формування іноземними засобами масової інформації альтернативної до дійсності викривленої інформаційної картини світу, у т.ч. - через призму подій в Україні, приниження української мови і культури, фальшування української історії тощо є однією з форм ведення інформаційної війни проти нашої держави та виправдання власної агресивної політики, спрямованої на підрив суспільно-політичної стабільності з метою знищення держави Україна і захоплення її території.

Головними інформаційним спрямуваннями іноземних країн, які використовуються для пропагування власних інтересів на території України і ескалації внутрішньополітичної ситуації на територіях, що є об’єктами геополітичних інтересів суміжних держав, вважаємо, є наступні:

- підрив авторитету вищих органів державної влади в Україні;
- ідеологічне обґрунтування федералізації України із трактуванням приналежності у минулому окремих регіонів України до суміжних країн;
- поширення автономістських та сепаратистських настроїв у регіонах геополітичних інтересів;
- інформаційна підтримка громадських об’єднань та рухів радикального і сепаратистського налаштування з відвертою антиукраїнською ідеологією;
- створення передумов до виникнення конфліктів на національному підґрунті, що може бути використано для «оправдання» самопроголошення нових територіальних автономних утворень.

Водночас, аналізуючи весь спектр засобів для реалізації зовнішньої інформаційної експансії, можна стверджувати, що головними негативними наслідками для України є наступні:

- загострення міжнаціональних, етноконфесійних та інших суспільно важливих відносин в регіонах, де компактно проживають представники інших національностей, що, в свою чергу зумовлює міжнародне напруження в питаннях забезпечення прав і свобод національних меншин між Україною та державами-сусідами;

- штучне створення на міжнародній арені іміджу України як «ненадійного» економічного партнера, наслідком чого є суттєве зменшення інвестиційної привабливості нашої країни та, як наслідок, відтоку інвестицій з території України та призупинення реалізації міжнародних комерційних проектів;

- блокування, шляхом здійснення точкових інформаційних операцій, підписання вигідних для України економічних договорів в частині налагодження вигідного експорту новітнього озброєння, продукції харчової, фармакологічної, металургійної, хімічної, енергетичної галузей промисловості, інших економічно вигідних та конкурентоспроможних продуктів народного господарства України.

Актуальним науковим і практичним завданням у сфері забезпечення інформаційної безпеки України є досягнення єдиного підходу до визначення оптимальних моделей і шляхів забезпечення інформаційної безпеки держави на основі виявлення найважливіших якісних і кількісних властивостей та параметрів цього явища.

Інформаційна безпека може бути реалізована як за умови побудови чітко структурованої системи протидії із залученням державних і громадських організацій, так і при виконанні першочергових превентивних заходів протидії в межах українського медіа-сектору, зокрема:

- допомога держави провідним українським агентствам, національним теле- і радіокомпаніям, друкованим ЗМІ у відкритті закордонних кореспондентських пунктів з метою розширення аудиторії зарубіжних споживачів їх продукції та оприлюднення раціонально підібраної та зваженої інформації, яка нівелюватиме негативні інформаційні акції на шкоду Україні;

- налагодження конструктивного діалогу із відповідальними представниками владних інституцій країн-сусідів з метою досягнення паритетних умов щодо формування взаємовигідної інформаційної політики між державами та дотримання основоположних принципів взаємоповаги в частині висвітлення суспільно важливих подій як з боку України, так і країн-партнерів;

- впровадження державного протекціонізму у підтримці вільної від політичної кон'юнктури ефективної просвітницької діяльності шляхом залучення мас-медіа та видавничо-поліграфічних підприємств: широке поширення і запровадження дотаційних проектів на друк літератури історичного, культурного, патріотично-виховного характеру, теле- та радіопроектів, виготовлення якісної соціальної реклами ідеологічно-патріотичного спрямування тощо;

- поетапне встановлення квот щодо присутності в ефірі телерадіоорганізації аудіовізуального продукту українського виробництва;

- фінансова і правова підтримка створення і поширення українськомовної інформаційної продукції, розповсюдження у світі вітчизняної культурно-мистецької та друкованої продукції;

- удосконалення нормативно-правового регулювання питань щодо користування каналами мовлення, ретрансляції програм, використання радіочастотного ресурсу України, стандартів діяльності телерадіоорганізацій;

- збалансування інтересів вітчизняних телерадіоорганізацій всіх форм власності, забезпечення проведення прозорої процедури ліцензування їх діяльності;

- реалізація програми створення системи суспільного телебачення та радіомовлення, із забезпеченням її незалежності від політичних, фінансово-промислових та вузько-ідеологічних впливів. Забезпечення отримання суб'єктам суспільного телебачення «ексклюзивної інформації від перших осіб», що може стати своєрідним «цехом гарячих новин», на який при цитуванні будуть змушені посилатися інші інформаційні ресурси.

*УДК 004.4:656.2 (477)*

**Чередниченко О.Ю.**
кандидат економічних наук, доцент
Інститут підготовки юридичних кадрів для СБ України
Національного юридичного університету
імені Ярослава Мудрого

## АКТУАЛЬНІСТЬ ОСУЧАСНЕННЯ СИСТЕМИ КОМПЛЕКСНОГО ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ НАЦІОНАЛЬНОГО ЗАЛІЗНИЧНОГО ПЕРЕВІЗНИКА – ПАТ «УКРЗАЛІЗНИЦЯ»

Залізничний транспорт – виробничо-технологічний комплекс підприємств залізничного транспорту, призначений для забезпечення потреб суспільного виробництва і населення країни в перевезеннях у внутрішньому і міжнародному сполученнях та надання інших транспортних послуг усім споживачам без обмежень за ознаками форми власності та видів діяльності тощо [1, с. 1]. В сучасних умовах залізнична галузь має стратегічне значення, без функціонування якої неможливо забезпечити не тільки потреби населення та суспільного виробництва в перевезеннях, а й оборону держави, її життєдіяльність.

Враховуючи вищенаведене та розпочату інтеграцію залізничного транспорту до європейської транспортної системи, виникає наявна потреба його переходу на нові, сучасні стандартів ЄС в логістичному секторі.

Це стосується не тільки виробничого процесу, а й організації документообігу, звітності і т. ін. В останні роки на залізницях України широке розповсюдження знаходить використання електронних документів та розвиток електронного документообігу, це стосується і документів де налічується інформації з обмеженим доступом, або такої що є власністю держави. Публічне акціонерне товариство (ПАТ) «Укрзалізниця», як головний національний залізничний перевізник постійно працює над впровадженням нових технологій, активно займатися комп'ютеризацією, інформатизацією та автоматизацією робочих місць, а також їх захистом. На даний час на залізницях вже діє певна модель ІТ-супроводження майже всіх виробничих процесів, яка дотримується норм діючого законодавства, хоча не є досконалою.

Згідно з вимогами законодавства України, інформація, що є власністю держави, або інформація з обмеженим доступом, повинна оброблятися із застосуванням комплексної системи захисту інформації (КСЗІ) з підтвердженою відповідністю. Комплексна система захисту інформації – взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації [1, с. 1]. Обмін інформацією повинен здійснюватися з використанням інформаційно-телекомунікаційних систем як внутрішнього так і загального користування. Згідно закону України «Про захист інформації в інформаційно-телекомунікаційних системах» інформація, що є власністю держави або інформація з обмеженим доступ, повинна бути захищена шляхом побудови КСЗІ з отриманням «Атестата відповідно-наслідком», який видається Державною службою спеціального зв'язку та захисту інформації (ДССЗЗІ).

В той же час, сучасна та якісна організація процесу перевезень пасажирів і вантажів, робота з клієнтами можлива при умові підключенні до інших інформаційно-телекомунікаційних систем, в тому числі міжнародних, а це неможливо без використання глобальної світової системи Інтернет. Тому, проблема захисту інформаційних ресурсів залізничного транспорту набуває актуальності та вимагає не тільки наявності саме комплексної системи захисту інформації, а й її постійної модернізації, осучаснення з метою дієвого протистояння новим ризикам та викликам з боку кіберзлочинності. В якості прикладу можна навести кібератаку на інформаційні ресурси залізничного транспорту влітку минулого року з використанням, так званих модифікацій, вірусу «Petya».

Комплексний підхід, як правило, використовується для захисту великих систем, саме такі системи впроваджуються на залізничному транспорті. В цьому випадку необхідно забезпечити виконання наступних заходів:

- організаційні заходи по контролю за персоналом, який має високий рівень повноважень на дії в системі (програмісти, адміністратори баз даних мережі ті ін.);

- організаційні та технічні заходи по резервуванню критично важливої інформації;

- комплексні заходи по відновленню працездатності системи у випадку виникнення нештатних ситуацій;

- комплексні заходи по управлінню доступом в приміщеннях де знаходиться обчислювальна техніка і т.д.

Залізнична галузь має певний досвід та напрацювання щодо захисту власних інформаційних ресурсів, має кваліфіковані кадри та в змозі фінансувати роботи з захисту інформаційних ресурсів. Виконання цієї роботи на залізничному транспорті покладено на фахівців підрозділів інформаційних технологій та Інформаційно-обчислювальних центрів (ІОЦ) товариства. На нашу думку, для більш ефективного функціонування комплексної системи захисту необхідна тісна взаємодія та плідна робота з фахівцями Держспецзв'язку, Департаменту кіберполіції Національної поліції України, Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБ України.

**Література**

1. Про залізничний транспорт : Закон України від 4 липня 1996 р. № 273/96-ВР // Відомості Верховної Ради України. – 1996. – № 40.

2. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07. 1994 р. № 80/94-ВР // Відомості Верховної Ради України. – 1994. – № 31.

*УДК 342.95*

**Черняк А. М.**
Департамент захисту
національної державності СБ України

## АКТУАЛЬНІ ПИТАННЯ ЗАХИСТУ ІНФОРМАЦІЙНОГО ПРОСТОРУ

На даний час ситуація в національній інформаційній сфері достатньо складна, що, серед іншого, пов'язане як з інформаційним впливом російських медіа на населення так і з технічними проблемами мовлення українських електронних засобів масової інформації в окремих регіонах нашої держави. Фіксуються деструктивного використання ЗМІ окремими політичними партіями, рухами, блоками, громадськими та фінансовими об'єднаннями, без урахування необхідності збереження в Україні загальнонаціональної стабільності. Водночас, спостерігаються непоодинокі спроби іноземних ЗМІ дестабілізувати суспільно-політичну обстановку,

шляхом оприлюднення матеріалів, зміст яких, за допомогою перекручування фактів історичної, національної самобутності українського народу, впливає на створення атмосфери бездуховності, негативного ставлення до культури та історичної спадщини у суспільстві.

Так, провідний інформаційний вплив країною-агресором здійснюється через можливості російських ЗМІ та проросійських мас-медіа, з позицій медіа-холдингу «Газпром-медіа» (підконтрольний Уряду РФ, телеканали «НТВ», «ТНТ», «НТВ+», радіокомпанія «Эхо Москвы» та ін.). В національному кабельному телебаченні рейтинговими були федеральні російські мовники: «ОРТ», «РТР», «Россия-1», «НТВ», «Russia Today» та ін. Зважаючи на наведені спрямування іноземної сторони, з урахуванням внесення змін до законодавства у сфері телерадіомовлення та/або рішень Національної ради України з питань телебачення і радіомовлення, вітчизняними теле- та радіоорганізаціями, провайдерами програмних послуг, що мають відповідну ліцензію, припинено трансляцію програм, зміст яких не відповідає вимогам Європейської конвенції про транскордонне телебачення і ретрансляція яких на території України обмежується згідно з ч. 1 ст. 42 Закону України «Про телебачення і радіомовлення» [1].

На даний час, Національною радою України з питань телебачення і радіомовлення виключено з переліку іноземних програм, дозволених для ретрансляції на території України, понад сімдесят російських телеканалів, серед яких «Первый канал. Всемирная сеть», «РТР-Планета», «Россия-24», «НТВ-Мир», «TVCI», «Россия-1», «НТВ», «ТНТ», «Петербург-5», «Звезда», «РЕН-ТВ», «Russia Today», «РБК-ТВ», «История» (ВГТРК), «365 дней», «24 Техно», «Мир 24» та ін.

Що стосуються технічних аспектів ситуації в національній інформаційній сфері, слід відмітити, що державою-агресором ефективно використовуються можливості передавальних центрів, які розташовані у таких прикордонних російських містах як Бєлгород, Шебекіне і Валуйки, Красноперекопськ АР Крим та Григоріополь і Тирасполь невизнаної Придністровської Молдавської Республіки, для поширення сигналів електронних засобів масової інформації Російської Федерації на частини територій північних і південно-східних регіонів нашої держави.

Поряд із цим, зазначеній діяльності російської сторони, суттєво сприяє відсутність якісного сигналу як аналогового, так і цифрового формату національного телемовлення у прикордонних областях України, що надає можливість місцевому населенню приймати відносно якісний сигнал телецентрів, які ретранслюють програми заборонених в Україні російських телеканалів, розташованих в Молдові, Румунії та невизнаній Придністровській Молдавській Республіці. Зазначене зумовлене завищеною потужністю іноземних передавачів та, частково, прорахунками українських фахівців щодо допустимого рівня випромінювання національних ретрансляторів.

Таке становище обумовлює доцільність надання пропозицій державним органам влади щодо покращення технічного забезпечення вітчизняної інформаційної сфери.

**Література**

1. Закон України «Про телебачення і радіомовлення» від 21.12.1993 року № 3759-XII // Відомості Верховної Ради. – 1994. – № 10.

*УДК 35.073.53*

**Чеховська М.М.**
доктор економічних наук, професор
Національна академія СБ України

## ЗАДОВОЛЕННЯ ПОТРЕБ ПІДПРИЄМСТВ І ОРГАНІЗАЦІЙ У ДОСТУПІ ДО ІНФОРМАЦІЇ ЯК ЕЛЕМЕНТ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

У Доктрині інформаційної безпеки України серед національних інтересів нашої держави в інформаційній сфері є, зокрема, «всебічне задоволення потреб громадян, підприємств, установ і організацій усіх форм власності у доступі до достовірної та об’єктивної інформації» та «забезпечення вільного обігу інформації» [2]. Разом з цим, Закон України «Про основні засади забезпечення кібербезпеки України» широко окреслює підприємства, установи та організації незалежно від форми власності, що відносяться до об’єктів критичної інфраструктури, та покладає на власників або керівників зазначених підприємств відповідальність за забезпечення кіберзахисту їх комунікаційних і технологічних систем [1]. Іншими словами, встановлюється персональна відповідальність за забезпечення кібербезпеки та інформаційної безпеки підприємств та установ усіх форм власності, у тому числі за допомогою наявних інформаційних та технічних ресурсів.

Серед зазначених ресурсів можна виокремити затверджену систему національних стандартів, у тому числі щодо заходів інформаційної безпеки та систем управління інформаційною безпекою. Наголосимо, що дотримання зазначених стандартів є життєво необхідним для ефективної діяльності будь-якого підприємства. Зокрема, для забезпечення інформаційної безпеки діють ДСТУ ISO/IEC 27001:2015 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги», ДСТУ ISO/IEC 27002:2015 «Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки», ДСТУ ISO/IEC 27005:2015 «Інформаційні технології. Методи захисту. Управління ризи-

ками інформаційної безпеки», ДСТУ ISO/IEC 27006:2015 «Інформаційні технології. Методи захисту. Вимоги до органів, які надають послуги з аудиту і сертифікації систем управління інформаційною безпекою». Наголосимо, що міжнародні стандарти, на які, власне, спираються національні стандарти, не є сталими і змінюються практично щороку. Відповідно, уповноважені органи оновлюють і національні стандарти.

Проблемою у даному випадку є платний доступ до зазначеної інформації для підприємств та організацій усіх форм власності. Тобто, з одного боку, процес перекладу міжнародних документів на державну мову є витратним, з іншого боку, доступ до таких документів обмежується фінансовими можливостями підприємства.

На нашу думку, державні стандарти є такими саме нормативно-правовими документами, як закони України, укази Президента, кодекси, постанови Верховної Ради України тощо і доступ до них має бути вільним. Тим більше, що такою є світова практика, коли існують ресурсні центри для забезпечення легкого доступу до правових матеріалів.

**Література**

5. Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163 – VIII [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/2163-19.

6. Указ Президента України № 47/2017 від 25 лютого 2017 року Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/47/2017.

# УДОСКОНАЛЕННЯ СИСТЕМИ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ ТА СЛУЖБОВОЇ ІНФОРМАЦІЇ УКРАЇНИ З УРАХУВАННЯМ ДОСВІДУ ПРОВЕДЕННЯ АТО

*УДК 341.824:338.47(043.2)*
**Богомолов О.О.**
Воєнно-дипломатична академія
імені Євгенія Березняка

## АВТОМАТИЗАЦІЯ РЕЖИМНО-СЕКРЕТНОЇ ДІЯЛЬНОСТІ ТА УПРАВЛІННЯ ДОСТУПОМ ДО ІНФОРМАЦІЙНИХ РЕСУРСІВ

Сьогодні застосування комп'ютерних технологій у системі документообігу та управлінської діяльності в більшості установ та організацій, бізнес структурах та навчальних закладах стало нормою сучасного стилю ділового життя. Будь-які процеси суспільства, бізнесу та виробництва потребують автоматизації, а на ринку праці нарощуються вимоги з професійних навичок до кандидатів на роботу, яка передбачає документування [1, 2].

Враховуючи стрімкість та невідворотність переходу управлінської діяльності з фізичного до електронного документування, в тому числі з використанням віртуальних ресурсів кібернетичного простору, більшість державних органів, установ та організацій вищої та середньої ланки мають успішні реалізації перших етапів автоматизації процесу управління шляхом утворення внутрішніх локальних обчислювальних мереж.

Не виключенням з правил є органи управління силових структур держави, зокрема Міністерство оборони України. Специфіка діяльності такого міністерства в складних умовах розбудови європейського вектору, а також ведення гібридної війни із сильним та технологічно розвинутим агресором, вимагає максимальної концентрації на оперативності обробки інформації що надходить з районів проведення антитерористичної операції (АТО), прихованості відомостей щодо провадження реформ системи управління збройними силами, а також використання сучасних форм та методів обробки й аналізу інформації в процесах вироблення рішень, які мають запобігти неправомірним діям ворожої сторони та локалізувати її агресивні наміри.

Цілком зрозуміло, що така інформація здебільшого містить відомості з обмеженим доступом, що суттєво ускладнює процеси її оперативної обробки, передачі каналами зв'язку або телекомунікаційними системами, а також доведення до споживача.

Розбіжність нормативно-правової бази в сфері охорони державної таємниці, криптографічного та технічного захисту інформації, сьогодні розмиває межі відповідальності щодо збереження саме електронних секретних документів, а також порушують стандарти щодо порядку надання доступу до таких документів. Наслідками таких спорів є численні факти витоку інформації з обмеженим доступом саме технічними каналами витоку [3-9].

Враховуючи зазначене, автоматизація секретного діловодства повинна інтегруватись в інформаційно-телекомунікаційні системи (ІТС) локального застосування, а режимно-секретні органи повинні мати авторські права на реалізацію функції надання доступу користувачам до електронних відомостей, що містять державну таємницю, а також здійснення незалежного аудиту дій користувачів з такою інформацією.

Для реалізації таких завдань в сфері охорони державної таємниці необхідно:

1. Визначити нормативно-правовими актами порядок створення та використання ІТС в інтересах провадження діяльності, пов'язаної з державною таємницею.

2. Розробити та ліцензувати єдині програмно-апаратні комплекси засобів захисту секретної електронної інформації для забезпечення повноцінного управління доступом до секретних інформаційних ресурсів.

3. Розробити спеціальне програмне забезпечення для впровадження електронних номенклатур (реєстрів) посад користувачів системи, які мають право на обробку інформації з обмеженим доступом в ІТС, на базі яких будуть сформовані електронні паспорта посад таких користувачів та визначені переліки дій в системі.

4. З метою недопущення несанкціонованого доступу до інформації в ІТС розглянути можливості провадження фвухфакторної аутентифікації в доменах операційних систем, а також використання носіїв ключової інформації не лише як носіїв цифрового підпису а й ключів входу в інформаційний простір із визначенням прав доступу до відомостей в системі.

## Література

1. Горбулін В.П. Качинський А.Б. Системно-концептуальні засади національної безпеки України. – К. : НВЦ Євроатлантикінформ, 2007. – С. 592.

2. Горбулін В.П. Проблеми захисту інформаційного простору України : моногр. / В.П.Горбулін, М.М.Биченок. – К. : Інтертехнологія, 2009. – С. 136.

3. Про інформацію : Закон України від 02.10.92 № 2657-XII. [URL: 05.02.2018] http://zakon2.rada.gov.ua/laws/show/2657-12– 2011.

4. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.94 № 80/94-ВР – [URL: 05.02.2018] http://zakon3.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80– 1994.

5. Про державну таємницю : Закон України від 21.01.94 № 3855-XII [URL: 05.02.2018] http://zakon1.rada.gov.ua/laws/show/3855-12 – 1994.

6. Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу “2” /НД ТЗІ 2.5-008-2002/ДСТСЗІ СБ України. – 2002.

7. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу / НД ТЗІ 1.1-003-99/ДСТСЗІ СБ України. – 1999.

8. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.17 № 2163-VIII [URL: 05.02.2018] http://zakon5.rada.gov.ua/laws/show/2163-19 – 2017.

9. Стратегія кібербезпеки України : Указ Президента України . №96/2016. [URL: 05.02.2018] http://zakon0.rada.gov.ua/laws/show/96/2016.

*УДК: 342.1+355/359*

**Болдир С.В.**
Начальник Департаменту охорони державної таємниці
та ліцензування Служби безпеки України

## АДАПТУВАННЯ ВИМОГ ЗАБЕЗПЕЧЕННЯ РЕЖИМУ СЕКРЕТНОСТІ ДО УМОВ ВЕДЕННЯ ВОЄННИХ (БОЙОВИХ) ДІЙ З УРАХУВАННЯМ ДОСВІДУ ПРОВЕДЕННЯ АТО

Виклики сьогодення, які зумовлені, передусім, збройною агресією Російської Федерації проти України, окупацією частини території нашої суверенної держави, вимагають вжиття суб’єктами забезпечення національної безпеки комплексу заходів, спрямованих, зокрема і на удосконалення системи охорони державної таємниці з урахуванням досвіду проведення антитерористичної операції.

Насамперед слід зазначити, що правові засади та підходи до забезпечення схоронності інформації з обмеженим доступом, запроваджені в Україні, за висновками експертів Офісу безпеки НАТО, безпекових структур ЄС, а також Національних органів безпеки держав-учасниць зазначених міжнародних організацій, є достатньо ефективними та збалансованими [1].

Водночас, практика застосування Службою безпеки України закріплених у Законах України «Про державну таємницю» та «Про Службу безпеки України» повноважень щодо забезпечення охорони державної таємниці в умовах антитерористичної операції на території Донецької та Луганської областей засвідчила, що процедури забезпечення охорони державної таємниці, передбачені на мирний час, не завжди є ефективними в умовах ведення (воєнних) бойових дій чи спеціальних операцій.

Саме тому, з метою вирішення нагальних проблемних питань, що виникли у ході забезпечення режиму секретності під час проведення антитерористичної операції, робочою групою у складі експертів підрозділів ЦУ СБУ та за участі представників заінтересованих державних органів вжито заходи з розробки Порядку забезпечення охорони державної таємниці в органах військового управління, військових частинах, установах і організаціях Збройних Сил України, інших військових формуваннях, правоохоронних органах спеціального призначення та підрозділах окремих державних органів в районах (зонах) ведення ними воєнних (бойових) дій або спеціальних операцій, який затверджено постановою Кабінету Міністрів України від 04.10.2017 № 750 (далі – Порядок-750).

Зазначений акт Уряду передусім спрямований на оптимізацію впровадження заходів охорони державної таємниці, адаптованих до умов ведення воєнних (бойових) дій, що сприятиме своєчасному реагуванню на загрози національним інтересам України.

Тому, з огляду на важливість забезпечення охорони секретної інформації під час ведення воєнних (бойових) дій, яким на сучасному етапі розвитку притаманно динамічність, рішучість, рухливість, маневреність учасників військового протистояння, вбачається за доцільне розглянути основні підходи до забезпечення режиму секретності за таких умов, що впроваджуються Порядком-750, а саме:

1. Окремий порядок надання спеціального дозволу на провадження діяльності, пов’язаної з державною таємницею військовим формуванням, які змінюють умовне найменування та/або місце дислокації, відмобілізовуються (доукомплектовуються).

2. Оптимізація та адаптація до існуючих умов порядку ведення секретного діловодства шляхом його спрощення для військових формувань, які виконують завдання безпосередньо в районі ведення воєнних (бойових) дій або спеціальних операцій (уникнення накопичення документів, можливість використання комбінованого журналу для реєстрації (обліку) матеріальних носіїв секретної інформації тощо);

3. Врегульовано окремі питання порядку доставки, зберігання матеріальних носіїв секретної інформації в районі ведення воєнних (бойових) дій чи спеціальних операцій:

- передбачено можливість зберігання матеріальних носіїв секретної інформації у валізах, мішках, ящиках, що опечатуються;

- спрощення порядку знищення секретних документів під час їх транспортування чи особистого зберігання особовому складу військових формувань, які виконують завдання в районі ведення воєнних (бойових) дій чи спеціальних операцій;

5. Встановлено вимоги до організації розміщення режимно-секретних органах в районах (зонах) ведення воєнних (бойових) дій та забезпечення

охорони і оборони (направлені, зокрема, і на надійне зберігання матеріальних носіїв секретної інформації, а також виключення можливості витоку такої інформації за межі режимного приміщення);

6. Заслуговує уваги й норма, якою оптимізовано процедуру побудови комплексної системи захисту інформації на автоматизованих системах, що задіяні під час виконання військовими формуваннями завдань з оборони держави, з урахуванням їх маневреності, у частині надання можливості таким військовим формуванням здійснювати обробку секретної інформації у разі зміни їх місця дислокації.

7. Унормовано порядок визначення обізнаності у відомостях, що становлять державну таємницю, військовослужбовців, які зникли або потрапили в полон (оскільки розголошення довіреної таємниці військовослужбовцем, на якого здійснено супротивником психологічний чи фізичний тиск, може призвести до невиправних наслідків та вплинути на оперативно-тактичну обстановку у районах ведення (воєнних) бойових дій чи спеціальних операцій);

Таким чином, підсумовуючи зазначене вище, слід наголосити, що висвітлені основні новації до забезпечення режиму секретності в умовах ведення воєнних (бойових) дій та спеціальних операцій розроблено з урахуванням трендів сьогодення, а також набутого Службою безпеки України досвіду під час участі у антитерористичній операції на сході України.

**Література**

1. NOS/12(2014)0029 від 10 листопада 2014 року.

*УДК 35.078.3*

**Бондаренко І.Д.**
Національна академія СБ України

## НАПРЯМКИ УДОСКОНАЛЕННЯ КРИМІНАЛЬНОГО ЗАКОНОДАВСТВА У СФЕРІ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ

В Україні кримінальна відповідальність за умисну незаконну передачу сторонній особі державної таємниці передбачена ст. 328 КК України «Розголошення державної таємниці» та ст. 422 КК України «Розголошення відомостей військового характеру, що становлять державну таємницю, або втрата документів чи матеріалів, що містять такі відомості». Загальноприйнятим в юридичній науці є твердження, що суб'єкт зазначених злочинів є виключно спеціальним, ним є не будь-яка особа, а лише та, якій

відомості, що становлять державну таємницю, були довірені або стали відомі у зв'язку з виконанням службових обов'язків. Вважається, що «розголосити» може лише та особа, яка на законних підставах була обізнана з відповідною інформацією та на яку було покладено обов'язок її не розголошувати. Будь-яка інша стороння особа таких законодавчих обмежень не має, відповідних зобов'язань на себе не брала, на підставі чого аргументується, що вона і не може бути суб'єктом вищезазначених злочинів.

Але в дійсності трапляються випадки, коли незаконну передачу інформації з обмеженим доступом здійснює не спеціальний суб'єкт, а загальний. Особливого поширення набув збут та розповсюдження комп'ютерних баз даних державних органів, що містять службову інформацію, а також баз даних різних приватних організацій, що містять персональні дані. Для протидії такій діяльності в 2005 році КК України було доповнено ст. 361-2. Предметом даного злочину є інформація з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створена та захищена відповідно до чинного законодавства, а отже ним може охоплюватися й державна таємниця. Суб'єкт даного злочину є загальним, ним є будь-яка особа, а не лише та, якій відповідна інформація була довірена чи стала відома у зв'язку з виконанням службових обов'язків.

Маємо парадоксальну ситуацію: якщо стороння особа (загальний суб'єкт) попередньо заволодівши секретною інформацією передає її іншій сторонній особі, то таке діяння не вважатиметься розголошенням державної таємниці (ст. 328 КК України) оскільки відсутні ознаки спеціального суб'єкта, водночас вважатиметься злочином, передбаченим ст. 361-2 КК України, але лише у тому випадку, якщо відповідна інформація зберігалася в комп'ютерній формі та була захищена згідно вимог чинного законодавства. Очевидно, що форма інформації, комп'ютерна в даному випадку, не змінює саму суть діяння із її незаконної передачі та, відповідно, ступінь його суспільної небезпечності. Тому слід констатувати існування суттєвої законодавчої неузгодженості, однією із складових якої є неоднакова позиція законодавця щодо того, чи лише спеціальний суб'єкт має притягатися до відповідальності за діяння із незаконної передачі інформації з обмеженим доступом, зокрема такого її виду як державної таємниці.

Слід зазначити, що в мережі Інтернет функціонують ціла низка ресурсів, що використовуються як тіньові майданчики для незаконної купівлі продажу наркотиків, зброї та інформації з обмеженим доступом. Окрім баз персональних даних, наприклад, бази даних клієнтів «Нової пошти» чи «Приватбанку», на таких ресурсах періодично збувають й інформацію, яка може становити державну таємницю України. Кричущим прикладом є поява в 2017 році оголошень щодо збуту бази даних співробітників Служ-

би безпеки України. Чи створюють дії особи, яка умисно, чітко усвідомлюючи характер відповідних відомостей та факт їх обмеженості у доступі, збуває або навіть безкоштовно їх розміщує в публічному доступі? Очевидно, це неабияка загроза державній безпеці. Але з позиції кримінально-правової норми, передбаченої ст. 328 КК України, якщо продавець інформації не підпадає під ознаки спеціального суб'єкта, то склад злочину буде відсутній. Наприклад, в 2017 році резонансу набув випадок, коли видання «Українська правда» опублікувала матеріали про зрив державної програми реформування оборонно-промислового комплексу, що містили державну таємницю, але за чинним КК України відповідальні за підготовку статті журналісти не могли бути притягнуті до відповідальності, бо не є спеціальними суб'єктами в розумінні ст. 328 КК України.

Слід звернути увагу, що не лише кримінально-правова норма, передбачена ст. 361-2 КК України, не встановлює вимог для суб'єкта злочину щоб відповідні відомості, що становлять державну таємницю, були йому довірені або стали відомі у зв'язку з виконанням службових обов'язків. Суб'єктом злочину, передбаченого ст. 111 КК України «Державна зрада» (в формі шпигунства) хоч і є лише громадянин України, але будь-який. Даному злочину характерна спеціальна мета, передача інформації іноземній стороні, прямий умисел, чітке усвідомлення суб'єктом факту таємності відомостей.

Пропонується норму, передбачену ст. 361-2 КК України, розділити на декілька за ознакою предмета злочину, конкретного виду інформації з обмеженим доступом, доповнивши або вдосконаливши існуючі в інших розділах КК України кримінально-правові інструменти. Зокрема, передбачити відповідальність для загального суб'єкта за умисний збут або розміщення в публічному доступі відомостей, що становлять державну таємницю. Безперечно, така пропозиція є дискусійною. Але, по-перше, зважаючи на приклади ст. 361-2, 111, 114 КК України слід констатувати, що законодавець фактично вже застосовував такий підхід (щодо загального суб'єкта), а по-друге, незаконний збут чи поширення в публічному доступі державної таємниці може цілком справедливо бути порівняний із збутом наркотичних засобів або зброї, що є злочинним для будь-якої особи, а не лише певного спеціального суб'єкта.

*УДК 35.078:342.738*
**Ботвінкін О.В.**
аспірант відділу аспірантури і докторантури
Національна академія СБ України

# ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ СЕКРЕТНОЇ ІНФОРМАЦІЇ ОРГАНАМИ ДЕРЖБЕЗПЕКИ НА ТЕРИТОРІЇ УКРАЇНИ (друга половина XX століття)

Важливість виконання Службою безпеки України завдань із захисту економічного, науково-технічного і оборонного потенціалу України від розвідувально-підривної діяльності іноземних спеціальних служб, а також забезпечення охорони державної таємниці, вимагає всебічного і постійного вдосконалення діяльності органів і підрозділів СБ України. Сприяти цьому може, зокрема, і вивчення досвіду минулого. Так, на нашу думку, доцільно є дослідити практичні питання організації та діяльності спецслужби у такій сфері як захист секретної інформації, зокрема в період, коли були напрацьовані та удосконалені ті методи захисту секретної інформації, які можуть становити певний інтерес і для національної спецслужби (1950-ті – 1980-ті роки).

Зміни в характері розвідувальних спрямувань іноземних спецслужб та акцентів при застосуванні тих чи інших методів здобування секретної інформації викликали відповідні зміни в організації контррозвідувальними органами заходів протидії та вплинули на формування самої системи цих органів, яка змінювалась і вдосконалювалась відповідно до змін в оперативній обстановці. Структурні перебудови дозволяють виділити кілька етапів розвитку системи органів держбезпеки, задіяних у проведенні контррозвідувальної діяльності, спрямованої на захист секретної інформації.

*Перший етап* – 1954–1959 рр. Характеризувався відсутністю об'єднуючого та координуючого органу, відповідального за організацію контррозвідувального захисту державних секретів. На цьому етапі зазначені заходи здійснювались: 2 Головним управлінням (головний контррозвідувальний орган); 3 Головним управлінням (військова контррозвідка); 5 Управлінням (контррозвідувальна робота на особливо важливих державних об'єктах); 6 Управлінням (контррозвідувальна робота на транспорті); 1 спецвідділом (контррозвідувальна робота на об'єктах атомної промисловості); 4 спецвідділом (радіоконтррозвідка). В КДБ при РМ УРСР діяли органи та підрозділи аналогічні союзним, крім органів військової контррозвідки, які підпорядковувались КДБ при РМ СРСР.

*Другий етап* – 1959–1981 рр. Характерною є централізація контррозвідувальної діяльності (крім військової контррозвідки). На цьому етапі комплексність діяльності іноземних розвідок викликала перехід до ком-

плексної протидії під керівництвом єдиного контррозвідувального органу – 2 Головного управління КДБ при РМ СРСР. Посилення діяльності іноземних технічних розвідок підвищило роль радіоконтррозвідувальних підрозділів органів держбезпеки, що вилилось у відповідних змінах у структурі в середині 60-х років XX століття.

*Третій етап* – 1981–1991 рр. – етап організаційного та практичного посилення органів безпеки на об'єктах промисловості та науки. На цьому етапі захист економічного та наукового потенціалу було виділено в окрему ділянку роботи та внесено організаційні зміни в структуру контррозвідувальних органів КДБ (створено 6 Управління КДБ СРСР та відповідні республіканські управління). Причинами таких змін стали з одного боку підвищення у 80-х роках інтересу іноземних спецслужб до інформації економічного та наукового характеру, з іншого – проблема недостатньої оперативності прийняття рішень в умовах повної централізації контррозвідувальної діяльності. Остання причина призвела також до створення 4 Управління, з метою зосередження зусиль на організаційних та оперативних заходах, спрямованих на захист об'єктів транспорту й зв'язку.

На нашу думку, до сильних сторін системи контррозвідувальних органів у досліджуваний період можна віднести: 1) гнучкість – здатність адаптуватись до змін в оперативній обстановці, викликаній зміною пріоритетів розвідувальної діяльності іноземних спецслужб та новими завданнями протидії цій діяльності; 2) централізація – поступовий перехід від розрізнених дій окремих контррозвідувальних органів до об'єднаних спільним задумом скоординованих заходів низки органів держбезпеки; 3) дублювання – перетинання сфер контррозвідувального забезпечення кількох органів, яке іноді мало місце, в кінцевому рахунку лише посилювало надійність захисту секретної інформації; 4) необмеженість в ресурсах – сили та засоби, задіяні в заходах захисту інформації не співставлялись з розміром шкоди, яка могла бути завдана державі в разі витоку такої інформації. В умовах зовнішнього протистояння держава не жаліла коштів на захист власних секретів.

За роки незалежності система контррозвідувальних органів СБ України неодноразово реформувалась та удосконалювалась. З огляду на реалії сьогодення це застосування історичного досвіду в сьогоднішній практиці захисту інформації є можливим лише частково. Основним же повинен залишатись принцип, за яким будь яка загроза секретній інформації повинна бути вчасно виявленою та усунутою.

*УДК 681.3:34*
**Гоц О.В.**
старший викладач
Національна академія Служби безпеки України

# ПРОБЛЕМНІ АСПЕКТИ ЗАХИСТУ БАНКІВСЬКОЇ ТАЄМНИЦІ В УКРАЇНІ

Євроінтеграція України впливає на напрями і темпи розвитку банківської системи, де одним із найбільш суттєвих факторів є забезпечення належного захисту банківської таємниці, яка останнім часом має проблемні аспекти щодо її збереження банківськими установами під впливом зовнішніх і внутрішніх чинників.

Основними проблемними аспектами щодо захисту банківської таємниці в Україні є:

1. Шахрайство ( шахрайські дії невідомих осіб, що полягають у обманному вивідуванні інформації з банківської карти або банківської таємниці клієнтів банку шляхом СМС-повідомлень або дзвінків).

2. Процес ліквідації банку (під час якого послаблюється контроль з внутрішньою безпекою і створюються передумови для витоку банківської таємниці клієнтів банку).

3. «Законодавча суперечність» (може слугувати передумовою для не мотивованого розкриття банківської таємниці)[1].

Проаналізуємо проблемні аспекти захисту банківської інформації на предмет підтвердження виділених нами загроз. Так, найбільш значною загрозою нами назване шахрайство. Внаслідок протиправних дій з боку невідомих осіб, які представляються працівниками банку, ошукуються мешканці різних верств населення та регіонів України. Зокрема, злочинці обманним шляхом отримують кошти за допомогою СМС повідомлень або телефонних дзвінків. Випадки звернень громадян до частин поліції із заявами про телефонні дзвінки з боку осіб, що представлялись працівниками служби охорони банку і, зловживаючи довірою, випитували особисту банківську інформацію заявників, після чого у них з карток зникали гроші, трапляються щодня [2]. Причини цих подій: розкриття банківської таємниці, її розголошення довіреними особами невідомим шахраям.

Можливим рішенням проблеми з шахрайством, яка впливає на стан захисту банківської таємниці в цілому, вважаємо, може бути широка соціальна рекламна кампанія, спрямована на захист персональних даних, і активне інформування громадськості про основи забезпечення особистої фінансової безпеки. В Україні дана практика активно не застосовувалась, тому її введення дозволить захистити мешканців країни від шахрайських дій з боку злочинних організації, груп і осіб.

Іншим видом загрози для захисту банківської таємниці можна виділити загрозу, що пов'язана з процесом ліквідації банку. Так, фінансовий експерт Олексій Кущ зазначає: «головні ризики пов'язані з банками, які знаходяться в стадії ліквідації. При передачі документів у процесі ліквідації від діючих керівників тимчасовим адміністраторам є дуже багато вузьких місць, коли у фінансових установах послаблюються питання, пов'язані з внутрішньою безпекою, контролем над дотриманням інформаційного захисту. Крім того, коли працює тимчасова адміністрація, у банку вже немає ні технічних, ні фінансових, ні кадрових можливостей здійснювати повноцінний захист такої інформації. Також є питання, як ці дані потім архівуються і де вони зберігаються» [3]. Вважаємо, що така безвідповідальність вимагає змін на законодавчому рівні шляхом посилення контролю за процесом ліквідації банків.

Також серед основних системних загроз збереженню банківської таємниці в Україні можна виділити певну «законодавчу суперечність». У рамках розслідування фактів корупції чи відмивання злочинних коштів та фінансування тероризму Державна фіскальна служба, а також інші уповноважені державні органи мають доступ до банківської таємниці і тим самим до її розкриття. У цьому випадку банківська таємниця повинна бути розкрита за запитом органу державної виконавчої служби (за письмовою вимогою) для примусового виконання судових рішень зі стягнення коштів боржників з їх банківських рахунків. Проте, керуючись Законом України «Про банки і банкову діяльність» (ст. 61) банки мають певні зобов'язання щодо збереження банківської таємниці, зокрема, шляхом обмеження кола осіб, що мають доступ до відповідної інформації, застосування спеціальних технічних засобів, здатних запобігти несанкціонованому доступу до електронних та інших носіїв інформації [1].

Також Закон України «Про банки і банкову діяльність» зазначає, що «органи державної влади, юридичні та фізичні особи, які при виконанні своїх функцій, визначених законом, або наданні послуг банку безпосередньо чи опосередковано отримали в установленому законом порядку інформацію, яка містить банківську таємницю, зобов'язані забезпечити зберігання такої інформації, не розголошувати цю інформацію і не використовувати її на свою користь чи на користь третіх осіб» [8]. З цього приводу Міністерство юстиції України висловило свою правову позицію, що порядок надання інформації іншим компаніям, що існують сьогодні, порушує права громадян, що закріплені в ст. 32 Конституції України: не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини [4].

Слід зазначити, що фінансові установи мають право надавати інформацію, яка містить банківську таємницю, у випадках, передбачених чин-

ним законодавством (ст. 62 закону «Про банки і банківську діяльність» [8], а також «Правилами зберігання, захисту, використання та розкриття банківської таємниці», затверджених постановою НБУ № 267 від 14.07.2006» [5]).

Отже, наведені окремі проблемні аспекти у сфері захисту банківської таємниці в Україні дозволяють зробити висновок, що забезпечення належного захисту цієї інформації вимагає законодавчого удосконалення та адаптації до європейських стандартів, гармонізації законодавства України та наближення його до законодавства європейських країн.

**Література**

1. Про банки і банківську діяльність [Електронний ресурс]: Закон України від 7 грудня 2000 р. № 2121 – III (із змінами та доповненням від 15.11.2016 № 1736-VIII). – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2121-14.

2. Люди! Будьте пильними: шахрайство процвітає [Электронный ресурс]. – Режим доступа: https://novyny.online.ua/khmelnytskyi/292713845/lyudi-budte-pilnimi-shahraystvo-protsvitae.

3. Банківська таємниця в Україні: чому все дуже погано [Электронный ресурс]. – Режим доступа: http://povin.com.ua/19028-23-07.html.

4. Конституція України від 28 червня 1996 р. № 30 [Електронний ресурс] / Верховна Рада України. – Режим доступу : http://www.zakon.rada.gov.ua.

5. Правила зберігання, захисту, використання та розкриття банківської таємниці [Електронний ресурс]: Постанова від 14.07.2006№ 267 / Правління національного банку України. – Режим доступу : http://www.zakon.rada.gov.ua.

*УДК 342.1*

**Гуз А.М.**
доктор історичних наук, професор,
завідувач СК-32 ННІ ІБ НА СБ України

## ОКРЕМІ ПИТАННЯ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ В ЛАТВІЙСЬКІЙ РЕСПУБЛІЦІ

У 1996 році був прийнятий Закон Латвійської Республіки «Про державну таємницю». Стаття 2.1 цього Закону дала визначення поняття державної таємниці, як «відомості військового, політичного, економічного, наукового, технічного або іншого змісту, які внесені в затверджений кабінетом міністрів перелік, і втрата чи незаконне розголошення яких може нанести збиток безпеці та економічним або політичним інтересам держави». Поняття державної таємниці у 2005 році було доповнено пунктом 4 про статус державної таємниці. Законодавством передбачено ступені сек-

ретності відомостей, які складають державну таємниці (ст.3), а також які саме відомості відносяться до того чи іншого ступеню. Звертають увагу положення законодавства Латвійської Республіки, які регулюють питання засекречування. Відомості, які складають державну таємницю, засекречуються під грифом «таємно» – на 5 років, під грифом «цілком таємно» – на 10 років, під грифом «особливої важливості» – на 20 років. Відомості про осіб, які займаються оперативно-розшуковою діяльністю, і осіб, які підпадають під дії спеціального процесуального захисту, засекречуються терміном на 75 років.

Охорона державної таємниці у Латвійській Республіці здійснюється на підставі ст. 7 Закону і полягає в цілеспрямованій діяльності з правового, технічного і організаційного характеру, яка здійснюється компетентними державними органами і їх посадовими особами з метою забезпечення збереження відомостей, які складають державну таємницю, і попередження їх незаконному поширенню.

Доступ до відомостей, які складають державну таємницю надається тільки тим особам, які згідно з посадовими обов'язками або конкретним службовим завданням повинні виконувати роботу, пов'язану з використанням чи захистом відомостей, які складають державну таємницю і, які мають допуск до державної таємниці. До початку трудових відносин з особами, яким буде надано допуск до держаної таємниці проводять комплекс заходів з перевірки.

Допуск до відомостей, які складають державну таємницю надається дієздатним громадянам Латвії з 18 років за умови, якщо особа підписала зобов'язання про нерозголошення, в якому вона зобов'язується зберігати і не розголошувати відомості, які складають держану таємницю і дало згоду на проведення органами державної безпеки перевірки відносно себе.

Організацію захисту державної таємниці Латвійської Республіки покладено на: Кабінет Міністрів, Бюро із захисту Конституції, Службу військової контррозвідки та Службу безпеки. Кожен орган має свої компетенції у цій сфері. За дотримання режиму секретності і забезпечення захисту державної таємниці в державних органах відповідає керівник органу або відповідний структурний підрозділ.

Відповідальність за розголошення державної таємниці регулюється на підставі статті 94 Кримінального закону Латвійської Республіки.

Усі органи місцевого самоврядування, а також юридичні і фізичні особи в розпорядженні яких знаходяться інформаційні системи, які здійснюють обробку чи збереження відомостей, які складають державну таємницю, зобов'язані зареєструвати їх в Бюро із захисту Конституції і одержати акредитаційний сертифікат, який підтверджує відповідність системи вимогам безпеки.

Варто зазначити, що правову основу охорони державної таємниці в Латвійської Республіки складають Закони: «Про державну таємницю»,

«Про свободу інформації, «Про захист персональних даних», постанова Кабінету Міністрів Латвійської Республіки Перелік відомостей які відносяться до державної таємниці.

У 2004 році Латвія вступила до ЄС та НАТО й почала приводити законодавство до стандартів цих структур.

Станом на липень 2017 року Урядом України підписано 51 угоду про взаємну охорону секретної інформації. Така угода з Латвійською Республікою була підписана у листопаді 2003 року, ратифіковано у жовтні 2004 року, набрала чинність з листопада 2004 року.

*УДК 658.586*

**Жевелєва І.С.**
Національна академія СБ України

## ПЕРСПЕКТИВИ ВЗАЄМОДІЇ ДЕРЖАВНОГО І НЕДЕРЖАВНОГО СЕКТОРІВ БЕЗПЕКИ У ПРОЦЕСІ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

У наш час роль недержавного сектору безпеки у забезпеченні інформаційної безпеки держави неухильно зростає, проте наявні правові та організаційні засоби функціонування недержавних служб безпеки в Україні, відсутність чіткої взаємодії їх з правоохоронними органами – не дозволяють в повній мірі реалізувати їх значний потенціал для сприяння державним суб'єктам із забезпечення національної та інформаційної безпеки України.

Погоджуємось із Чистоклетовим Л.Г., який вважає, що основними принципами взаємодії правоохоронних органів із суб'єктами господарювання у сфері захисту інформації з обмеженим доступом повинні бути:

- взаємна відповідальність держави і недержавних організацій за дії, що завдають збитків національним інтересам;
- захист державою законних інтересів у відповідних сферах господарської діяльності;
- надання пріоритетної допомоги недержавним організаціям, що безпосередньо беруть участь в забезпеченні економічної безпеки і незалежності країни;
- повага й дотримання прав і свобод людини і громадянина [1, с. 487].

Разом з цим необхідно чітко визначити ті напрями взаємодії у сфері забезпечення безпеки підприємств, де обопільно правоохоронні органи і недержавні служби безпеки мають певний інтерес.

Взаємодія державного і недержавного секторів безпеки у сфері захисту інформації з обмеженим доступом може здійснюватися за такими *напрямами:*

– кадровий – перевірка правоохоронними органами кандидатів на роботу до недержавних служб безпеки, повідомлення підприємців про порушення конкретними особами законодавства України або притягнення їх до кримінальної відповідальності, участь правоохоронних органів у підготовці працівників для недержавних служб безпеки тощо;

– інформаційний – взаємний обмін інформацією про спроби та способи вчинення протиправних дій, потенційно небезпечних осіб, осіб, що перебувають у розшуку, проведення спільних семінарів, конференцій, навчань тощо;

– організаційна взаємодія – створення системи спільної протидії незаконній діяльності з боку фізичних та юридичних осіб (організація охорони, встановлення сигналізації, системи швидкого оповіщення правоохоронних органів).

Одним з перспективних напрямів взаємодії служб безпеки підприємств і правоохоронних органів є укладення відповідних угод. На сьогодні цей напрям діяльності гальмується розрізненістю і відокремленістю приватних охоронних структур, а також відсутністю Закону «Про приватну детективну діяльність». В даному напрямі доцільно чітко розмежовувати компетенцію правоохоронних органів і служб безпеки підприємств.

Недержавні служби безпеки досить ефективно можуть доповнювати державну правоохоронну систему. Вони надають допомогу правоохоронним органам за наступними напрямками:

– прийняття на себе зобов'язання щодо забезпечення режиму секретності та захисту інформації з обмеженим доступом на території, охоронюваної на договірній основі з юридичною особою або органами виконавчої влади, об'єктах економіки, соціальної інфраструктури, територіях, об'єктах муніципальної власності;

– інформування правоохоронних органів про вчинені і підготовлювані злочини, сприяння у затриманні осіб, підозрюваних у скоєнні злочинів, розшукуваних злочинців, а також розшуку безвісти зниклих осіб, втраченого майна і грошових коштів;

– сприяння державним органам у виконанні ними своїх завдань при проведенні оперативних та слідчих заходів (збереження слідів злочину, виявлення очевидців, участь в якості понятих), при надзвичайних обставинах (в якості допоміжних сил для оточення і т.п.);

– участь у проведенні профілактичних заходів (читання лекцій населенню, організація дитячих та юнацьких шкіл, секцій, надання послуг по правовому консультуванню);

– сприяння у проведенні експертної оцінки підготовлених нормативних актів, що регламентують питання інформаційної безпеки [2, с. 178].

Резюмуючи, зазначимо, що взаємодія державного і недержавного секторів безпеки умовах сьогодення стає необхідним напрямком здійснення

діяльності по забезпеченню національної безпеки держави. Зважаючи на це, необхідність розроблення правових та організаційних засад такої взаємодії у процесі захисту інформації з обмеженим доступом є нагальним та актуальним завданням.

**Література**

1. Чистоклетов Л. Г. Формування адміністративно - правового забезпечення безпеки діяльності суб'єктів господарювання в Україні : моногр. / Л.Г.Чистоклетов. – Львів, 2013. – 556 с.

2. Сачаво А.Г. Взаємодія державних правоохоронних органів та недержавних охоронних структур у забезпеченні правопорядку в Україні / А. Г. Сачаво // Науковий вісник Національної академії внутрішніх справ України. – 2003. – № 5. – С. 176-180.

*УДК 681.3.07*

**Жердєв М.К.**
доктор технічних наук, професор
Військовий інститут телекомунікацій
та інформатизації імені Герої Крут
**Пампуха І.В.**
кандидат технічних наук, доцент
Військовий інституту Київського національного
університету імені Тараса Шевченка
**Пусан В.В.**
Військовий інституту Київського національного
університету імені Тараса Шевченка

## МОБІЛЬНІ ПРИСТРОЇ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ЦИФРОВОЇ ІНФОРМАЦІЇ

Проблема захисту інформації шляхом її перетворення, що виключає її прочитання сторонньою особою, хвилювала людський розум з давніх часів. Історія криптографії - ровесниця історії людської мови. Більш того, спочатку писемність сама по собі була криптографічного системою, так як в древніх суспільствах нею володіли лише обрані.

Розробка та впровадження мобільних пристроїв криптографічного перетворення цифрової інформації, які б використовували для передачі даних загальні мережі має велике значення. По-перше, з точки зору економічної доцільності, що не потребує окремих виділених ліній та технічних засобів. По-друге, гнучкість застосування в залежності від обстановки і наявності загальних мереж для передачі даних. По-третє, оперативність обміну інформацією між споживачами (абонентами). По-четверте, не по-

требується задіяння системи генерації та розподілу ключів між споживачами. На сьогодення ця проблема є актуальною, як елемента системи охорони державної таємниці та службової інформації України з урахуванням досвіду проведення АТО.

Авторами розроблено алгоритм БА-05 (в подальшому за текстом - алгоритм) - блоковий, симетричний алгоритм призначений для апаратної, програмної або програмно-апаратної реалізації, який задовольняє криптографічним вимогам і за своїми параметрами надає можливість для конфіденційної захисту інформації, яка захищається. Блок даних, який обробляється, становить 128 біт. При цьому алгоритм можна досить легко модифікувати для обробки даних розмірностей 128, 256, і т.д. біт. Довжина блоку даних на швидкість обробки істотно не впливає (при кожному збільшенні довжини блоку даних на 128 біт, швидкість обробки зменшується на 3%).

В основу розробленого алгоритму БА-05 покладена ідея Вернама, в якій він запропонував відмовитися від детермінованих ключів і випадковим чином їх генерувати, при цьому їх довжина повинна бути дорівнює довжині повідомлення. Така схема отримала назву стрічки одноразового використання (або схеми з одноразовим блокнотом). Вернама і Шенноном доведено, що в цьому випадку зашифрована інформація «злому» не піддається.

Складність практичного застосування цього алгоритму полягає в тому, що і відправник і одержувач повинні мати один і той же випадковий ключ. Тому, незважаючи на переваги способу Вернама перед іншими способами, виконаними на електронних пристроях, на практиці його реалізувати складно і дуже дорого. Основною трудністю є те, що генератори випадкових чисел на передавальної і приймальні сторонах повинні працювати синхронно і синфазно.

У пропонованому алгоритмі вдалося забезпечити синхронну і синфазну роботу випадкових генераторів на передавальної і приймальні сторонах, при цьому відправник і одержувач мають один і той же випадковий ключ. Тобто, реалізована схема Вернама. В алгоритмі використовуються симетричні випадкові і особисті ключі. Крім зашифрования (розшифрування) інформації БА-05 дозволяє вирішити ряд додаткових завдань:

1. За рахунок використання індивідуальних випадкових ключів цифровий підпис і аутентифікацію.

2. За рахунок автоматичного формування хеш-функції в процесі шифрування (розшифрування) інформації:

а) досягнення цілісності і високу вірогідність інформації (до одного біта) в системі в процесі обміну, так як здійснюється автоматичний контроль в процесі обміну між абонентами за допомогою хеш-функції (при зміні хоча б одного біта інформації в посилці призведе до зміни виду хеш-

функції з ймовірністю, де $n$ - розмірність блоку інформації, що обробляється становить 128 біт. Для нашого випадку $P \approx 1$);

б) виключений людський фактор розголошення ключів (так як вони автоматично формуються випадковими генераторами алгоритму в процесі шифрування (розшифрування) інформації і змінюються вони з кожним блоком, що додатково дозволяє скоротити сили і засоби, які виділяються в інших алгоритмах захисту інформації);

в) високий рівень захисту від несанкціонованого доступу в термінали хакерів, вірусів та ін.;

г) досягається високий ступінь криптографічного захисту інформації з еквівалентної довжиною ключа на один блок інформації.

В умовах сучасного розвитку інформаційних технологій, створення розподілених інформаційних систем стало об'єктивною реальністю. Необхідність забезпечення безпеки інформаційних ресурсів таких систем не викликає сумніву. При цьому ринок засобів захисту настільки великий, що забезпечує найрізноманітніший вибір при побудові систем захисту інформації та електронного підпису.

**Література**

1. Столинг Вильям Криптография и защита сетей: принципы и практика, 2-е изд.; пер. с англ. – М.: Издательский дом «Вильямс», 2001. – 672 с.

2. Атаки спеціального виду на криптопристрої та методи боротьби з ними; за наук. ред. д.т.н., проф. В.П. Широчина. – Кременець: Видавничий центр КОГПІ, 2009. – 264 с.

*УДК 342.1:35.083.8*

**Князєв С.О.**
кандидат юридичних наук,
старший науковий співробітник
Національна академія СБ України

## ВИЗНАЧЕННЯ МОЖЛИВИХ ШЛЯХІВ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ДІЯЛЬНОСТІ ПРАЦІВНИКІВ РЕЖИМНО-СЕКРЕТНИХ ОРГАНІВ

Відповідно до Закону України «Про державну таємницю» режимно-секретний орган (далі – РСО) визначається, як важливий, окремий структурний підрозділ в державних органах, органах місцевого самоврядування на підприємствах, установах чи організаціях, діяльність яких пов'язана з державною таємницею (далі - установи). До повноважень даного підрозділу відноситься розроблення та здійснення заходів щодо забезпечення ре-

жиму секретності та постійний контроль за його додержанням. При цьому ефективність діяльності РСО в повній мірі залежить від дій працівників, які безпосередньо працюють в цьому підрозділі.

Саме працівників РСО окремі науковці називають першим, захисним бар'єром щодо охорони державної таємниці в країні. Разом з тим, цей бар'єр іноді виявляється достатньо вразливим.

Сучасні підходи до вивчення впливу людського фактору в різних сферах діяльності досить часто ґрунтуються на двох ключових критеріях: надійність особи та компетентність особи. Зважаючи на ці два критерії проаналізуємо правове регулювання професійно-кваліфікаційних вимог до працівників РСО.

Закон України «Про державну таємницю» у статті 21 визначає, що РСО комплектуються спеціалістами, яким надано допуск до державної таємниці із ступенем секретності відповідно до діяльності пов'язаної із державною таємницею, що провадить установа. Таким чином, важливою умовою комплектування кадрами РСО є оформлення допуску, що включає спеціальну процедуру перевірки громадянина України у зв'язку із допуском до державної таємниці.

Отже, спеціальна перевірка на допуск до державної таємниці кандидатів на роботу в РСО фактично стає підтвердженням їх можливої надійності для даної сфери. Звідти, надійність працівників РСО, у контексті такої перевірки на допуск до державної таємниці, спрямована на підтвердження дієздатності особи, вивчення його психічного стану та виявлення можливої протиправної діяльності у теперішній час та у минулому, що може вплинути на подальшу ефективність охорони державної таємниці.

Періодичне переоформлення допуску повинно сприяти здійсненню контролю за надійністю вже прийнятого на роботу працівника РСО установи.

Слід зазначити, що стандартна, спеціальна перевірка громадян у зв'язку із допуском до державної таємниці перш за все спрямована на виявлення обставин, передбачених Законом України «Про державну таємницю» і при наявності яких допуск до державної таємниці не буде наданий. Звідти чинники на кшталт моральних якостей, конфліктності, стресостійкості, прагнення до саморозвитку, патріотизм (охороняти доведеться державну таємницю і, іноді в особливих умовах) враховуватись не будуть.

У цьому зв'язку, варто зазначити, що для даної категорії осіб, зважаючи на особливу важливість діяльності працівників РСО для сфери охорони державної таємниці, є необхідність реалізовувати більш поглиблену перевірку та вивчення як за терміном її проведення, так і за кількістю питань необхідних для опрацювання.

Наступним важливим критерієм відбору кандидатів на посаду в РСО є їх компетентність, що досить часто співвідноситься із наявністю необхід-

них знань та умінь. На теперішній час, загальні завдання та права працівників РСО, без можливого розподілу за посадами, визначені у 21 статті Закону України «Про державну таємницю».

Проте, ще донедавна у сфері охорони державної таємниці діяв Довідник типових професійно-кваліфікаційних характеристик основних посад керівників та інших працівників РСО установ. Даний документ містив детальний опис різних посад РСО та активно використовувався під час підготовки як посадових інструкцій, так і формуванні номенклатури посад в установах.

Підсумовуючи, можливо дійти висновку, що зважаючи на можливі негативні наслідки від неефективної діяльності працівників РСО для сфери охорони державної таємниці, певні питання пов'язані із правовим забезпечення професійно-кваліфікаційних характеристик працівників РСО потребують додаткового вирішення.

Зокрема, формування та введення в дію нового Довідника професійно-кваліфікаційних характеристик працівників РСО. Такий довідник повинен розмежувати за різними посадами РСО: кваліфікаційні вимоги (освіта, стаж роботи тощо); знання і уміння; повноваження (права, обов'язки тощо). Містити рекомендації щодо закріплення персональної відповідальності за збереження секретних відомостей тощо.

Зважаючи на динамічні процеси в інформаційній сфері, появу нових загроз існуванню державної таємниці, оновлення нормативно-правових актів, варто передбачити у законодавстві обов'язковість подальшого періодичного підвищення кваліфікації різних категорій працівників РСО (керівники, діловоди тощо), а також працівників РСО із різним досвідом роботи.

Крім того, потребують додаткового вивчення правові підстави, щодо можливості збільшення переліку питань перевірки кандидатів на різні посади в РСО стосовно врахування: моральних якостей, конфліктності, стресостійкості, патріотизму тощо.

*УДК 338.482.224*

**Козлова А.О.**
кандидат економічних наук,
старший викладач
Харківський національний університет
міського господарства імені О.М.Бекетова

## АКТУАЛЬНІ ПИТАННЯ ЗАПОБІГАННЯ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ, ЩО ЦИРКУЛЮЄ В ІНФОРМАЦІЙНИХ РЕСУРСАХ ТУРИСТИЧНИХ ПІДПРИЄМСТВ

Незважаючи на лібералізацію певних візових процесів та збільшення кількості громадян, які самостійно організовують туристичні подорожі за

межі України, існує значна кількість осіб, які користуються послугами які надаються туристичними агентами та операторами. Це обумовлено декількома факторами, основними з яких є неможливість самостійно замовити квітки на чартерні авіарейси, обмежена кількість місць в готелях, особливо у «високий сезон» через їх бронювання крупними туроператорами, бажання отримати комплексну послугу, менталітет та звички певної ланки суспільства і т. ін. Туристичні агенції безпосередньо працюють з туристичними операторами, авіакомпаніями, страховими компаніями, спортивними, культурними, освітніми закладами в різних країнах світу через Інтернет. А обробка інформації здійснюється саме за допомогою інформаційних автоматизованих систем [2, с. 1].

Для отримання бажаного туру потенційному туристу необхідно надати туристичному підприємству документи, які містять інформацію, що підпадає під поняття інформацію з обмеженим доступом, а саме: оригінали та копії їх закордонних паспортів (у разі подорожі за кордон та оформлення авіаквитків), загальнодержавних посвідчень особи (у разі подорожі у межах держави), тобто надати інформацію про персональні дані. Крім того, надається інформація, що містить банківську таємницю (банківські картки для безготівкових розрахунків або чеки) у разі оформлення віз до країн відвідування, іншу інформацію про особистість, що стосується, наприклад, неповнолітніх і т. ін.

Такого роду інформація потім використовується не тільки туристичною агенцією, до якої звернулася особа, а й стає доступною для туристичних операторів, авіакомпаній, страхових установ, інших систем та вищезгаданих структур. Тобто вже виходить з-під контролю її власника, який навіть не уявляє масштабів її циркуляції в інформаційних мережах, доречи не завжди захищених від несанкціонованого доступу. Наприклад, AMADEUS - провідна глобальна розподільна система, що забезпечує в режимі реального часу доступ до ресурсів провайдерів туристичних послуг (авіакомпаній, готелів, компаній по прокату автомобілів, страхових компаній і т.д.) 139 країн світу. Система Amadeus надає доступ до ресурсів 513 авіакомпаній, що складає більше 95% світового ринку регулярних пасажирських авіаперевезень, а також 52 731 готелів, 46 компаній по прокату автомобілів і дозволяє працювати з продуктами туроператорів, залізницями, круїзними і страховими компаніями.

З одного боку це передбачено специфікою їх діяльності, наприклад неможливо замовити авіаквитки на авіарейси інкогніто, забронювати номери в готелях без паспортних даних, з іншого боку існує реальна можливість використання інформації про особу, інформації з обмеженим доступом про її фінансовий стан з боку сторонніх структур. Так, доступ до такого роду інформаційних масивів можуть мати не тільки державні органи влади та управління, спецслужби, правоохоронні органи, а й злочинні

угрупування. Додаткових проблем такого роду додають країни досить привабливі у туристичному відношенні, але зі складною криміногенною обстановкою, високими корупційними ризиками, що може сприяти витоку персональних даних та іншої конфіденційної інформації до кримінальних угрупувань, терористичних організацій тощо. В результаті існують реальні передумови для використання персональних даних туристів, банківської таємниці та іншої інформації з обмеженим доступом у шахрайських цілях, спроб викрадення осіб з метою отримання викупу, або їх банального шантажу.

Повністю уникнути вказаних негативних чинників під час глобальної «прозорості» інформаційних ресурсів неможливо, але для мінімізації негативних наслідків доцільно дотримуватися вже напрацьованих рекомендацій, які доступні при бажанні майже кожному. Основними з них є: дотримання заходів безпеки як на стадії оформлення турпоїздки в туристичній агенції так і в процесі подорожі чи перебування за межами країни. Наприклад: вимагати при укладанні угоди на надання туристичних послуг дотримання вимог щодо захисту персональних даних. Дотримуватися вимог щодо безпечного зберігання банківських документів (карток), не залишати документи без догляду чи в місцях необлаштованих засобами зберігання, не користуватися без нагальної потреби комп'ютерними пристроями, незахищеними інформаційними мережами для передачі інформації з обмеженим доступом, вимагати документального оформлення послуг тощо.

З метою підвищення рівня туристичного обслуговування, сприяння споживачам у свідомому виборі туристичних послуг у туристичних закладах нашої країни [1, с. 1], було б доцільним активізувати методологічну, профілактичну роботу та посилити контроль з боку компетентних державних органів щодо використання в туристичних закладах ліцензійного програмного продукту, впровадження систем захисту для комп'ютерних мереж. Вимагати та ретельно контролювати дотримання вимог щодо діючого порядку оформлення документації, яка містить інформацію з обмеженим доступом, її умови зберігання та передачі, насамперед в інформаційних автоматизованих системах.

**Література**

1. Про туризм : Закон України від 15 вересня 1995 р. № 325/95-ВР // Відомості Верховної Ради України. – 1995. – № 31.

2. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07. 1994 р. № 80/94-ВР // Відомості Верховної Ради України. – 1994. – № 31.

*УДК 004.056.5*
**Корченко О.Г.**
доктор технічних наук, професор
Національна академія СБ України
**Дрейс Ю.О.**
кандидат технічних наук, доцент
Національний авіаційний університет
**Романенко О.О.**
Національний авіаційний університет

# ФОРМУВАННЯ МНОЖИНИ ПАРАМЕТРІВ ОЦІНЮВАННЯ НАСЛІДКІВ ВИТОКУ ДЕРЖАВНОЇ ТАЄМНИЦІ ВІД КІБЕРАТАК НА КРИТИЧНУ ІНФОРМАЦІЙНУ ІНФРАСТРУКТУРУ ДЕРЖАВИ

З огляду на наявність в державі тимчасово окупованих територій та районів проведення антитерористичної операції, гостро постає питання щодо необхідності забезпечення захисту державних інформаційних ресурсів на об'єктах критичної інфраструктури (ОКІ), які є важливими для забезпечення національної безпеки України від терористичних загроз. Наразі основним завданням політики національної безпеки є захист державного суверенітету України, її територіальної цілісності, недоторканості державного кордону, що базується на принципі своєчасності й адекватності заходів захисту національних інтересів реальним і потенційним загрозам. В інформаційній сфері до таких загроз належить розголошення інформації, яка становить державну таємницю (ДТ), або іншої інформації з обмеженим доступом, спрямованої на задоволення потреб і забезпечення захисту національних інтересів суспільства і держави. Тому оцінювання негативних наслідків (шкоди) витоку державної таємниці від кібератак на інформаційно-телекомунікаційні системи (ІТС) ОКІ є актуальним завданням.

Розроблено модель представлення параметрів шкоди у вигляді кортежу, при $m$ = 14 визначимо як [1-5]:

$$\mathbf{IDN} = < \mathbf{IDN_1}, \mathbf{IDN_2}, \mathbf{IDN_3}, \mathbf{IDN_4}, \mathbf{IDN_5}, \mathbf{IDN_6}, \mathbf{IDN_7}, \mathbf{IDN_8}, \mathbf{IDN_9}, \mathbf{IDN_{10}}, \mathbf{IDN_{12}}, \mathbf{IDN_{13}}, \mathbf{IDN_{14}} > =$$
$$< \mathbf{U}, \mathbf{N}, \mathbf{E}, \mathbf{A}, \mathbf{D}, \mathbf{DS}, \mathbf{T}, \mathbf{CS}, \mathbf{CW}, \mathbf{L}, \mathbf{P}, \mathbf{CA}, \mathbf{TD}, \mathbf{LCT} >,$$

де $\mathbf{IDN_i} \subseteq \mathbf{IDN}$ $(i = \overline{1,m})$ – компонент кортежу, що відображає $i$-й ідентифікатор об'єкта, $m$ їх кількість, а для всіх членів **IDN** характерна властивість порядку: 1) **U** – множина ідентифікаторів адміністративно-територіальних одиниць України, в межах якої знаходиться ОКІ – суб'єкт режимно-секретної діяльності (СРСД) і відображається як [1]: $\mathbf{U} = \{\bigcup_{i=1}^{m_1} U_i\} = \{U_1, ..., U_{m_1}\}$, де $U_i \subseteq \mathbf{U}$ $(i = \overline{1,m_1})$ – ідентифікатор адміністративно-територіальної одиниці, а $m_1$ їх кількість ($m_1 = 27$); 2) **N** – множина назв або/та унікальних ідентифікаційних номерів юридичної особи в Єдиному

державному реєстрі підприємств та організацій України (ЄДРПОУ) організацій-власників / розпорядників ІТС як об'єкта критичної інформаційної інфраструктури, визначається виразом [1]: $\mathbf{N} = \{\bigcup_{i=1}^{m_2} N_i\} = \{N_1, \ldots, N_{m_2}\}$, де $N_i \subseteq \mathbf{N}$ $(i = \overline{1, m_2})$ – *i*-та назва СРСД та/або номер ЄДРПОУ організації (підприємства, установи), а $m_2$ їх кількість; 3) **E** – множина подій (порушень), які стали обставиною для оцінювання наслідків (шкоди), набуде вигляду [2]: $\mathbf{E} = \{\bigcup_{i=1}^{m_3} E_i\} = \{E_1, \ldots, E_{m_3}\}$, де $E_i \subseteq \mathbf{E}$ $(i = \overline{1, m_3})$ – *i*-та подія, а $m_3$ їх кількість $(m_3 = 2)$; 4) **A** – множина атак (подія-загроза), що призвела до появи ***E***, визначимо як [2]: $\mathbf{A} = \{\bigcup_{i=1}^{m_4} A_i\} = \{A_1, \ldots, A_{m_4}\}$, де $A_i \subseteq \mathbf{A}$ $(i = \overline{1, m_4})$ – *i*-та атака, а $m_4$ їх кількість; 5) **D** – множина відомостей, що становлять ДТ у вигляді номера статті ЗВДТ та їх ступінь секретності (СС) щодо яких відбулася подія **E**, сформуємо як [2]:

$$\mathbf{D} = \{\bigcup_{i=1}^{m_5} \mathbf{D_i}\} = \{\bigcup_{i=1}^{m_5} \{\bigcup_{j=1}^{m_{5i}} \{\bigcup_{k=1}^{m_{5ij}} D_{ijk}\}\}\} = \{D_{1.1.1}, D_{1.1.2}, \ldots, D_{1.1.m_{51}}\}, \{D_{1.2.1}, D_{1.2.2}, \ldots, D_{1.2.m_{52}}\}, \ldots$$

$$\{D_{m_5.1.1}, D_{m_5 1.2}, \ldots, D_{m_5.m_{5m_5 i}.m_{5m_5 ij}}\}, (i = \overline{1, m_5},\ j = \overline{1, m_{5i}}, k = \overline{1, m_{5ij}});$$

6) **DS** – множина СС відомостей ***D***, набуде наступного виду [2]: $\mathbf{DS} = \{\bigcup_{i=1}^{m_6} DS_i\} = \{DS_1, \ldots, DS_{m_6}\}$, де $DS_i \subseteq \mathbf{DS}$ $(i = \overline{1, m_6})$ – *i*-та СС відомостей ***D***, а $m_6$ їх кількість $(m_6 = 3)$; 7) **T** – множина завдань з охорони ДТ (ОДТ) як комплекс *k* заходів (способів) з нейтралізації визначеного переліку можливих атак **A**, визначається виразом [2]: $\mathbf{T} = \{\bigcup_{i=1}^{m_7} T_i\} = \{T_1, \ldots, T_{m_7}\}$, де $T_i \subseteq \mathbf{T}$ $(i = \overline{1, m_7})$ – *i*-те завдання, а $m_7$ їх кількість; 8) **CS** – множина значень коефіцієнту захищеності інформації в СРСД, відображається як [2]: $\mathbf{CS} = \{\bigcup_{i=1}^{m_8} CS_i\} = \{CS_1, \ldots, CS_{m_8}\}$, де $CS_i \subseteq \mathbf{CS}$ $(i = \overline{1, m_8})$ – *i*-те значення коефіцієнту захищеності інформації, а $m_8$ їх кількість $(m_8 = m_2)$; 9) **SW** – множина значень питомої ваги об'єкта відомостей **D**, набуде вигляду [2]: $\mathbf{SW} = \{\bigcup_{i=1}^{m_9} SW_i\} = \{SW_1, \ldots, SW_{m_9}\}$, де $SW_i \subseteq \mathbf{SW}$ $(i = \overline{1, m_9})$ – *i*-те значення питомої ваги об'єкта відомостей ***D***, а $m_9$ їх кількість; 10) **L** – множина показників рівня зниження ефективності складової частини об'єкта (СЧО) відомостей ***D***, представимо виразом [2]: $\mathbf{L} = \{\bigcup_{i=1}^{m_{10}} L_i\} = \{L_1, \ldots, L_{m_{10}}\}$, де $L_i \subseteq \mathbf{L}$ $(i = \overline{1, m_{10}})$ – *i*-те значення рівня зниження ефективності СЧО відомостей ***D***, а $m_{10}$ їх кількість; 11) **P** – множина значень відносної вартості СЧО відомостей ***D***, визначається як [2]: $\mathbf{P} = \{\bigcup_{i=1}^{m_{11}} P_i\} = \{P_1, \ldots, P_{m_{11}}\}$, де $P_i \subseteq \mathbf{P}$ $(i = \overline{1, m_{11}})$ – *i*-та відносна вартість СЧО, а $m_{11}$ їх кількість; 12) **CA** – множина значень коефіцієнту морального старіння відомостей ***D***, набуде виду [2]: $\mathbf{CA} = \{\bigcup_{i=1}^{m_{12}} CA_i\} = \{CA_1, \ldots, CA_{m_{12}}\}$, де $CA_i \subseteq \mathbf{CA}$ $(i = \overline{1, m_{12}})$ – *i*-те значення коефіцієнту морального старіння відомостей ***D***, а $m_{12}$ їх кількість $(m_{12} = m_5)$; 13) **TD** – множина показників сукупної шкоди, визначається виразом [2]: $\mathbf{TD} = \{\bigcup_{i=1}^{m_{13}} TD_i\} = \{TD_1, \ldots, TD_{m_{13}}\}$, де

$TD_i \subseteq \mathbf{TD}\ (i = \overline{1, m_{13}})$ – $i$-тий показник сукупної шкоди, а $m_{13}$ їх кількість; 14) **LCT** – множина ідентифікаторів рівня класифікації терористичних загроз, має вигляд [3]: $\mathbf{LCT} = \{\bigcup_{i=1}^{m_{14}} LCT_i\} = \{LCT_1, ..., LCT_{m_{14}}\}$, де $LCT_i \subseteq \mathbf{LCT}\ (i = \overline{1, m_{14}})$ – $i$-тий ідентифікатор рівня терористичної загрози, а $m_{14}$ їх кількість ($m_{14} = 4$).

У даному дослідженні запропоновано кортежну модель представлення базових параметрів оцінювання негативних наслідків витоку ДТ від кібератак на критичну інформаційну інфраструктуру держави.

**Література**


1. О. Корченко, Ю. Дрейс, О. Романенко, "Формування множини ідентифікаторів для класифікації об'єктів критичної інформаційної інфраструктури", Актуальні проблеми забезпечення кібербезпеки та захисту інформації: тези доповідей учасників IV Міжнародної науково-практичної конференції 21-24 лютого 2018 р. – К.: Вид-во Європейський університет, 2018. – С.81-86.

2. Корченко О., Архипов О., Дрейс Ю. "Оцінювання шкоди національній безпеці України у разі витоку державної таємниці : монографія, К.: Наук.-вид. центр НА СБ України, 332 с., 2014, ISBN 978-617-7092-26-0.

3. Корченко О., Дрейс Ю. "Додаткові критерії оцінювання шкоди, нанесеної розголошенням державної таємниці або втрати матеріальних носіїв секретної інформації за рівнем класифікації терористичних загроз", Актуальні проблеми забезпечення кібербезпеки та захисту інформації: тези доповідей учасників II Міжнародної науково-практичної конференції, 24-27 лютого 2016 р. – К: Вид-во Європейський університет, 2016. – С. 90-91.

4. Дрейс Ю. "Аналіз базової термінології і негативних наслідків кібератак на інформаційно-телекомунікаційні системи об'єктів критичної інфраструктури держави", Захист інформації. – 2017. – Т. 19. – № 3. – С. 214-222.

5. Корченко О., Дрейс Ю., Романенко О. "Критична інформаційна інфраструктура України: терміни, сектори і наслідки", Захист інформації. – 2017. – Т. 19. – № 4. – С. 303-309.



*УДК 342.1:355/359*



**Лебедєв О.Р.**
кандидат юридичних наук, доцент
Національна академія СБ України


## ЗАБЕЗПЕЧЕННЯ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ У ВІЙСЬКОВИХ УМОВАХ У КОНТЕКСТІ БОРОТЬБИ З ІНІЦІАТИВНИМ ШПИГУНСТВОМ

Процес становлення та розвитку України як незалежної держави з моменту проголошення суверенітету проходить в умовах складних геопо-

літичних та економічних змін, які зумовлені загостренням протистояння соціально-політичних систем, перерозподілом сфер впливу між провідними країнами світу.

Окрему, гостру проблему для держави на сьогодні становить зовнішня збройна агресія, внаслідок чого частина території України залишається окупованою. При цьому, в окремих південно-східних районах країни проводяться цілеспрямовані антитерористичні заходи. В цих умовах відмічається активізація діяльності в державі іноземних спеціальних служб, що вимагає адекватної протидії з боку контррозвідувальних органів і підрозділів Служби безпеки України.

Відповідно до пункту 4 статті 24 Закону України "Про Службу безпеки України" СБ України зобов'язана здійснювати контррозвідувальні заходи з метою попередження, виявлення, припинення і розкриття будь-яких форм розвідувально-підривної діяльності проти України.

Через зовнішню військову агресію одними із першочергових і актуальних завдань СБ України є здійснення контррозвідувального забезпечення оборонного комплексу, Збройних Сил України, інших утворених відповідно до законів України військових формувань, військово-технічного співробітництва, охорони державної таємниці, що передбачено положеннями пункту 6 статті 24 та пункту 2 статті 6 Закону України "Про контррозвідувальну діяльність".

Зазначені завдання зобов'язують СБ України постійно проявляти пильність, забезпечувати збереження відомостей, що становлять державну таємницю, як від посягань спецслужб іноземних держав, так і від ініціативного шпигунства.

Однією із важливих складових боротьби з ініціативним шпигунством є своєчасне виявлення, попередження та припинення дій громадян України, які за власною ініціативою займаються передачею або збиранням з метою передачі іноземній державі, іноземній організації чи їх представникам інформації, у тому числі з обмеженим доступом, що може завдати шкоди державній безпеці України.

Результати аналізу сучасної оперативної обстановки та тенденції її розвитку свідчать, що іноземні спеціальні служби поряд із легальними, конфіденційними і технічними можливостями активно використовують у розвідувальній діяльності громадян України, які ініціативно пропонують їм свої послуги в отриманні інформації, що становить оперативну зацікавленість, – т.зв. "ініціативників", які ініціативно пропонують свої послуги іноземній спецслужбі для проведення розвідувально-підривної діяльності проти власної країни.

Небезпечність такої діяльності зростає в умовах ускладнення оперативної обстановки (зокрема, що вимагає посиленого контррозвідувального забезпечення Збройних Сил України, інших національних військових формувань і, взагалі, військової сфери.

Боротьба з шпигунством та ініціативним шпигунством була і залишається однією з найважливіших задач спеціальних служб будь-якої держави, у тому числі й Служби безпеки України.

Сучасні умови протидії діяльності іноземних спецслужб із здобування в Україні відомостей військового, військово-промислового, науково-технічного характеру, що становлять державну таємницю, які можуть бути передані іноземній стороні у тому числі й "ініціативниками", вимагають вжиття цілеспрямованих контррозвідувальних заходів у вказаних життєво-важливих сферах, а також розробки відповідних керівних і методичних документів на загальнодержавному та відомчих рівнях.

*УДК 681.3, 621.396*

**Меленті Є.О.**
кандидат технічних наук
**Гарбузов О.А.**
**Пономарьов В.О.**
Інститут підготовки юридичних кадрів
для СБУ Національного юридичного
університету імені Ярослава Мудрого

## УДОСКОНАЛЕННЯ КОМПЛЕКСУ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ ОБ'ЄКТІВ ВІЙСЬКОВОГО УПРАВЛІННЯ

Наразі відбувається глобальна інформатизація та комп'ютеризація всіх сфер життєдіяльності людини: державні установи переходять на електронний документообіг, в урядових інформаційно-телекомунікаційних системах формуються досить об'ємні бази даних, об'єктами критичної інфраструктури керують автоматизовані системи управління, в органах військового управління також створюються системи автоматизації та прийняття рішення, які містять інформацію з обмеженим доступом. Слід навести приклад масованої атаки комп'ютерного вірусу PetyaA на українські фінансові установи, урядові організації та медіа компанії, локальні мережі, великі промислові об'єкти влітку 2017 року. Така кібернетична загроза паралізувала роботу зазначених установ та організацій на тривалий час. Для мінімізації загроз державним інформаційним ресурсам Службою безпеки України, зокрема Департаментом контррозвідувального захисту інтересів держави у сфері інформаційної безпеки, у взаємодії з іншими правоохоронними органами України та міжнародними партнерами здійснено заходи щодо локалізації розповсюдження шкідливого програмного забезпечення.

Таким чином, останні суспільно-політичні події, що відбувалися в Україні, досить яскраво показав, що для забезпечення національної безпе-

ки в інформаційній сфері слід більше приділяти уваги захисту важливих інформаційних ресурсів, баз даних держави, що містять інформацію з обмеженим доступом. З огляду на те, що комп'ютерна техніка стає основним засобом обробки і зберігання інформації, можливості засобів технічної розвідки постійно зростають.

Перевагами використання технічних засобів розвідки є:

- безперервне отримання розвідданих в режимі реального часу;
- постійне поліпшення їх тактико-технічних характеристик;
- можливість перехоплення інформативного сигналу на значній віддаленості від об'єкту спостереження;
- немає потреби ризикувати агентом (співробітником) для отримання закритої інформації.

Також до однієї з загроз інформації належить виток технічними каналами. При цьому відбувається виток інформації технічними каналами за рахунок розповсюдження інформативного сигналу через фізичну середовище від джерела корисного сигналу до приймача технічного засобу розвідки, що здійснює перехоплення інформації.

В доповіді проаналізовано можливі технічні канали витоку інформації та наведено їх характеристики. Особливу уваги приділено способам й формам застосування та тактико-технічним характеристикам сучасних засобів розвідки щодо зняття інформативного сигналу поблизу об'єктів військового управління.

З метою мінімізації можливості щодо зняття інформативного сигналу запропоновано при створенні комплексу технічного захисту застосовувати заходи електромагнітної сумісності та зашумлення простору навколо об'єктів інформаційної діяльності, де здійснюється обробка інформації з обмеженим доступом. Наведено математичні співвідношення, які можуть бути використанні при проведені розрахунків напруженості електромагнітного поля, яке збуджується технічним засобом обробки інформації з обмеженим доступом. Запропонований математичний апарат може бути використаний при розрахунках меж контрольованої зони.

*УДК 347.1*

**Мікуліна М.М.**
доктор юридичних наук, доцент
Національна академія СБ України

## ЩОДО ВІДПОВІДНОСТІ ПРИНЦИПІВ ЗАХИСТУ ФІЗИЧНИХ ОСІБ ПРИ ОБРОБЦІ ПЕРСОНАЛЬНИХ ДАНИХ

На сьогодні суспільним відносинам притаманне достатньо активне використання персональних даних в процесі обігу інформації, товарів, послуг, що актуалізує забезпечення вільного потоку інформації про особу та

її надійного захисту відповідно до основних прав і свобод людини. Стрімкі новації у галузі інформаційних технологій, активність формування баз персональних даних надзвичайно загострили проблему захисту приватного життя фізичних осіб й захисту інших прав і свобод людини. Протягом тривалого часу суспільство створювало базові принципи та стандарти щодо персональних даних, удосконалювало законодавство щодо безпечного їх функціонування й захисту.

Однак, ураховуючи накопичений досвід застосування законодавства щодо забезпечення і захисту прав та свобод людини, й, зокрема, персональних даних на європейському та світовому рівнях, національні регулятивні підходи ускладнюють розуміння сучасних проблем правового регулювання відносин із захисту відомостей про особу загалом, а також персональних даних фізичних осіб зокрема. Аналізуючи публікації за цією проблематикою, насамперед можна виокремити Закон України «Про захист персональних даних», що містить загальні питання нормативно-правового забезпечення під час обробки та циркуляції персональних даних [1]. Деякі з його положень зазнали обґрунтованої критики незалежних експертів з питань захисту даних [2] та українських науковців [3]. Питання охорони та захисту персональних даних правовими засобами, правового режиму охорони бази персональних даних, передумов та принципів захисту персональних даних в умовах розвитку інформаційного суспільства стали предметами досліджень І.М. Сопілко [4], І. Бойко [5], І.В. Костенко [6], Д.В. Карпенко [7], Т.І. Обуховської [8], М.М.Перепелиці [9] та інших. Однак поза увагою залишаються, зокрема, визначальні поняття Закону України «Про захист персональних даних» щодо принципів оброблення персональних даних та їх відповідність Конвенції «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» і Директиві 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних».

Конвенція «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» [9] одним із принципів автоматизованого оброблення персональних даних визначає якість таких даних. Статтею 5 Конвенції передбачено, що персональні дані повинні: а) отримуватися та оброблятися сумлінно та законно; б) зберігатися для визначених і законних цілей та не використовуватися в спосіб, не сумісний із цими цілями; в) бути адекватними, відповідними та не надмірними стосовно цілей, для яких вони зберігаються; г) бути точними та в разі необхідності оновлюватися; ґ) зберігатись у формі, яка дозволяє ідентифікацію суб'єктів даних не довше, ніж це необхідно для мети, для якої такі дані зберігаються.

Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» [10] містить такі принципи якості персональних даних, як: а)

оброблення чесно і законно; б) збирання для встановлених, чітких і законних цілей та надалі не оброблятися у спосіб, несумісний з цими цілями; в) бути достовірними, відповідними і не надлишковими відносно цілей, заради яких вони збираються і/або надалі обробляються; г) бути точними і, якщо необхідно, обновлятися; слід вжити всіх розумних заходів, щоб гарантувати, що дані, які є неточними чи неповними, з урахуванням цілей, заради яких вони були зібрані чи заради яких вони надалі обробляються, стиралися чи виправлялися; ґ) зберігатися у формі, що дозволяє встановлювати особу суб'єктів даних не довше, ніж це необхідно для цілей, заради яких дані були зібрані чи заради яких вони надалі обробляються.

У Законі України «Про захист персональних даних» відсутнє пряме зазначення принципу законності під час оброблення персональних даних, однак можна припустити, що дотримання вимог статті 3 Закону, а саме Конституції України, цього Закону, інших законів та підзаконних нормативно-правових актів, міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України, означає застосування зазначеного принципу. Окрім цього принципу у міжнародних актах містить зазначення принципу «сумлінності, чесності», яке відсутнє у Законі України. Натомість йдеться про відкритість і прозорість оброблення персональних даних.

*Сумлінністю* вважається етична відповідальність за свою поведінку перед оточенням; моральна свідомість; дія або здатність, що відрізняє правильну та помилкову поведінку тощо. *Чесністю* є моральною якістю та включає правдивість, принциповість, вірність взятим зобов'язанням, суб'єктивну переконаність у правоті справи, щирість перед іншими, визнання і дотримання прав інших людей на те, що їм законно належить. *Відкритість* – це щирість, довіра, здатність до спілкування. *Прозорість* – транспарентність, доступність для сприймання, зрозумілість, ясність. Порівнюючи застосування понять у названих вище правових актах, помічаємо різне наповнення їх змісту щодо застосування до процесу оброблення персональних даних. Український законодавець застосував відмінні від тих, що означають якісні характеристики у Конвенції № 108 та Декларації 95/46/ЄС.

Наступний принцип оброблення персональних даних визначений як: зберігатися для визначених і законних цілей та не використовуватися в спосіб, не сумісний із цими цілями (Конвенція № 108) та збирання для встановлених, чітких і законних цілей та надалі не оброблятися у спосіб, несумісний з цими цілями (Декларації 95/46/ЄС). У Законі «Про захист персональних даних» п. 5 ст. 6 містить положення про те, що «обробка персональних даних здійснюється для конкретних і законних цілей, визначених за згодою суб'єкта персональних даних, або у випадках, передбачених законами України, у порядку, встановленому законодавством».

Як зазначають експерти Євросоюзу, що давали незалежну оцінку Закону «прочитання цих двох положень разом припускає, що особи можуть надавати згоду лише на цілі, передбачені законодавчими або іншими нормативно-правовими інструментами. Це логічно узгоджується. Однак, навіщо тоді потрібен виняток? Не може ж такого бути, що він там є, щоб дозволити обробку (на противагу визначенню цілі) без згоди, оскільки це передбачається в шостому пункті статті 6» [2]. Український законодавець взагалі не використав конструкцію щодо «не використання в спосіб, не сумісний із цими цілями», тобто можна припускати, що а) таке використання, оброблення можливе, б) зібрані дані можна обробляти з іншою метою, якщо друга мета «сумісна» з першою; в) можна розголошувати дані, якщо вони пройшли відбір щодо «несумісності».

Принцип адекватності, відповідності та ненадмірності стосовно цілей, для яких вони зберігаються; достовірності і ненадлишковості відносно цілей, заради яких вони збираються і/або надалі обробляються втілений у Законі аналогічно.

Принцип захисту осіб при операціях з персональними даними, що вимагає точності та за необхідності їх оновлення, також передбачає гарантування подальшого стирання чи виправлення неточних або неповних даних, ураховуючи цілі, заради яких вони збиралися чи будуть надалі оброблятися. Застосування українським законодавцем термінів «точний» і «достовірний» навряд чи доречне, бо «точний», що означає «той, який суворо дотримується встановленого порядку; який цілковито відповідає дійсності, істині; який цілком відповідає певному зразку, вимогам; конкретний, максимально визначений» за значенням поглинає поняття «достовірний».

Принцип зберігання у формі, яка дозволяє ідентифікацію суб’єктів даних не довше, ніж це необхідно для мети, для якої такі дані зберігаються; зберігання у формі, що дозволяє встановлювати особу суб’єктів даних не довше, ніж це необхідно для цілей, заради яких дані були зібрані чи заради яких вони надалі обробляються сприйнятий вітчизняним Законом відповідно до того, що персональні дані обробляються у формі, що допускає ідентифікацію фізичної особи, якої вони стосуються, не довше, ніж це необхідно для законних цілей, у яких вони збиралися або надалі оброблялися. Подальша обробка персональних даних в історичних, статистичних чи наукових цілях може здійснюватися за умови забезпечення їх належного захисту.

Насамкінець можна констатувати, що загалом загальні принципи захисту фізичних осіб при обробці персональних даних, визначені у міжнародних правових актах, сприйняті та відображені у Законі України «Про захист персональних даних». Однак законодавець повинен мобільно реагувати на будь-які суспільні, технічні та інші зміни.

**Література**

1. Закон України «Про захист персональних даних» : Закон України від 01.06.2010 № 2297-VI. – URL: http://zakon.rada.go.ua/go/.

2. Марі Жорж. Аналіз Закону України «Про захист персональних даних» / Марі Жорж, Грем Саттон. URL: http://: file:///G:/Нові%20статті/Аналіз%20ЗУ%20ПД.pdf.

3. Усенко І. Коментар до Закону України «Про захист персональних даних» [Електронний ресурс]. – URL: http://Khpg.org > index pxp? Id=1330343937.

4. Сопілко І.М. Сучасне поняття персональних даних: доктринальний та нормативний аспекти / І.М. Сопілко // Юридичний вісник 3(28) 2013. – С. 63-68.

5. Бойко І. Охорона й захист персональних даних адміністративно-правовими засобами / І. Бойко // Вісник Національного університету «Юридична академія України імені Ярослава Мудрого» № 4(67) 2011. – С. 144-151.

6. Костенко І.В. Організаційно-правове забезпечення персональних даних в діяльності правоохоронних органів України / І.В. Костенко // Наукові праці МАУП, 2014, вип. 2(41). – С. 87-90.

7. Карпенко Д.В. Правовий режим охорони бази персональних даних на підприємствах України / Д.В. Карпенко // Форум права. – 2012. - № 1. URL: http:// : http://www.nbuv.gov.ua/e-journals/FP/2012-1/12kdvnpu.pdf.

8. Обуховська Т.І. Захист персональних даних в умовах розвитку інформаційного суспільства: передумови, принципи та міжнародне законодавство / Т.І. Обуховська // Вісник НАДУ. – 2014. – № 1. – С. 95-103.

9. Конвенція «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних». URL: http://: http://zakon5.rada.gov.ua/laws.

10. Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних». URL: http://: http://zakon3.rada.gov.ua/laws.

*УДК 355.40*

**Настрадін В.П.**
кандидат технічних наук, професор
Національна академія СБ України
**Горєлова В.Ю.**
кандидат юридичних наук
Університет економіки та права «КРОК»

## РОЗВІДКА В ІНФОРМАЦІЙНОМУ ПРОСТОРІ: ПРАВОВІ МЕЖІ

Протягом останнього десятиріччя Україна наполегливо крокує в бік Європейського співтовариства, яке ставить акценти на необхідності не тільки розбудови інформаційного суспільства, а й забезпечення безпеки в

інформаційному просторі, що однозначно має впливати на процес вдосконалення вітчизняного законодавства в цьому питанні.

Одним з ключових та проблемних моментів в інформаційному просторі є категорія «інформаційна розвідка». В США і країнах Європи прийнято розрізняти конкурентну розвідку (competitive intelligence); також можна зустріти назви «ділова розвідка», «бізнес-розвідка», «комерційна розвідка») і «промислове шпигунство». Відмінністю конкурентної розвідки від промислового шпигунства є те, що її методи є невід'ємними від самої життєдіяльності людини, а сама вона проводиться в рамках діючих правових норм, і отримує результати завдяки аналітичній обробці величезної кількості різноманітних відкритих (в тому числі і ніде не опублікованих, але законно отриманих від їх носіїв) інформаційних матеріалів. На практиці всі методи збору інформації конкурентним розвідником зводяться лише до трьох законних методів: спостереження (за навколишнім світом), з опитуванням (точніше, бесід з людьми) і збору зразків.

За відсутності окремого законодавчого визначення та відповідної юридичної бази зрозуміло, що конкурентний розвідник не може проводити інформаційну розвідку методами оперативно-розшукової діяльності, чи виконувати роботу приватного детектива. Але виникає питання законності самого доступу до окремих видів інформації. Державна таємниця чи державні секрети є основною категорією інформації, забороненої для інформаційної розвідки. В той же час існує нетаємна інформація, оприлюднення якої може нанести шкоду державі. До другої категорії іншої інформації, що захищається, можна віднести персональні дані та особисте життя особи, відомості, що стосуються таємниці слідства та судочинства, службову таємницю, професійну таємницю, комерційну та банківську таємниці, відомості про сутність винаходу, корисної моделі чи промислового зразку до офіційної публікації інформації про них.

Збираючи інформацію про комерційну структуру аналітик може і не знати, чи захищена вона режимом комерційної таємниці (залежить від рівня організації інформаційної безпеки такої структури), чи ні. А за відсутності відповідного правового регулювання він може бути вимушений доказувати законність збору інформації у суді. Також законодавчо інформація про фізичну особу (персональні дані) захищена, але коли особа дає письмову згоду на обробку відомостей про себе, то не рідко вони свідомо чи через службову недбалість потрапляють до інших рук та оприлюднюються і це також потребує відповідного врегулювання.

Інформаційна розвідка в просторі Інтернет, при цьому, є особливим видом аналітичного опрацювання даних, адже саме мережевий простір дозволяє збирати будь-яку інформацію правомірно та без застосування оперативно-розшукових заходів, що є виключною прерогативою відповідних органів, хоча саме методи інформаційної розвідки напрочуд є схожими з

тими, що застосовуються спецслужбами. Інтернет, насамперед, використовується для отримання бізнес-інформації, пов'язаної з вирішенням ряду економічних, маркетингових, охоронних та інших задач. Розвідка у відкритому доступі до інформації дозволяє, наприклад, отримати інформацію про фактичних контрагентів чи конкурентів (їх місцезнаходження, інформацію про засновників, розмір статутного фонду та фінансовий стан тощо), недобросовісного страховика або страхувальника при укладанні договору страхування, інформацію про імідж компанії при укладанні комерційних договорів, інформацію про наявність та дії конкурентів, інформацію при оцінці фінансових ризиків тощо, а також для розвідування каналів витоку власної інформації.

Таким чином, інформаційна складова у сучасному світі фактично набуває статусу «товару», а отже є ціннісним і охоронюваним об'єктом, на що в сучасних правових умовах має акцентуватись увага законодавця. Разом з тим, на нашу думку, має бути чітке законодавче розмежування категорії «інформаційної розвідки» від «інформаційного шпигунства» у секторі забезпечення національної безпеки.

**Література**

1. Богуш В.М., Юдін О.К. Інформаційна безпека держави. – К. : «МК-Прес», 2005. – 432с.

2. Арістова І. В. Інформаційна розвідка як напрямок удосконалення державного управління інформаційною сферою / І. В. Арістова // Право і Безпека. – 2005. – Т. 4. – № 1. – С. 11-13. – Режим доступу: http://nbuv.gov.ua/UJRN/Pib_2005_4_1_5.

3. Богуш В.М. Розвідка в інформаційному суспільстві : довідник-словник. – К.: МОУ, 2000. – 768 с.

*УДК 355.40: 35.083.8:343.45*

**Попутніков В.Б.**
професор спеціальної кафедри № 1
ННІ КРД НА СБУ

## АКТУАЛЬНІ ПРОБЛЕМИ ЗАКОНОДАВЧОГО РЕГУЛЮВАННЯ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ ПРИ ВИКОРИСТАННІ КОНФІДЕНЦІЙНОГО СПІВРОБІТНИЦТВА

Внаслідок агресії проти України з боку РФ виникли нові загрози, що мають довгостроковий характер та кардинальним чином впливають на зовнішнє і внутрішнє безпекове середовище нашої держави. Вказане зумовило необхідність створення нової системи забезпечення національної безпеки України. На сьогодні в рамках затвердженої Указом Президента

України від 26.05.2015 № 287/2015 Стратегії національної безпеки України реалізуються заходи, спрямовані серед іншого на подолання застарілості системи охорони державної таємниці. Для цього, в рамках Програми дій щодо адаптації та гармонізації національного законодавства до стандартів НАТО та ЄС та розпорядження ЦУ СБУ № 256-2015р. напрацьовано концептуальні пропозиції по реформуванню системи охорони держтаємниці. Актуальність даної проблематики підтверджується й тим, що розпочате реформування Служби безпеки України має на меті забезпечити концентрацію зусиль саме на контррозвідувальній діяльності та надійному захисті державних секретів.

У цьому контексті вкрай важливим питанням є забезпечення охорони державної таємниці конфіденційного співробітництва, оскільки головну роль при здійсненні органами і підрозділами СБУ контррозвідувальної, оперативно-розшукової діяльності та НСРД пріоритет мають негласні методи отримання інформації, серед яких провідна роль належить негласному апарату та іншим категоріям оперативних джерел. При цьому, згідно з положеннями законів України «Про контррозвідувальну діяльність», «Про оперативно-розшукову діяльність» та «Службу безпеки України», держава гарантує конфіденційність відносин між оперативними підрозділами СБУ та особами, які надають їй допомогу. У свою чергу, особи, які залучаються до виконання оперативних завдань, зобов'язані зберігати таємницю, що стала їм відома.

Ґрунтуючись на приписах частини четвертої статті 27 Закону України «Про державну таємницю», яка визначає, що порядок надання доступу до державної таємниці залученим до конфіденційного співробітництва особам визначається керівниками відповідних спеціально уповноважених органів, які проводять оперативно-розшукову, розвідувальну або контррозвідувальну діяльність, в системі СБУ чітко відпрацьовано на рівні відомчих нормативно-правових актів відповідний механізм.

Водночас, напрацьована практика свідчить про наявність низки проблемних питань при наданні доступу особам, залученим в негласний апарат, до секретних відомостей.

У зв'язку із цим, в рамках підготовки проекту Концепції реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом фахівцями Національної академії СБУ були підготовлені відповідні пропозиції.

Разом із цим, концептуальне вирішення низки проблемних питань на теперішній час необґрунтовано відтерміновується на невизначений строк.

Виходячи із зазначеного, доцільно ще раз акцентувати увагу на таких пропозиціях до чинного законодавства:

1. Для більш чіткого визначення, що доступ до державної таємниці залученим до конфіденційного співробітництва особам надається без оформлення їм допуску вбачається за доцільне:

- частину першу статті 27 Закону України «Про державну таємницю» викласти у такій редакції:

*«Доступ до державної таємниці надається дієздатним громадянам України, яким надано допуск до державної таємниці та які потребують його за умовами своєї службової, виробничої, наукової чи науково-дослідної діяльності, навчання або у зв'язку зі здійсненням конфіденційного співробітництва»*;

- статтю 9 Закону України «Про контррозвідувальну діяльність» доповнити новою частиною другою у наступній редакції:

*«Доступ особам, залученим до конфіденційного співробітництва з підрозділами, які здійснюють контррозвідувальну діяльність, до державної таємниці та службової інформації з обмеженим доступом надається згідно із законом у порядку, визначеному нормативно-правовими актами Служби безпеки України»;*

- доповнити частину третю статті 11 Закону України «Про оперативно-розшукову діяльність» [12] новим першим реченням такого змісту:

«*Особам, які залучаються до конфіденційного співробітництва для надання негласної допомоги (сприяння) у підготовці чи проведенні негласних оперативно-розшукових заходів надається доступ до відомостей з обмеженим доступом в обсязі, необхідному для якісного виконання ними оперативних завдань»*.

2. Тривалий час існує правова колізія між положеннями статей 328 та 422 Кримінального кодексу України та приписами частини 4 статті 27 Закону України «Про державну таємницю» і частини 3 статті 11 Закону України «Про оперативно-розшукову діяльність».

З метою її усунення пропонується:

- у частині першій статті 328 (Розголошення державної таємниці) КК України після слів «довірені або стали відомі у зв'язку з виконанням службових обов'язків» доповнити словами «*чи у ході конфіденційного співробітництва з уповноваженими органами*» і далі за текстом;

- аналогічні редакційні зміни потрібно внести й до частини першої статті 422 (Розголошення відомостей військового характеру, що становлять державну таємницю, або втрата документів чи матеріалів, що містять такі відомості).

Такі зміни створять належні правові підстави для можливого притягнення до відповідальності осіб, з якими здійснюється конфіденційне співробітництво, у разі розголошення ними секретної інформації оперативного характеру, що стало їм відома під час такого співробітництва.

*УДК 242*
**Розвадовський О.Б.**
доктор юридичних наук,
Національна академія СБ України

# ДЕРЖАВНА ПОЛІТИКА ЩОДО ЗАБЕЗПЕЧЕННЯ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ ТА СЛУЖБОВОЇ ІНФОРМАЦІЇ У СУЧАСНИХ УМОВАХ

У наш час політика розглядається як цілеспрямована діяльність пов'язана з прийняттям відповідальних рішень у певній галузі взаємовідносин. Тобто це управлінська діяльність стратегічного рівня, щодо внутрішніх та зовнішніх правостосунків і взаємодій. В широкому розумінні політика це визначений напрямок такої діяльності (програма дій), або сукупність засобів (інструментів) та методів для реалізації певних інтересів задля досягнення визначених цілей у певному соціальному середовищі.

На основі аналізу загальних теоретичних уявлень про державну політику взагалі, *державна політика щодо забезпечення охорони державної таємниці та службової інформації* – це діяльність уповноважених органів державної влади з управління системою забезпечення охорони інформації з обмеженим доступом, що передбачає визначення мети, завдань, принципів, напрямів і комплексних заходів, спрямованих на запобігання витоку та розголошення державної таємниці й службової інформації, впровадження інших превентивних заходів, а також своєчасне виявлення та припинення розвідувальних спрямувань спеціальних служб іноземних держав, а також організацій, окремих груп та осіб до такої інформації, інших правопорушень у цій сфері.

Метою вказаної політики є своєчасне виявлення джерел реальних і потенційних загроз у цій сфері, аналіз причин їх виникнення, способів нейтралізації й упередження шляхом розробки адекватних організаційно-правових заходів.

Основними завданнями державної політики щодо забезпечення охорони державної таємниці та службової інформації є:

- створення умов для своєчасного виявлення джерел загроз у цій сфері та визначення можливих наслідків їх дії;
- визначення комплексу превентивних заходів із запобігання витоку і розголошення інформації з обмеженим доступом та нейтралізації або зменшення негативних наслідків реалізації загроз;
- забезпечення отримання своєчасної, повної і точної інформації для прийняття управлінських рішень із охорони державної таємниці та службової інформації;
- удосконалення організаційно-правової діяльності відповідних суб'єктів з метою гармонізації державних, суспільних і особистих інтере-

сів у цій сфері, недопущення обмеження права громадян на вільний доступ до інформації;

- забезпечення технічного захисту інформації з обмеженим доступом;
- здійснення взаємовигідного міждержавного співробітництва у сфері забезпечення охорони інформації з обмеженим доступом.

На етапі формування державної політики щодо забезпечення державної таємниці та службової інформації важливим є зосередження уваги на її експертно-аналітичному забезпеченні, розробленні методології аналізу, виробленні механізму моніторингу впровадження та критеріїв оцінки ефективності її реалізації.

Результативність державної політики щодо забезпечення охорони державної таємниці та службової інформації забезпечується:

по-перше, визначенням чітких та реалістичних цілей (мети) і напрямів;

по-друге, якістю аналізу проблеми у цій сфері та розроблених альтернативних управлінських рішень;

по-третє, обізнаністю з метою, принципами, напрямами державної політики та дотриманням уповноваженими державними органами основоположних управлінських цінностей, до яких відносять надійність, прозорість, підзвітність, відповідальність, адаптивність, ефективність.

Необхідно враховувати, результати впровадження державної політики можуть бути отримані лише протягом тривалого часу, шляхом проведення постійного оцінювання та дієвого моніторингу, які повинні бути пріоритетом. При визначенні критеріїв оцінки необхідно враховувати їх різний характер (розрізняючи між виміром сприйняття політики і практичними результатами) та рівень надійності, а також збалансованість якісних і кількісних показників.

Вкрай важливе значення має наукове забезпечення державної політики. Воно полягає у проведенні фундаментальних і прикладних досліджень, формуванні наукових центрів, дослідницьких груп, які займаються вивченням актуальних проблем у цій сфері й виробленням рекомендацій для уповноважених державних органів.

У*ДК: 342.1:35.083*

**Рябцова Л.П.**
Департамент охорони державної таємниці
та ліцензування СБ України

## НОРМАТИВНЕ ЗАБЕЗПЕЧЕННЯ ПИТАНЬ ОХОРОНИ ІНФОРМАЦІЇ, ОБМІН ЯКОЮ ЗДІЙСНЮЄТЬСЯ В РАМКАХ СПІВРОБІТНИЦТВА УКРАЇНИ З НАТО

Одним з пріоритетних напрямів зовнішньої політики України є розвиток партнерства з Організацією Північноатлантичного договору.

З метою створення правових засад для обміну інформацією з обмеженим доступом, який здійснюється між установами України та НАТО в рамках відповідних програм співробітництва, 13 березня 1995 року у м. Брюссель укладено Угоду про безпеку між Урядом України і Організацією Північноатлантичного Договору.

Зазначена угода, зокрема передбачає можливість здійснення між Україною та НАТО консультацій і обміну інформацією з обмеженим доступом з політичних питань та питань, пов'язаних з безпекою, а також інтенсифікацію політичного та військового співробітництва. Обмін такою інформацією має здійснюватися відповідно до узгоджених спільних стандартів.

З огляду на те що Угода про безпеку носить рамковий характер, та з метою практичної реалізації вказаного міжнародного договору, Службою безпеки України розроблено правила поводження та забезпечення охорони інформації НАТО з обмеженим доступом в Україні, які затверджено наказом.

Водночас, з метою деталізації процедур із забезпечення безпеки інформації з обмеженим доступом відповідно до статті 4 Угоди про безпеку, а також визначення правових засад забезпечення взаємної охорони інформації з обмеженим доступом 28 вересня 2016 року підписано Адміністративні домовленості щодо охорони інформації з обмеженим доступом між Урядом України та Організацією Північноатлантичного Договору, які ратифіковані Законом України від 24 травня 2017 року № 2068-VIII [1].

Зазначені Адміністративні домовленості закріплюють на міжнародному рівні зобов'язання сторін і детальний порядок охорони інформації з обмеженим доступом, обмін якою здійснюється між Україною та НАТО.

Зокрема, у положеннях Адміністративних домовленостей визначаються:

формат, статус та сфера дії цього міжнародного документу;

органи безпеки, відповідальні за їх імплементацію (СБУ та Офіс безпеки НАТО) та зобов'язання органів безпеки щодо надання сприяння у проведенні взаємних консультацій та інспектувань з метою оцінки стану охорони інформації з обмеженим доступом, переданої іншою стороною;

співставлення грифів обмеження доступу для застосування рівнозначних заходів охорони інформації, обмін якою здійснюватиметься між сторонами;

мінімальні стандарти безпеки, за якими сторони зобов'язуватимуться забезпечувати взаємну охорону інформації з обмеженим доступом, зокрема у сферах допускної системи, фізичної безпеки, ведення діловодства, технічного захисту інформації тощо;

окремий статус та роль Місії України при НАТО, яка діє як первинний пункт входу до України інформації НАТО з обмеженим доступом.

Після укладення Адміністративних домовленостей постала потреба у здійсненні заходів, спрямованих на забезпечення виконання положень зазначеного міжнародного договору.

Пріоритетними завданнями у контексті імплементаційних просувань у вказаному напрямку наразі вбачаються:

реалізація зусиль, спрямованих на адаптацію законодавства України з питань захисту та охорони інформації з обмеженим доступом до стандартів безпеки НАТО;

впровадження в державних органах та установах механізмів дотримання на внутрішньодержавному рівні міжнародних зобов'язань відповідно до Адміністративних домовленостей;

продовження здійснення заходів з укладення угод про взаємну охорону інформації з обмеженим доступом з державами - членами НАТО.

У розрізі створеного правового підґрунтя Адміністративними домовленостями виникла необхідність у перегляді положень Правил та виданні нормативно-правового акта щодо порядку охорони інформації НАТО в Україні, гармонізованого із спільно узгодженими в міжнародному договорі стандартами.

З огляду на викладене, СБУ розроблено новий наказ про затвердження Правил забезпечення охорони інформації НАТО з обмеженим доступом в Україні.

У зазначеному нормативному акті враховано запроваджені Адміністративними домовленостями нововведення щодо термінології та вимог з охорони інформації з обмеженим доступом, які відповідають безпековим стандартам НАТО [2].

Зокрема в оновлених Правилах оптимізовано процедури щодо:

порядку маркування обмежувальними позначками документів НАТО згідно з еквівалентністю грифів обмеження доступу, встановленою Адміністративними домовленостями;

механізмів обміну інформацією НАТО в рамках реєстраційної системи;

вимог надання доступу до інформації НАТО та опрацювання документів, що містять таку інформацію;

алгоритмів знищення матеріальних носіїв інформації НАТО з обмеженим доступом;

особливостей контролю за станом забезпечення охорони інформації, обмін якою здійснюється тощо.

*Таким чином, завдяки втіленим зусиллям з удосконалення механізмів безпеки інформації з обмеженим доступом, що надходить від установ НАТО, в Україні створено надійну систему охорони такої інформації, яка водночас є гнучкою для вчасного реагування на нові виклики, обумовлені міжнародною ситуацією.*

**Література**

1. Адміністративні домовленості щодо охорони інформації з обмеженим доступом між Урядом України та Організацією Північноатлантичного Договору від 28 вересня 2016 року, ратифіковані Законом України від 24 травня 2017 року № 2068-VIII.

2. Політика безпеки НАТО С-М (2002)49 від 17.06.2002.

*УДК 65.012.8 (477)*

**Сидоренко С.М.**
Національна академія СБ України

# ОРГАНІЗАЦІЙНО-ПРАВОВІ ЗАСАДИ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ ЕСТОНСЬКОЇ РЕСПУБЛІКИ

Зміст організаційно-правових засад охорони державної таємниці Естонської Республіки зводиться до організації захисту державних таємниць шляхом встановлення єдиних вимог та спеціальної процедури щодо забезпечення такої діяльності.

Ефективність організації захисту державних таємниць в Естонії забезпечується наступним: встановленням кримінальної (дисциплінарної) відповідальності за порушення процедури доступу до державних таємниць, порушення вимог обробки державних таємниць і носіїв секретних відомостей, а також – за незаконне розсекречення державних таємниць; захист державних таємниць від незаконного розсекречення; згода на дотримання вимог, встановлених для обробки державних таємниць і секретних носіїв.

Процедура захисту державних таємниць регулюється постановою Уряду Естонської Республіки. Вказаний норматив врегульовує вимоги до органів, інституцій і юридичних осіб, що володіють державними таємницями з метою організації їх захисту; особливу процедуру обробки державних таємниць і носіїв секретних відомостей; вимоги щодо сховищ, доставки, транспортування й переміщення носіїв секретних відомостей; вимоги щодо організації роботи служб безпеки і Генерального штабу Сил оборони стосовно здійснення контролю, покладеного на них Законом «Про державні таємниці» [1].

Державні таємниці Естонії класифікуються наступним чином:

1) державні таємниці, визначені як «обмеженого доступу»;

2) державні таємниці, визначені як «конфіденційні»; 3) державні таємниці, визначені як «таємні»; 4) державні таємниці, визначені як «цілком таємні».

Така класифікації пояснюється тим, що у серпні 2001 року до закону Естонії «Про державні таємниці» були внесені зміни і доповнення з метою приведення його у відповідність до вимог НАТО [1].

Згідно із законом Естонської Республіки «Про державні таємниці», рішення щодо передчасного розсекречування, або продовження терміну секретності інформації, приймає Уряд Естонії [1, 3].

Поряд з відмовою у допуску до державної таємниці, або відмовою у продовженні терміну дії дозволу на допуск, відомство, що здійснює перевірку для допуску до секретної інформації, зобов'язане протягом п'яти робочих днів надіслати до відомства, яке засвідчує необхідність у допуску до секретної інформації, офіційно завірену копію рішення про відмову у наданні дозволу [1, 2].

Згідно § 23 розділу 6 закону Естонії «Про державні таємниці» право доступу до державних таємниць, незважаючи на їх секретність, мають посадові особи: Президент Республіки – з метою виконання обов'язків, покладених на нього Конституцією і Законами Естонської Республіки; члени Рійгікогу у випадках, передбачених законом «Про внутрішні норми Рійгікогу»; члени Уряду Республіки у випадках, передбачених Законом «Про Уряд Естонської Республіки»; судді у випадках, передбачених у Кодексі з процедури; Командувач і Головнокомандувач Сил оборони у випадках, передбачених Законами стосовно національної оборони; Канцлер права з метою виконання обов'язків, покладених на нього Конституцією Республіки Естонія і Законами; Генеральний фінансовий інспектор у випадках, передбачених Законом про державний департамент з аудиту; Президент Нацбанку Естонії, а також голова і члени Департаменту Нацбанку Естонії у випадках, передбачених Законом «Про Нацбанк Естонії» [4, 5, 6].

Порядок здійснення перевірки осіб для допуску до секретної інформації здійснюється відповідно до процедури встановленої виключно законодавством, зокрема, Законом «Про нагляд» та Законом «Про служби безпеки». Терміни проведення спеціальної перевірки становлять три місяці для фізичних осіб та шість місяців для юридичних осіб. Терміни можуть бути подовжені на три і шість місяців відповідно на підставі рішення відомства, яке проводить спеціальну перевірку, або рішення Комітету з питань захисту державних таємниць.

Стосовно обмеження щодо оприлюднення, передачі або поширення іншим чином секретної інформації, то законодавство Естонії у сфері охорони державної таємниці не містить чіткої норми, однак включає окремі положення, які стосуються доступу іноземців до державної таємниці, а також передачі відомостей, що становлять державну таємницю [2, 3, 4].

Зокрема, § 26 розділу 6 закону «Про державні таємниці» визначає норми щодо доступу іноземців до державних таємниць та передачі державної таємниці іноземним державам чи міжнародним організаціям [1].

Зміни до законодавства Естонії є результатом входження країни до євроатлантичних структур та адаптації її законодавства до стандартів НАТО. Внесені вони з метою гарантування безпеки інформації НАТО, яка

надається Естонській Республіці країнами-членами Північноатлантичного альянсу.

**Література**

1. Закон Естонської Республіки «Про державні таємниці» від 26 січня 1999 року, зі змінами та доповненнями від 12 лютого 2003 року // www.rus.log.ee.

2. Закон Естонської Республіки «Про внесення змін до Закону про статус суддів» від 2001 року // www.rus.log.ee.

3. Закон Естонської Республіки «Про внесення змін до Закону про внутрішній регламент Рійгікогу» від 2003 року // www.rus.log.ee.

4. Закон Естонської Республіки «Про внесення змін до Кримінального Кодексу» від 2001 року // www.rus.log.ee.

5. Закон Естонської Республіки «Про внесення змін до Кодексу про адміністративні правопорушення» від 2001 року // www.rus.log.ee.

6. Закон Естонської Республіки «Про внесення змін до Закону про Національний Банк Естонії» від 2003 року // www.rus.log.ee.

# ПОГЛЯД НА ПРОБЛЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ МОЛОДИХ УЧЕНИХ І СТУДЕНТІВ

*УДК 351.862.4 (477)*

**Алєйников І.В.**
ад'юнкт Національного університету
оборони України ім. Івана Черняховського

## ДО ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ У ВОЄННІЙ СФЕРІ

Об'єктами забезпечення інформаційної безпеки у воєнній сфері є:

- інформаційна інфраструктура центральних органів воєнного управління, органів воєнного управління видів Збройних Сил, об'єднань, з'єднань, військових частин і організацій, які входять до складу Збройних Сил, навчальних закладів Збройних Сил, науково-дослідних установ Міністерства оборони;
- інформаційні ресурси підприємств оборонного комплексу і науково-дослідних установ, які займаються оборонною проблематикою;
- програмно-технічні засоби та інформаційні ресурси автоматизованих і автоматичних систем управління військами і зброєю, озброєння і військової техніки, оснащених засобами інформатизації;
- керівний і особовий склад Збройних Сил.

До загроз національній безпеці в інформаційній сфері відносяться:

- обмеження свободи слова та доступу громадян до інформації, руйнування системи цінностей, духовного та фізичного здоров'я особи, суспільства, негативні зміни їх цільових настанов;
- блокування діяльності державних ЗМІ по інформуванню внутрішньої і зарубіжних аудиторій, обмеження можливостей органів державної влади приймати адекватні рішення;
- порушення штатного режиму функціонування (знищення) критично важливих інформаційних мереж, систем управління, несанкціонований витік таємної, конфіденційної та іншої інформації з обмеженим доступом;
- знищення інформаційних ресурсів, програмного забезпечення, створення умов для технологічної залежності країни в інформаційній сфері;
- низький рівень інтегрованості країни в світовий інформаційний простір.

Головна інформаційна загроза національній безпеці України створюється через інформаційний вплив іншої сторони на свідомість, підсвідомість, інформаційні ресурси, інформаційну інфраструктуру країни з метою

нав’язати особистості, суспільству та державі бажану (для іншої сторони) систему цінностей, поглядів, інтересів і рішень у життєво важливих сферах суспільної і державної діяльності, керувати їхньою поведінкою і розвитком у бажаному для іншої країни напрямку. Це є загрозою суверенітету України в життєво важливих сферах суспільної й державної діяльності, в тому числі і у воєнній сфері, що реалізовується на інформаційному рівні.

Основними напрямками державної діяльності щодо забезпечення інформаційної безпеки держави на думку автора має бути:

- забезпечення інформаційного суверенітету, вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів;
- впровадження новітніх інформаційних технологій;
- наповнення внутрішнього та світового інформаційного простору достовірною інформацією про країну;
- активне залучення засобів масової інформації до боротьби з корупцією, зловживанням службовим становищем, іншими явищами, які загрожують національній безпеці країни;
- забезпечення неухильного дотримання конституційного права громадян на свободу слова, доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції;
- вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери країни.

Потребують негайного вирішення такі проблеми:

- розробка концепції інформаційної безпеки ЗС України, яка повинна затвердити термінологію у цій галузі, визначити основні проблеми та шляхи їх вирішення;
- розробка стратегії і тактики ведення інформаційної боротьби в інтересах вирішення завдань національної безпеки в цілому і воєнної та економічної безпеки зокрема: створення функціональних підрозділів інформаційної боротьби в Збройних Силах України;
- вироблення механізмів взаємодії між міністерствами і відомствами України з питань інформаційної боротьби в інтересах забезпечення національної (воєнної, економічної) безпеки держави;
- удосконалення нормативно-правової бази в сфері інформаційної безпеки, у тому числі в частині регулювання розробки, виробництва, поширення і застосування інформаційної зброї.

**Література**

1. Основи воєнної безпеки держави: підруч. / Ю. В. Пунда, В. П. Грищенко, П. М. Грицай та ін. – К.: НУОУ ім. Івана Черняховського, 2017. – 204 с.

2. Указ Президента України “Про рішення Ради національної безпеки і оборони України від 01.03.2014 “Про невідкладні заходи щодо забезпечення національної безпеки, суверенітету і територіальної цілісності України” від 02.03.2014 № 189/2014 // URL: http://zakon.rada.gov.ua. (дата звернення 26.02.2018).

3. Закон України “Про Збройні Сили України” від 06.12.1991 № 1934-XII (зі змінами). / ВР України. URL: http://zakon.rada.gov.ua. (дата звернення 26.02.2018).

*УДК 340.15:351.746.1*

**Бараннік В.В.**
студентка Національної академії СБ України

## ДІЯЛЬНІСТЬ ОРГАНІВ НАЦІОНАЛЬНОГО САМОВРЯДУВАННЯ КРИМСЬКОТАТАРСЬКОГО НАРОДУ ЯК ОБ’ЄКТ ІНФОРМАЦІЙНОГО ВПЛИВУ РАДЯНСЬКОЇ РОСІЇ (1917 – 1928 РР.): ІСТОРИКО-ПРАВОВИЙ АНАЛІЗ

Після анексії Криму у 2014 р. Російська Федерація докладає значних зусиль до руйнування національної самосвідомості мешканців півострова, використовуючи широкий арсенал відпрацьованих ще за часів Радянського Союзу методів інформаційного впливу. Серед них окремо потрібно виділити методи цілеспрямованої дискредитації діяльності органів національного самоврядування. У кримських татар такими виступають Курултай – вищий представницький повноважний орган кримськотатарського народу та національна партія кримських татар – Міллі-Фірка. Тому, в контексті розуміння сучасних подій, які відбуваються в Криму важливого значення набуває вивчення тактики боротьби радянської Росії з Першим Курултаєм кримськотатарського народу (далі – Курултай) та національною партією кримських татар – Міллі-Фірка.

Кримськотатарська революція, що розпочалася у березні 1917 р., а влітку й на початку осені вилилася у формування самоврядних національних органів і перших військових підрозділів чітко викристалізувала прагнення кримських татар до національно-державного самовизначення.

Після проголошення Курултаєм у грудні 1917 р. Кримської Народної Республіки, створення національного уряду – Директорії та прийняття першої кримськотатарської Конституції більшовицький уряд Росії – Рада Народних Комісарів Росії (Раднарком) розпочав активну роботу із фальсифікації його досягнень, дискредитації діяльності «Міллі-Фірки», прагнучи сформувати уявлення у більшості населення півострова про можливість їх самовизначення виключно в межах радянської Росії. Для досягнення поставленої мети Раднарком охопив агітаційною пропагандою широкі верстви населення та в повній мірі використовував потужності друкованих видань.

На підставі аналізу історичного досвіду можна виділити наступні етапи інформаційної дискредитації Курултаю та «Міллі-Фірки».

Перший етап (грудень 1917 р. – січень 1918 р.) спрямований на розпуск Курултаю.

Пересвідчившись, що серед переважної більшості населення півострова жовтневий переворот не користується підтримкою більшовики озброюють загони червоної гвардії, оголошують національний уряд кримських татар «контрреволюційним» урядом звинувативши його у прийнятті рішення про вихід Криму зі складу Росії та змові з Українською Центральною Радою, яка планувала за допомогою кримськотатарських військ захопити у свої руки увесь Крим [4; 5]. Вдаючись до поширення провокативних повідомлень, фальшування реального стану справ, більшовики зуміли переконати більшість солдат, моряків і революційно налаштованих робітників міс півострова у необхідності захисту завоювань революції від нібито наступаючих контрреволюційних збройних сил Директорії. Під такими гаслами червоні загони розпочали бойові дії у Ялті, Євпаторії, Керчі [2].

За рахунок чисельної переваги у військовій силі у Криму була встановлена Радянська влада. 22 січня 1918 року спеціальною декларацією Раднарком розпустив Курултай [5]. Згодом, на конференції рад робітничих та солдатських депутатів та військово-революційних комітетів Таврійської губернії, яка відбулась 28-30 січня 1918 року, було ухвалено кінцеве рішення щодо розпуску Курултаю, як такого що «не висловлює волю кримського народу» [2].

Другий етап охоплює нетривалі періоди перебування більшовиків на Кримському півострові у влади (січень-лютий та березень – квітень 1918 р.) і характеризуються активною дискредитацією обраної Курултаєм форми політичного устрою та його позиції у розподілі землі. Так, запропонована Курултаєм форма влади на півострові у вигляді парламентської республіки більшовиками трактується, як диктатура буржуазії з відповідним збереженням всіх політичних та економічних важелів впливу за кримськотатарською і російською буржуазією та створення лише видимості прав і свобод для простого народу [1; 3].

Наступне питання, що «не захотів» вирішувати Курултай на користь татарських селян пов’язане з землею. Позиція Курултаю про те, що земельне та інші питання можуть бути вирішенні лише після скликання кримських установчих зборів використовувалась більшовиками, з одного боку для звинувачення татарського уряду у недієздатності, захисті інтересів поміщиків та небажанні опікуватись потребами народу, а з іншого, для насаджування серед кримської інтелігенції думки про контрреволюційну сутність партії Міллі-Фірка [3].

У 1919 р. більшовики демонструють кардинальні зміни у власному ставленні до національного питання. Протягом існування Кримської Ра-

дянської Соціалістичної Республіки (травень – червень 1919 р.) відбувається активне залучення кримських татар до процесу державотворення. Зокрема, у новоствореному уряді вони обіймали посади комісарів (очільників) внутрішніх справ, юстиції, освіти, іноземних справ. Звучать неодноразові гучні заяви від перших осіб уряду радянської Росії про можливість відтворення автономної Кримської держави [2].

Розкол, який відбувся наприкінці 1918 – початку 1919 рр. у лавах партії Міллі-Фірка був використаний більшовиками на свою користь. Спокусившись привабливими обіцянками щодо можливості відтворення кримської держави частина її членів вийшла зі складу Курултаю, вступила до більшовицької партії і утворила там мусульманську секцію. Враховуючи популярність партії вона була офіційно легалізована більшовицьким урядом і навіть отримала дозвіл на випуск власної газети «Єні-Дун'я» [*2*].

Однак, попри зазначені кроки, уряд радянської Росії лише демонстрував підтримку національних меншин, але надавати реальну владу не мав наміру, про що свідчить наступне. Головою Кримського Раднаркому був призначений росіянин за походженням, а не представник від мусульманської організації Криму. Робота всіх мусульманських секцій проводилась під безпосереднім наглядом більшовиків та полягала лише у пропаганді і агітації серед мусульман.

На третьому етапі (листопад 1920 р. – листопад 1927 р.) який розпочався після остаточного укорінення Радянської влади в Криму, продовжується робота з дискредитації досягнень Курултаю шляхом подання у негативному ракурсі політичної лінії, яку проводила партія Міллі-Фірка під час окупації Криму військами Німеччини, Добровольчої армії, Антанти та звинуваченнях у спробах політичної реабілітації контреволюційного національно-буржуазного минулого партії і відродженні націоналізму в галузі освіти [3].

Намір створення у 1918 р. партією Міллі-Фірка в Криму незалежного ханства під протекторатом Німеччини і Туреччини та подальше зближення з Українською Радою були розцінені, як намір повернути старі порядки за яких буржуазія мала необмежені права і можливості. Спроба призупинення самовільного захоплення земель селянами, участь членів партії Міллі-Фірка мілліфарківців у боротьбі з комуністами використовувалась для демонстрації антинародної сутності партії.

Упереджено оцінюється більшовиками, як робота Міллі-Фірка з підготовки проекту Національно-культурної автономії Криму, так і переслідування, яких вона зазнала від командування Добровольчої армії А. Денікіна. Основні положення вказаного проекту щодо поширення автономного управління кримських мусульман на релігійні, судові, культурно-просвітницькі і опікунські справи, на питання народної освіти, самообслуговування, управління вакуфним майном та капіталами, а також за-

провадження татарського національного парламенту (Меджеліс-Мебусан) і національного уряду (Директорія) трактувались, як форма буржуазного державного устрою, що забезпечує самостійність та необмежені права буржуазії на Кримському півострові. Переслідування членів партії кримських татар були розцінені, як такі, що мали декларативний характер і здійснювались про всяк випадок.

Намагання членів партії Міллі-Фірка, навесні 1919 р., зупинити громадянську війну шляхом заклику до необхідності забезпечення розвитку виробничих сил, відмови від політики догоджання певним класовим елементам більшовицький уряд використовує для розкриття буржуазної сутності ідеології партії та звинувачення у прийнятій позакласовій позиції. Остання, стверджували більшовики, є лише ширмою, насправді партія продовжує закликати до боротьби з червоними повстанцями та відстоювати недоторканість панської землі.

Після закінчення Громадянської війни в Криму лідери національної партії кримських татар Чобан-Заде, Озенбашлі та багато її членів починають працювати у Народному комісаріаті просвіти Кримської радянської Соціалістичної республіки. Виступи проти введення нового латинізованого алфавіту, підготовка аполітичних шкільних підручників, залучення до їх написання національно свідомих кримських татар, підтримка вимоги шкільних вчителів до створення татарського видавництва, публікації в газетах і журналах радянського Криму історії Міллі-Фірка та заклики татарської молоді і інтелігенції до культурного будівництва були визнані, як антирадянські і сприяли порушенню, у 1927 р. кримінальної справи проти Міллі-Фірка, як контрреволюційної організації. [3]. За її результатами у 1928 р. було засуджено 58 осіб, 11 з яких були розстріляні [6].

Таким чином, радянська Росія, використовуючи власний інформаційний ресурс, здійснювала цілеспрямоване формування у суспільній свідомості населення Кримського півострова викривленого уявлення про діяльність Першого Курултаю кримськотатарського народу та національної партії кримських татар «Міллі-Фірка». Дискредитація проводилась поетапно. Спочатку акцентувалась увага на окремих, зручних владі епізодах їх діяльності; потім – висувались звинувачення у небажанні вирішувати актуальні для більшості населення півострова питання; в подальшому проводилось висвітлення лише у негативному ракурсі діяльності партії за часів окупації Криму і на закінчення – оголошено звинувачення у контрреволюційній діяльності.

**Література**

1. Атлас М. Л. Борьба за Советы. Очерки по истории Советов в Крыму 1917–1918 гг. / М. Л. Атлас. – Крымиздат, 1933. – 144 с.

2. Бикова Т.Б. Створення Кримської АСРР (1917–1921 рр.) : моногр. / Т. Б. Бикова. – К., 2011. – 246 с.

3. Бочагов А.К. Милли-Фирка. Национально-буржуазная контрреволюция в Крыму / А.К. Богачов. – Симферополь, 1932. – 129 с.

4. Горбань Т. Крим в революційних процесах 1917-1920 рр.: історіографія проблеми / Т. Горбань // Наукові записки. Збірник. К.: Пі ЕНД, 2003. – С. 17–54.

5. Пащеня В.Н. Этнонациональное развитие в Крыму в первой половине XX века (1900-1945 гг.) : моногр. / В.Н. Пащеня. – Симферополь, 2008. – 288 с.

6. Семена Н. Дело Вели Ибрагимова и «Милли Фирка» / Н.Семена // «Зеркало недели, Украина» от 19.03.1999. [Електронний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/ Милли_Фирка #cite_ref-Семена_6-1.

*УДК 342.9*

**Білан М.В.**
студент 3-го курсу
ННІ ІБ Національної академії СБ України
**Тугарова О.К.**
кандидат юридичних наук, доцент
Національна академія СБ України

## ОСНОВНІ НАПРЯМИ РЕФОРМУВАННЯ ІНФОРМАЦІЙНОГО ЗАКОНОДАВСТВА УКРАЇНИ

Аналіз нормативно-правового поля України засвідчує, що в нашій державі є низка законодавчих та інших нормативно-правових актів спрямованих на регулювання, захист та розвиток вітчизняного інформаційного простору. Зовнішня експертиза, яка неодноразово здійснювалася, зокрема представниками ОБСЄ, підтвердила, що законодавча та нормативно-правова база функціонування інформаційної сфери України в цілому відповідає європейським нормам [3]. Тобто можна вести мову про те, що сьогодні в нашій державі вже створено основи такої галузі українського законодавства як інформаційне право.

Поряд з тим, що в Україні прийнято низку нормативно-правових актів на означеному напрямі, важливою проблемою залишається несистемність вітчизняної правової політики в інформаційній сфері, зокрема з огляду на те, що законодавчі акти ухвалюються з метою вирішення тактичних завдань, без урахування стратегічних орієнтирів та об’єктивних українських умов. Окрім того, частина інформаційних відносин регулюється підзаконними, а подекуди й відомчими нормативними актами. Як наслідок, значна кількість питань функціонування інформаційної сфери в Україні залишається досі недостатньо врегульованою на законодавчому рівні – це стосується як проблем інфраструктури, так і діяльності ЗМІ, інформаційно-аналітичних установ тощо.

На сьогодні актуальним є питання вдосконалення українського інформаційного законодавства у сфері створення, поширення та використання інформації відповідно до сучасних потреб та викликів. На думку вітчизняних правознавців таке вдосконалення має відбуватися шляхом кодифікації – розробки та прийняття Інформаційного кодексу України (Кодексу України про інформацію).

Варто зауважити, що про необхідність розробки такого кодексу йшлося ще в Указі Президента України «Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 року «Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України». Окрім того, необхідність прийняття Інформаційного кодексу України законодавчо закріплено в «Основних засадах розвитку інформаційного суспільства в Україні на 2007–2015 роки». Отже, впродовж більше ніж десяти останніх років ведуться численні дискусії про необхідність розробки та прийняття Інформаційного кодексу України та про те, яким він має бути [1].

Найбільшого поширення при цьому набули три підходи. Перший підхід був запропонований і розроблявся Державним комітетом телебачення і радіомовлення України, який був заснований на тому, що в основі Інформаційного кодексу має стати «Концепція національної інформаційної політики», а також змінений відповідно до сучасних вимог суспільного розвитку Закон України «Про інформацію».

Другий підхід було розроблено групою фахівців Інституту держави і права ім. В. Корецького. На їх думку Інформаційний кодекс має складатися із чотирьох частин: 1) базова (загальна), яка містила б системоутворюючі норми, що регулюють базові відносини у сфері інформації та інформатизації; 2) галузева частина, яка має регулювати інформаційні відносини в окремих сферах життя особи, держави, суспільства; 3) третя частина має містити видові норми і регулювати інформаційні відносини суб’єктів у сфері створення, пошуку, одержання, використання, зберігання та поширення окремих видів (категорій) інформаційної продукції або в окремих складових інформаційного процесу; 4) частина щодо спеціальних норм, яка регулює відносини стосовно створення і використання інформаційних технологій та телекомунікаційних систем.

Третій підхід було запропоновано Урядовою комісією з питань інформаційно-аналітичного забезпечення діяльності органів виконавчої влади у проекті «Концепції реформування законодавства України у сфері суспільних інформаційних відносин». Цей підхід передбачав здійснювати систематизацію інформаційного законодавства в три етапи:

1) інкорпорація законодавства – визначення ієрархічної системи та структури інформаційного законодавства на рівні правової доктрини;

2) виокремлення в системі законодавства галузі та її закріплення у Зводі законів України як розділу – «Інформаційне законодавство»;

3) кодифікація – розробка і прийняття Верховною Радою України такого нормативного акту, як Кодекс України про інформацію. При цьому систематизація інформаційного законодавства на думку розробників мала проводитися методом агрегації – удосконалення окремих правових норм чи створення нових міжгалузевих правових інститутів не повинно було порушувати цілісність та призначення інформаційного законодавства, а покращувати його дієвість у цілому [2].

Незважаючи на різні підходи, правознавці наполягають на необхідності розробки та прийняття Інформаційного кодексу України та вважають за необхідне об'єднати в ньому механізми регулювання провідних суспільних відносин, об'єктом яких є інформація незалежно від форми, способу, засобу чи технології її поширення. Такий кодекс має чітко визначити об'єкт, предмети інформаційного права, суб'єкти інформаційних правовідносин, правовий режим доступу до інформації, а також передбачити механізми забезпечення інформаційного суверенітету України та забезпечення інформаційної безпеки громадян, суспільства та держави як складових національної безпеки України.

**Література**

1. Корейба Ю. В. Конституція України як визначальне джерело інформаційного права / Ю. В. Корейба // Підприємництво, господарство і право. – 2013. – № 9. – С. 48-52.

2. В.А Ліпкан Систематизація інформаційного законодавства України: [монографія] / В.А Ліпкан, В.А. Залізняк ; за заг. ред. В.А. Ліпкана. – К.: ФОП О.С. Ліпкан, 2012. – 332 с.

3. Корейба Ю. В. Міжнародний рівень системи джерел інформаційного права України / Ю. В. Корейба // Науковий вісник Херсонського державного університету. – Сер.: Юридичні науки. – 2014. – Вип. 4. – Т. 2. – С. 64-69.

*УДК 340.68+342.5+347.83*

**Богдан Д. М.**
аспірант відділу аспірантури і докторантури
Національна академія СБ України

## ПОШУК ЕФЕКТИВНИХ ШЛЯХІВ ПРОТИДІЇ ІНФОРМАЦІЙНІЙ АГРЕСІЇ РФ ЩОДО УКРАЇНИ

Інформація, засоби масової інформації і комунікації, а також суспільні відносини, що виникають у процесі збору, обробки, зберігання, передачі й поширення інформації створюють безпосередній вплив на політичний, економічний, соціальний і духовний розвиток держав та міжнародної спільноти в цілому. В умовах гібридної війни, яку розв'язала Російська

Федерація проти України, інформація та використання медіа-ресурсів трансформувалися в ефективний інструмент досягнення цілей окремих політичних та олігархічних сил, що прагнуть до світового лідерства.

Інформаційно-технологічна революція генерує принципово нові виклики й загрози життєдіяльності окремих держав та їх альянсів. У найбільш небезпечній формі це виявляється у таких явищах як агресія однієї держави щодо іншої або тероризм, які максимально використовують можливості сучасного інформаційного суспільства. Швидкий розвиток інформаційних технологій суттєво розширює можливості держав-агресорів та терористичних організацій у створенні й широкому застосуванні технологій маніпулювання свідомістю населення держав-мішеней.

Питанням дослідження зовнішнього втручання РФ в інформаційну сферу України та можливостям протидії приділяли увагу науковці: В. Горбулін, Д. Золотухін, В. Ліпкан, А. Марущак, Г. Новіцький, В. Панченко та інші. У наукових працях А. Коростилека, В. Лопатіна, О. Штоквиша та інших переважно розкриті теоретичні засади ведення спеціальних інформаційних операцій. Проте практичні висновки з аналізу вітчизняного досвіду протидії інформаційній агресії РФ щодо України почали формуватися лише останнім часом.

Сьогодні одними з актуальних завдань СБ України з протидії російській агресії в інформаційній сфері є: протидія спеціальним інформаційним операціям і впливам; моніторинг контенту медіапростору з перевіркою поданих фактів на достовірність («фактчекінг»); інформаційна робота з громадянами України та зовнішньою аудиторією шляхом надання об’єктивної інформації про напрями державної політики в усіх сферах життєдіяльності суспільства, офіційної позиції щодо значущих подій усередині країни і за кордоном, висвітлення діяльності органів державної влади; оприлюднення доказів присутності збройних формувань РФ на території України та дискредитація діяльності іррегулярних незаконних збройних формувань, озброєних банд та груп найманців, створених та фінансованих РФ; розширення каналів і підвищення якості інформування зарубіжної громадськості.

На основі аналізу заходів, що вживають контррозвідувальні підрозділи СБ України для протидії агресії РФ в інформаційній сфері виокремлені найбільш ефективні з них. Крім того, запропоновані деякі нові шляхи протидії, що у подальшому можуть показати свою ефективність.

Найменш ефективними на нашу думку є інформаційні заходи, що вживаються тільки після актів зовнішньої інформаційної агресії і не передбачають активної запобіжної діяльності, а також радикальні («репресивні») заходи.

Зокрема, блокування операторами мереж кабельного телебачення російських радіо-, телеканалів (Первый канал, Звезда, LifeNews) спонукає до альтернативи – наземного (особливо у прикордонних районах), супутни-

кового та інтерактивного (IPTV) телебачення. Реакцією громадян (особливо молоді) на блокування інтернет-провайдерами доступу до російських сайтів («Яндекс», «ВКонтакте» тощо) стало використання сайтів-анонімайзерів, браузера Tor або встановлення на гаджети програмного забезпечення для організації VPN-серверу, що забезпечує високу приватність обміну інформацією. Водночас поширення російської пропаганди продовжується у соціальних мережах «Facebook», «Twitter». Заборона в'їзду на територію України та видворення за межі України журналістів – часто не залишаються поза увагою європейських та міжнародних правозахисних організацій й, в окремих випадках, розцінюється останніми як наступ на свободу слова. Цілком погоджуємося з висновками експертів, що фактчекінг також не є ефективним й не зможе бути наступальним, оскільки його робота спрямована на ті наративи та новини, які вже існують. Тобто щоразу використовуючи методики розвінчування фейків, нам необхідно переконувати людей у тому, що їхні вірування є хибними. При цьому ми все одно говоримо про нав'язані нам наративи, а отже РФ зможе безкінечно формувати наш порядок денний [2].

Водночас свою ефективність довели наступні шляхи протидії російській інформаційній агресії: розбудова інформаційної інфраструктури та національного інформаційно-культурного простору (творці, канали комунікації, споживачі, регуляторні структури) з високими якісними характеристиками; розвиток регіональних ЗМІ, що розміщують контент на території Донецької та Луганської областей, та стажування регіональних журналістів на медіа-курсах в європейських державах; використання за єдиним замислом патріотичного ресурсу (працівників недержавних організацій, блогерів, хакерів-аматорів) для формування суспільної думки в інтернет-просторі – через соціальні мережі, форуми, блоги; використання можливостей інформаційних агентств («УНІАН», «Укрінформ») як платформ для медійного спілкування; формування пильності, морально-психологічної стійкості, згуртованості та навчання населення правилами поведінки в умовах зростання терористичної загрози.

Основним напрямом подальших наукових розробок є дослідження нових методів запобігання зовнішнім інформаційним загрозам.

**Література**

1. Сірик А. О., Озеров С. В. Напрями протидії інформаційним заходам під час російської агресії на території України // Збірник наукових праць Харківського університету Повітряних Сил, № 4(45), 2015. С. 43-46.

2. Золотухін Д. Ю. Протидія інформаційній агресії Росії на рівні законодавчих актів: Резолюція Європарламенту. Аналіз. URL: http://detector.media/infospace/article/121555/2016-12-18-protidiya-informatsiinii-agresii-rosii-na-rivni-zakonodavchikh-aktiv-rezolyutsiya-evroparlamentu-analiz/ (дата звернення 01.03.2018).

*УДК 342.9*
**Бондарчук Б.О.**
студент 3-го курсу
ННІ ІБ Національної академії СБ України
**Гоц О.В.**
Національної академії СБ України

# УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ РЕСУРСАМИ КНИЖКОВОЇ ПАЛАТИ УКРАЇНИ ІМЕНІ ІВАНА ФЕДОРОВА

Книжкова палата України імені Івана Федорова – це наукова неприбуткова установа у сфері видавничої справи та інформаційної діяльності, заснована на загальнодержавній власності і підпорядкована Державному комітету телебачення і радіомовлення України, яка керується у своїй діяльності законодавчими та нормативними актами України, наказами Державного комітету телебачення і радіомовлення України та Статутом.

Одним із основних завдань Книжкової палати – управління інформацією, яку слід вирішувати в двох аспектах: по-перше, усередині установи має бути покращене управління наявними інформаційними ресурсами з метою підвищення продуктивності, ефективності та якості надання послуг; по-друге – у зовнішній сфері потрібно розуміти інформаційні потреби найрізноманітніших користувачів (клієнтів) і відповідним чином регулювати управління інформацією, удосконалюючи способи обслуговування їхніх специфічних потреб.

Управління інформацією пов’язане з плануванням, організацією, реалізацією і контролем інформаційних ресурсів, до яких входять інформаційні фонди (змістовні комплекси), інформаційні системи, інформаційна інфраструктура та інформаційні процеси, що їх супроводжують.

Комп’ютерна мережа Книжкової палати України належить до класу мереж з розгалуженою структурою. Її основу створено в 1996 році, а протягом наступних років відбувалося розширення і модернізація. Серцем мережі є сервер, від якого, як кровеносні судини, тягнуться гілки до всіх відділів Книжкової палати.

Користувачі локальної мережі мають змогу не лише працювати над поповненням інформаційних ресурсів Книжкової палати, а й отримувати інформацію з інформаційно-довідкового серверу Internet, що містить добірку загальнодержавних і внутрішніх нормативних документів, інші документи, необхідні в роботі Палати. Окремий сервер "Ліга-Закон", що створює ще одну гілку мережі, містить повну базу законодавства України і забезпечує працівників Палати відомостями про найновіші зміни в ньому.

Інформаційні ресурси Книжкової палати знаходяться у постійному розвитку, а інформаційне обслуговування набуває нові форми. В процесі

розроблення знаходиться ряд проектів, що висуває Книжкову палату України в число провідних інформаційних провайдерів нової видавничої системи України. Серед цих проектів є декілька з установами й фірмами Сполучених Штатів Америки. Сучасні інформаційні технології складають матеріальну основу формування зв'язків і виробничих відносин між підприємствами – елементами видавничої системи, сприяючи їхній консолідації.

Основними «елементами» та «дійовими особами» інформаційного ринку є розповсюджувачі інформації, тобто посередники між постачальниками інформації й інформаційними службами та споживачами інформації; потім йдуть користувачі інформаційних послуг; далі допоміжні служби.

Створення інформаційних систем ставить за мету обмін інформацією між потенційними джерелами і користувачами. Інформаційними бар'єрами на цьому шляху є: різниця рівнів знань джерела інформації і споживача, мовні перешкоди, відсутність навичок інформаційного пошуку. Але головним є віддалення користувачів від джерел засобів масової інформації у часі та просторі.

Вплив часового бар'єру зводиться до мінімуму шляхом фіксації повідомлення на будь-якому носії з його подальшим відтворенням. Усе, що встигло створити людство, чого спромоглось досягти й придумати – зберігається на сторінках книг та рукописів. Збереження і розповсюдження людських знань у різні куточки всіх країн світу на різноманітних носіях інформації роблять їх доступними величезній кількості користувачів.

Взаємний зв'язок інформаційних систем між собою дає змогу в принципі надавати кожному споживачу всі знання, створені людським генієм. Але економічні міркування роблять нереальною можливість доступу кожної людини до зафіксованих на носіях знань суспільства. Сховища інформації неминуче будуть обмежені за тематикою і за обсягом вибіркового комплектування. Тому звернення до всього обсягу людських знань можливе тільки за наявності зв'язків з іншими фондами й інформаційними системами, що мають можливість передавати повідомлення, які вони зберігають.

Інформаційні технології, що з'явилися разом з комп'ютерами і засобами комунікації, уможливлюють подолання просторових перешкод під час передавання різних інформативних повідомлень. Проте існує проблема розповсюдження інформації, зафіксованої на паперових носіях, розв'язати яку можна тільки за допомогою створення цифрових бібліотек.

Для вирішення питання ефективного управління інформацією потрібні відповідні бази даних бібліографічної і повнотекстової інформації. Тому першочергове завдання - створення повного електронного каталогу книг і брошур, що зберігаються в Державному архіві друку Палати, і ор-

ганізація доступу до нього з бібліотек та інформаційних центрів. Цей фонд налічує майже 900 тисяч назв. Сьогодні створено службові електронні каталоги книг і брошур, що надійшли до архіву з 1991 року. Каталоги містять бібліографічну інформацію про понад 240 тисяч видань. Виконавши комплекс робіт із ретроконверсії хронологічного каталогу книг і брошур, можна забезпечити ефективний доступ до джерел інформації Палати.

Реєстрація та збирання друкованих праць має величезне наукове й культурне значення для загального поширення знань й поглиблення освіти, науки та культури. І це сьогодні визнано в усіх цивілізованих країнах світу. Нині немає держави, яка б не реєструвала твори власного друку і не видавала б літописів національної бібліографії.

**Література**

1. Гуцол Г. Новітні розробки у галузі інформатизації Книжкової палати України// Вісник Книжкової палати. – 2006. – № 4. – С. 29-34.

2. Нелепина Г. Книжная палата Украины:История создания, проблемы и перспективы развития // Книжное обозрение. – 1999. – № 3. – С. 11-13.

3. Сенченко М. Книжкова палата України: вчора, сьогодні, завтра// Вісник Книжкової палати. - 2004. - № 1.(До 85-річчя з дня заснування Книжкової палати України. – С. 3-7.

4. Сайт Книжкової палати України // http://www.ukrbook.net.

*УДК 32.019.51*

**Гаврилюк К.І.**
Національна академія СБ України

## ПОНЯТТЯ ТА РОЛЬ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ У СФЕРІ ПУБЛІЧНОЇ ДИПЛОМАТІЇ США

За останні десятиріччя масштаби діяльності міжнародного тероризму постійно зростають. Зростає не тільки кількість скоєних терористичних актів, а й найважчі їх наслідки – жертви. Це спонукає усе більшу кількість країн до розробки власних національних антитерористичних систем. У більшості країн були сформовані спеціальні антитерористичні організації, які можуть кооперуватись з іншими державними відомствами з метою недопущення пропаганди та розповсюдження тероризму та, як наслідок, терактів.

Боротьба з тероризмом до недавнього часу залишалась внутрішньодержавним питанням та полягала, здебільшого, у виявленні вже сформованих терористичних груп (організацій, окремих терористів-одинаків) та їх

ліквідації (нерідко в рамках проведення антитерористичної операції після або під час скоєння терористичного акту). Проте, як показують реалії сьогодення, такі дії з боку держави та органів боротьби з тероризмом не можуть забезпечити достатній рівень антитерористичної безпеки, а тим паче забезпечити недопущення подальшого розширення діяльності вже існуючих терористичних організацій або створення нових.

Як одним з головних елементів недопущення створення терористичних організацій, радикалізації окремих груп населення та для інформування суспільства про рівні терористичної небезпеки, Указом Президентом США Б. Обамою у 2011 році вперше законодавчо закріплюється концепція стратегічних комунікацій. Цим Указом була затверджена розробка комплексної ініціативи зі стратегічних комунікацій, націленої на боротьбу з проявами тероризму як на території США, так і за її межами. Оскільки цей Указ був прийнятий у відповідь на зростаючі терористичні загрози, насамперед в середині США, то й терористична загроза поставала в особі Аль-Каїди.

Стратегічна комунікація (англ. - strategic communication) являє собою комплекс заходів, які реалізуються Міністерством оборони та іншими державними органами Сполучених Штатів Америки з метою інформаційного впливу на зарубіжне суспільство. [1]

У більш широкому розумінні «стратегічні комунікації» полягають у цілеспрямованому впливі органів державної влади США на інформаційне суспільство (таке суспільство, в якому інформація і знання продукуються в єдиному інформаційному просторі [2]) з метою створення та забезпечення сприятливих умов для реалізації зовнішньої політики. Проте не слід ототожнювати стратегічні комунікації із односторонніми формами впливу на аудиторію. Основна відмінність полягає у тому, що стратегічні комунікації мають діалоговий характер, тобто забезпечують двосторонній обмін інформацією, в той час як традиційний односторонній вплив спрямований лише на її поширення.

Стратегічні комунікації спрямовані, насамперед, на протидію ідеології тероризму та екстремізму шляхом розповсюдження та обміну інформацією, яка покликана позитивно впливати на елементи населення, сприятливого до радикалізації, вербування терористичними організаціями та схильного до сугестивності (здатність швидко та легко піддаватися чужому впливові [3]).

З метою координації та здійснення зовнішньої політики США у сфері стратегічних комунікацій був створений Центр стратегічних антитерористичних комунікацій (Center for Strategic Counterterrorism Communications). Головною метою діяльності CSCC визначається координація, направлення та інформування уряду США про всю діяльність активних громадських комунікацій, спрямованих на закордонну аудиторію і орієнтованих на бо-

ротьбу з проявами екстремізму та терористичної діяльності. Проте окрім зовнішньодержавного впливу CSCC також здійснює аналіз, оцінку та функції з планування антитерористичної боротьби разом з Національним центром по боротьбі з тероризмом [4].

З метою конкретизації практичного застосування стратегічних комунікацій у сфері публічної дипломатії США, а також у світлі постійного розповсюдження та мінливості терористичної загрози Президентом США Б. Обамою 14 березня 2016 року був підписаний новий Указ.

Для координації дій урядових організацій у сфері комунікаційної діяльності спрямованої на іноземні аудиторії для попередження та зменшення впливу міжнародних терористичних організацій (ІДІЛ, Аль-Каїда та інших агресивно налаштованих іноземних екстремістських угрупувань) був заснований Центр міжнародної співучасті (Global Engagement Center) [5].

Підсумовуючи все вищевикладене, ми приходимо до висновку, що метою публічної дипломатії США є підтримка досягнення державою зовнішньополітичних цілей та задач, просування національних інтересів та укріплення національної безпеки шляхом інформування та впливу на міжнародне суспільство, а також шляхом розширення та укріплення відносин між суспільством, Урядом Сполучених Штатів Америки та громадянами інших країн [6].

Використання Сполученими Штатами стратегічних комунікацій у сфері публічної дипломатії показує, що отриманий досвід є вкрай важливим для використання в Україні. Окрім зміцнення та налагодження зовнішніх відносин публічна дипломатія України спрямовуватиметься і на забезпечення антитерористичної безпеки шляхом використання стратегічних комунікацій.

**Література**

1. Стратегическая коммуникация. URL: https://ru.wikipedia.org/wiki/Стратегическая_коммуникация (дата звернення 03.03.2018).

2. От информационного общества – к обществам знания. ЮНЕСКО // Всемирный саммит по информационному обществу: Информационное издание/ Сост.Е.И. Кузьмин, В.Р. Фирсов. – СПб., 2004. – С. 82-84.

3. Словник української мови : в 11 томах. – Т.9. – 1978. – С. 820.

4. Center for Strategic Counterterrorism Communications. URL: https://2009-2017.state.gov/documents/organization/116709.pdf (дата звернення 05.03.2018).

5. Global Engagement Center. URL: https://www.state.gov/r/gec/ (дата звернення 03.03.2018).

6. Under Secretary for Public Diplomacy and Public Affairs. URL: https://www.state.gov/r/index.htm (дата звернення 05.03.2018).

*УДК 004.58 / 316.776*
**Давидюк А.В.**
ІСЗЗІ НТУУ «КПІ ім. І. Сікорського»
**Петрик В.М.**
кандидат наук з державного управління, доцент
ІСЗЗІ НТУУ «КПІ ім. І. Сікорського»

# ПРОТИДІЯ АВТОМАТИЗОВАНИМ ЗАСОБАМ ВИКОРИСТАННЯ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

В наш час проблема захисту інформаційних ресурсів є надзвичайно актуальною, що зумовлено наявністю гібридної війни на теренах нашої держави, конкуренцією в бізнесі, цінністю конфіденційних даних громадян.

З точки зору спеціалістів з інформаційної безпеки найуразливішим місцем будь-якої системи є людина, помилки якої можуть бути вдало використані при досягненні мети зловмисника.

Разом з тим змінюється і підхід зловмисників, атаки яких називають APT (Advanced persistent threat) [1].

Основою таких атак найчастіше є методи соціальної інженерії, що забезпечують більш швидкий та менш затратний за ресурсами несанкціонований доступ до цільових інформаційних ресурсів.

В контексті захисту від засобів соціальної інженерії, спрямованих на маніпулювання людиною з метою отримання певної вигоди, створення методів захисту є досить не простою задачею, що потребує негайного вирішення.

Одним з рішень даної задачі є періодичне проведення аудиту з застосуванням засобів соціальної інженерії, що має на меті виявлення слабких місць політики інформаційної безпеки організації, співробітників, що порушують дану політику чи мають неналежну компетенцію для виконання службових обов'язків [2].

Звісно, даний метод має достатньо переваг, проте не є дешевим для власника компанії, тому не кожна організація може собі це дозволити. Також не простою є задача пошуку спеціалістів для проведення такого роду аудиту.

Бюджетним варіантом для широкого загалу є безкоштовний продукт Social-Engineer Toolkit (SET), доступний у дистрибутиві Kali Linux. Даний програмний засіб дає змогу рядовому користувачеві в автоматизованому режимі виконати прості атаки з застосуванням соціальної інженерії. До переліку можливостей даного за стосунку можемо віднести: виконання масової email атаки, створення формату файлу з навантаженням, застосування наступних методів атак: метод атаки з Java апплетом, метод екс-

плойта для браузера Metasploit, метод атаки збору облікових даних, метод атаки Tabnabbing, метод атаки Web Jacking, метод множинних веб атак, метод атаки повного екрану, метод атаки з HTA та інші [3].

Даний функціонал може бути використаний при проведенні зовнішнього або внутрішнього аудиту на етапі тесту на проникнення. Проте не варто забувати, що ці ж засоби одночасно є досить небезпечною зброєю зловмисника, від якої важко вберегтись. Доцільним є зосередитись на досягненні високого рівня підготовки персоналу, що значно зменшить вплив наслідків проведення атак зловмисником на безперервність бізнес процесів організації.

В ході дослідження даної проблеми для підвищення кваліфікації співробітників пропонується алгоритм протидії автоматизованим засобам соціальної інженерії.

Даний алгоритм включає наступні кроки:

1. Визначення пріоритетних інформаційних ресурсів, наслідки від втрати яких є найбільшими.

2. Проведення перевірок співробітників, діяльність яких пов’язана з даними ресурсами, використанням засобів соціальної інженерії на базі Kali Linux.

3. Формування звіту про успішність застосування вище вказаних засобів.

4. Перегляд політики безпеки організації з внесенням відповідних змін (у разі виявлення проблем на попередньому кроці).

5. Проведення занять з персоналом з врахуванням особливостей внутрішнього та зовнішнього контексту організації.

6. Регулярне повторення починаючи з другого кроку даного алгоритму.

Даний алгоритм не є вирішенням всіх можливих проблем інформаційної безпеки, проте в поєднанні з методиками менеджменту ризиків та вразливостей інформаційних систем є корисним інструментом для підвищення рівня інформаційної безпеки організації уцілому.

**Література**

1. Rouse, M. (2010). What is advanced persistent threat (APT)? – Definition from WhatIs.com. SearchSecurity. URL: http://searchsecurity.techtarget.com/definition /advanced-persistent-threat-APT (дата звернення 28. 02. 2018).

2. Konopasek, K. (2014). Social Engineering Audit & Security Awareness. Slideshare.net. URL: https://www.slideshare.net/CBIZinc/social-engineering-audit-security-awareness (дата звернення 28. 02. 2018).

3. Security Through Education. (2018). Social Engineer Toolkit (SET) – Security Through Education. URL: https://www.social-engineer.org/framework/se- tools/computer-based/social-engineer-toolkit-set/ (дата звернення 28. 02. 2018).

*УДК 327.5:316.776.23*
**Даценко А.Ю.**
аспірант
Національний інститут стратегічних досліджень

# БОРОТЬБА З РОСІЙСЬКОЮ ДЕЗІНФОРМАЦІЄЮ ЯК НАПРЯМ ЗАХИСТУ ІНФОРМАЦІЙНОГО ПРОСТОРУ УКРАЇНИ В УМОВАХ «ГІБРИДНОЇ ВІЙНИ»

Проведення правлячою елітою Російської Федерації агресивної пропаганди, дезінформаційних кампаній та кібератак є основним інструментом впливу на інформаційний простір України в умовах розв'язаної РФ в 2014 р. «гібридної війни» проти України та її західних союзників. Саме тому протистояння пропаганді РФ є актуальним як у близько строковій, так і середньостроковій перспективі.

Використання дезінформації як засобу інформаційної війни відрізняється від традиційних форм пропаганди. Завдання тут полягає не в тому, щоб переконати чи схилити на свій бік певну цільову аудиторію, а в тому, щоб підірвати чи зруйнувати світоглядні засади цієї аудиторії, її ідентичність. Замість того, щоб агітувати певну аудиторію, дезінформатори прагнуть тримати її «на гачку своїх меседжів», відволікати її увагу, робити її пасивною, зневіреною.

Російську дезінформацію її організатори поширюють як відкритим шляхом – за допомогою радіо й телебачення та різноманітних онлайнових засобів різними мовами (SputnikNews, RussiaToday, NovorossiaToday тощо), так і прихованим способом, використовуючи номінально незалежних журналістів, експертів і коментаторів (у багатьох з яких за межами Росії немає відповідного легітимного статусу чи авторитету) та інтернет-тролів (платних онлайнових пропагандистів, які зазвичай розміщують свої «пости» у соціальних мережах).

На основі аналізу контенту ЗМІ Росії можна виділили такі типові меседжи пропаганди щодо України [1]:

– реформи в Україні провалились або йдуть дуже повільні;
– рівень корупції в Україні нині навіть вищій, ніж був за часів президентства Януковича;
– євроінтеграція провалилася, Україна Європі не потрібна, її використовують у своїх меркантильних інтересах;
– в Україні, яку захопили праві радикали, панує фашистська ідеологія;
– якби Крим та Донбас своєчасно не вийшли з-під впливу України, їхнє населення стало би жертвою правих радикалів;
– Україна відповідальна за невиконання Мінських угод;
– прийняття нового закону про реінтеграцію Донбасу перекреслює Мінські угоди.

Дезінформаційну кампанію проти України Росія проводить за допомогою різноманітних методів, адаптуючи меседжі під різні цільові аудиторії. Нахабно поширюючи дезінформацію, керівництво російської пропагандистської машини водночас намагається діяти в популярному нині й на Заході стилі «постправди»: брехня має бути розважальною та емоційно привабливою; неправду слід подавати з використанням найкращих прийомів переконувальної риторики з врахуванням упереджень та установок конкретних аудиторій. Щоб привернути увагу до подібного контенту, дезінформатори з Росія готові фабрикувати історії з використанням фото- й відеоматеріалів для своїх потреб. Ціла низка ЗМІ – від кіно до новин, ток-шоу, друкованих медіа та соціальних мереж – займається просуванням такого комплексу офіційних російських установок.

На думку іноземних фахівців, характерними особливостями російської пропаганди є величезні обсяги дезінформації, швидкість надання та постійне її повторювання, відсутність логіки і байдужість до реальності. Автори доповіді «Брандспойт брехні» – модель російської пропаганди» [2] визнають: «Протистояти російській пропаганді – непросте завдання. Вирішити його шляхом заборони окремого ЗМІ чи зняття з онлайну окремого повідомлення неможливо. Величезний об'єм пропагандистських повідомлень і використання для їхньої трансляції багатьох каналів робить пропаганду не тільки ефективною, а також менш вразливою. Спростування потребує багатьох зусиль, отже, пропаганда може бути знівельована, лише у разі, якщо аудиторія отримає правдиву інформацію раніше, ніж брехню». Тому автори згаданої доповіді вважають за потрібне діяти «на випередження», а саме: постійно попереджати про можливість дезінформації; повторювати спростування; надавати факти для розуміння ситуації, які знадобляться після того, як будуть спростовані брехливі тези.

Європейські організації (Європейське агентство з протидії кремлівським дезінформаційним кампаніям – «EU East StratCom Task Force»; словацький аналітичний центр The European Values та ін.), визначаючи головною метою захист ліберальної демократії, пропонують такі напрями протидії російській дезінформації:

1. Протидія дезінформації має бути пріоритетом у формуванні зовнішньої та внутрішньої політики, а також в питаннях безпеки.

2. Публічно ставити під сумнів і відкидати пропагандистські заяви прокремлівських політиків і публічних осіб.

3. Розкривати кампанії з дезінформації, їхню суть та канали поширення.

4. Систематично підвищувати стійкість до пропаганди та дезінформації у суспільстві.

Саме в контексті реалізації останнього напряму пропонується вжити ряд заходів, спрямованих на посилення «імунітету» («опірності») вітчизняного інформаційного простору до дезінформаційних впливів російського агресора.

Передусім корисно в процесі медіа-моніторингу надавати рейтинги російським медіа за частотою й ступенем потенційної впливовості дезінформації, присутньої у їх новинних повідомленнях, розважальних сюжетах політичного спрямування (ток-шоу тощо). Подібний перелік, у якому медіа були б розташовані за ступенем їхньої доброчесності чи недоброчесності й точністю чи неточністю подачі інформації з присвоєнням тому або іншому медіа відповідного рейтингу дозволив би більш цілеспрямовано чинити тиск на прокремлівські ЗМІ з боку української медіа спільноти та вповноважених органів влади. У свою чергу такий захід дозволив би вплинути на поліпшення контрпропагандистського контенту, більш ефективно шукати й отримувати фінансову допомогу від донорів (грантодавців) для створення нового контенту.

В Україні необхідно також провести послідовну роз'яснювальну кампанію, спрямовану на пояснення широкому загалу, яким чином рекламодавці й продакшн-компанії безпосередньо підживлюють ЗМІ, які розповсюджують ворожу дезінформацію, купуючи у російського «партнера» ті або інші розважальні формати.

Зазначене вище дозволить уникнути «голого адміністрування» й розробити та реалізувати більш ефективні механізми медіа-контролю з боку Національної ради з питань телебачення і радіомовлення, Міністерства інформаційної політики, Міністерства культури, Служби безпеки України.

З одного боку, такий механізм має передбачити заохочення та публічне схвалення ЗМІ, які є зразковими у подачі об'єктивних новин, що, у свою чергу, має бути позитивним сигналом для заохочення потенційних донорів та рекламодавців.

З іншого боку, пропонований механізм «м'якої» протидії ворожій пропаганді та дезінформації створить запобіжники для незаангажованих ЗМІ, які дозволять їм своєчасно уникати тиску пропаганди ворога або проросійськи налаштованих впливових осіб з України. Передусім йдеться про ефективний захист журналістів, яким в умовах «гібридної війни» можуть погрожувати фізичною розправою та яких можуть тролити в кіберпросторі. Вони передусім мають бути захищені органами національної безпеки та кіберполіцією, що в цілому позначиться на більш безпечних умовах роботи вітчизняних медіа.

**Література**

1. Журналістика vs міфотворчість: хто і що формує імідж України в Європі. URL:https://mind.ua/openmind/20172752-zhurnalistika-vs-mifotvorchist-hto-i-shcho-formue-imidzh-ukrayini-v-evropi (дата звернення 28.02.2018).

2. Christopher Paul and Miriam Matthews. The Russian "Firehose of Falsehood" Propaganda Model. URL:https://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/ RAND_PE198.pdf (дата звернення 28.02.2018).

*УДК 351.746.1*
**Думанська В.О.**
Навчально-науковий інститут інформаційної безпеки
Національної академії Служби безпеки України

# НЕДОСКОНАЛІСТЬ НОРМАТИВНО-ПРАВОВОЇ БАЗИ У СФЕРІ КІБЕРБЕЗПЕКИ

Інформаційна безпека є однією із суттєвих складових частин національної безпеки країни. З розвитком і вдосконаленням глобальних комунікаційних мереж, комп'ютерного забезпечення відбувається і еволюція кримінального середовища як окремо взятої держави, так і всього світового співтовариства в цілому. Більш того, під впливом сучасних глобалізаційних процесів, інформаційна безпека набуває відносно самостійного наднаціонального характеру.

*Актуальність* обраної теми полягає у тому, що сутність кіберзлочинності висуває особливі вимоги до стратегії і тактики формування виваженої державної політики забезпечення інформаційної безпеки, яка повинна передбачати систему заходів державного та міжнародного характеру, належне місце в якому займатиме протидія кіберзлочинності. . Кіберзлочинність не обмежується рамками злочинів вчинених у глобальній інформаційній мережі Інтернет, вона поширюється на всі види злочинів вчинених в інформаційно-телекомунікаційній сфері, де інформація може виступати предметом злочинних посягань, середовищем, в якому відбуваються правопорушення і або знаряддям злочину.

*Метою* статті є дослідження причин недосконалості нормативно-правової бази у сфері кібербезпеки та шляхи її вдосконалення.

Відповідно до мети визначено *завдання*: розглянути документи, що охоплюють проблеми забезпечення кібербезпеки держави; розглянути проблеми, що ускладнюють боротьбу проти злочинів в кіберсфері; провести аналіз можливих заходів покращення регулювання кібербезпеки в Україні.

Чинна вітчизняна нормативно-правова база у сфері протидії злочинам в кіберпросторі лише частково задовольняє потреби часу та не завжди охоплює всі ключові елементи, які необхідні для ефективної протидії кіберзлочинам всіх рівнів складності. На сьогоднішній день в Україні діє низка Законів України та нормативних документів різних рівнів, що охоплюють проблеми забезпечення кібербезпеки держави.Це, зокрема, Закони України, «Про інформацію», «Про державну таємницю», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основи національної безпеки України». Крім того в межах даної проблеми діє два стратегічних документа: Стратегія національної безпеки України та Докт-

рина інформаційної безпеки України, а також ратифікована Верховною Радою України «Конвенція про кіберзлочинність» та «Стратегія кібербезпеки» (2016 року) [1].

Водночас спостерігається вільне використання значної кількості термінів, що часто не узгоджені між собою. Так у Законі України «Про основи національної безпеки України» згадуються «комп'ютерна злочинність» та «комп'ютерний тероризм», при чому жоден з цих термінів на має свого визначення а ні в цьому, а ні в інших нормативних документах. У «Стратегії національної безпеки України» (в редакції від 12 лютого 2007 року № 105/2007) комп'ютерні загрози не згадуються, а «кібербезпека» - лише в контексті необхідності «розробки та впровадження національних стандартів та технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих з відповідними європейськими стандартами, у тому числі згідно з вимогами ратифікованої Верховною Радою України Конвенції про кіберзлочинність». Отже можна констатувати, що в більшості своїй вітчизняне нормативно-правове поле в сфері інформаційної (кібернетичної) безпеки потребує нормативного визначення [2].

Таким чином, на сьогоднішній день можна виділити три основні проблеми, що ускладнюють боротьбу проти злочинів в кіберсфері:

1. Перевірка практично нових визначень ключових термінів («кіберпростір», «кібербезпека», «кіберзахист», «кібератака», «кібервійна», «кібертероризм», «кіберзброя», «кіберінфраструктура», «критична кіберінфраструктура»), але й таких, що можуть ефективно застосовуватись в практиці правоохоронної діяльності і при необхідності їх вдосконалення.

2. Несформованість високоефективного чинного нормативно правового поля.

3. Низька ефективність загальнодержавної системи протидії кіберзлочинності через слабку систему відповідності визначеним законодавством нормам [3].

Спираючись на досвід провідних країн світу ,важливо створити комплекс заходів спрямований на адекватне реагування на виклики та загрози у кіберпросторі,таких як:

- формування системи забезпечення кібербезпеки;
- створення кіберкомандування та кібервійськ;
- організаційне,технічне та законодавче забезпечення дій кіберпідрозділів;
- посилення контролю за національним кіберпростором;

**Література**

1. Про ратифікацію Конвенції про кіберзлочинність: закон України від 07.09.2005 № 2824-IV // Відомості Верховної Ради України. –2006. – № 5–6. – Ст. 71.

2. Орлов О. В. Актуальні напрями державної політики України у сфері боротьби з кіберзлочинністю [Електронний ресурс] Режим доступу:http://www.kbuapa.kharkov.ua/e-book/tpdu/2013-3/doc/1/01.pdf.

3. Струков В. М. До визначення напрямів протидії кіберзлочинності / В. М. Струков // Системи обробки інформації. – 2013. –Вип. 3 (110). – С. 203–207.

*УДК 340.15:351.746.1*

**Душкевич В.С.**
студентка ННІ ІБ
Національної академії СБ України

# РОЛЬ ПРОПАГАНДИСТСЬКОЇ ДІЯЛЬНОСТІ В ІНСТИТУЦІАЛІЗАЦІЇ ПЕРШОГО КУРУЛТАЮ КРИМСЬКОТАТАРСЬКОГО НАРОДУ (ГРУДЕНЬ 1917 Р. – СІЧЕНЬ 1918Р.): ІСТОРИКО-ПРАВОВИЙ АНАЛІЗ

Здійснивши анексію Автономної Республіки Крим (далі – АРК) у 2014 р., Російська Федерація (далі – РФ) вдається до поширення через своїх уповноважених представників фальсифікацій окремих фактів історико-правової дійсності з метою ідеологічного обґрунтування вчиненого діяння. Застосування методу історичної аналогії надає можливість встановити подібність між діяльністю РФ та радянської Росії у попередні періоди. Остання вдавалася до дискредитації органів національного самоврядування кримських татар (зокрема, Курултаю) шляхом поширення серед місцевого населення неправдивих відомостей щодо їх діяльності.

100 років тому в боротьбі за незалежність кримські татари в листопаді 1917 р. на чолі з Н. Челебіджиханом, який на той час був головою Всекримського Мусульманського виконкому і муфтієм – головою Таврійського мусульманського духовного управління. Н. Челебіджихан був фахівцем у галузі релігії та права, завдяки чому мав можливість об’єднати зусилля кримськотатарського національного руху з метою реалізації його національного суверенітету [4]. Цим самим першим кроком було скликання Курултаю –органу народного представництва, загальнонаціонального з’їзду,під час якого вирішуватися найважливіші питання нації. І одне із головних питань: встановлення Кримської народної республіки. Основна ідея Курултаю полягала в створенні автономії. Гасло «Крим для кримчан» стало першоосновою [2].

Нарешті, в останній день роботи – 26 грудня 1917 р.– Курултай ухвалив «Основні кримськотатарські закони», Відповідно до ст. 8 утворювався Національний уряд (більш відомий як Директорія) – його Головою та ди-

ректором юстиції став Н. Челебіджихан. Ст. 16 «Законів» задекларувала проголошення Курултаєм «Народної республіки». Закони КНР гарантували свободу особистості, вибору місця проживання, свободу слова, совісті, спілок, друку, зборів, страйків і страхування, а також права національних меншин, запроваджували рівноправність людей і рівноправність жінок і чоловіків та, нарешті, ліквідовували становий поділ (але знову - лише серед кримських татар), пільги й привілеї. Таким чином, кримські татари першими серед мусульман світу стали на шлях побудови модерного суспільства у його націонал-демократичній формі [1].

З одного боку все йшло добре, а з іншого більшовицькі організації півострову після отримання повідомлення з Петрограду також активізували свої дії. В Севастополі вони почали надсилати агітаторів на кораблі, підприємства та військові частини. На початку листопада місцеві більшовики отримали нове підкріплення: в Крим з Петрограду прибула значна група партійних працівників, котрі мали «досвід революційної боротьби».Моряки Чорноморського флоту теж відгукнулись на ці події. Завдяки тому, що вони перебували під впливом більшовиків, моряки підтримали жовтневий переворот. 6 листопада 1917 р. в Севастополі відкрився Загальночорноморський флотський з'їзд. Спочатку на ньому головував есер Моренко, але вже на другий день його зняли, а натомість головою став більшовик, матрос Платонов . З'їзд прийняв резолюцію, в якій зазначалося, що він вважає «обраний Центральний виконавчий комітет Всеросійського З'їзду рад єдиним носієм верховної влади та закликає всіх матросів, солдатів, робітників та селян згуртуватися навколо рад і підтримати їх в боротьбі з контрреволюцією» [3].

Але не внутрішні суперечки всередині кримськотатарського національного руху і незгода у стосунках із іншими політичними силами завинили у тому, що Кримська народна республіка припинила своє існування,а все тому, що наприкінці січня 1918 року більшовики захопили увесь Крим, оголосили про розпуск Курултаю і Ради народних представників.

Таким чином, пропагандистська діяльність відігравала важливу роль у діяльності радянської влади з дискредитації діяльності Курултаю кримськотатарського народу. Разом з тим, представники Курултаю також вдавалися до застосування широкого комплексу заходів, спрямованих на формування серед місцевого населення позитивного образу цього органу національного самоврядування кримських татар як такого, котрий спроможний сприяти реалізації їх національного суверенітету. Вбачається, що активізація органів національного самоврядування кримських татар на сучасному етапі сприяла б мінімізації згубного впливу пропаганди РФ на свідомість широких кіл населення.

**Література**

1. Шурхало Д. Якої Кримської республіки прагнули кримські татари в 1917 році? / Д. Шурхало // [Електронний ресурс]. Режим доступу : https://www.radiosvoboda.org/a/28905827.html**.**

2. Чубаров Р.100 років Курултаю кримськотатарського народу / Р. Чубаров // [Електронний ресурс]. Режим доступу : https://day.kyiv.ua/uk/article/podrobyci/100-rokiv-kurultayu-krymskotatarskogo-narodu.

3. Атлас М.Л. Борьба за советы. Очерки по историисоветов в Крыму 1917-1918 гг. /М.Л. Атлас. – Крымиздат,1933. – 145–147с.

4. Бекірова Г. Перший Курултай кримськотатарського народу: віхи, події, особистості (закінчення) / Г. Бекірова // [Електронний ресурс]. Режим доступу : https://ua.krymr.com/a/28897534.html.

*УДК 356.35 : 355.40 (045)*

**Коваль М.О.**
ад'юнкт
**Шуліка В.І.**
курсант 5 курсу
Військовий інститут
Київського національного університету
імені Тараса Шевченка

## ІНФОРМАЦІЙНА СКЛАДОВА СУЧАСНИХ ЗБРОЙНИХ КОНФЛІКТІВ

*Публікація присвячена розгляду впливу інформації на ведення бойових дій у сучасному світі, як інформаційна складова діяльності військ змінює сам характер ведення війни. Проблема є актуальною з огляду на гостру необхідність вироблення нових підходів до ведення бойових дій в умовах АТО на Сході України.*

ЗМІ завжди були супутниками війн, але поява таких понять як "інформаційна війна", "медіа-агресія", "інформаційна безпека", свідчить не тільки про тісний зв'язок мас-медіа з конфліктними ситуаціями, але і про якісно нову роль ЗМІ в збройних конфліктах: у сучасних війнах боротьба на інформаційному полі є не менш важливою, ніж безпосередньо бойові дії. І якщо донедавна переважно війна впливала на інформаційну сферу, зокрема, на журналістику (наприклад, Перша світова війна обумовила появу в США аналітичної журналістики – американці просто не могли зрозуміти, яким чином вбивство ерцгерцога Фердинанда стало приводом для конфлікту такого масштабу), то останнім часом спостерігається зворотний зв'язок: ЗМІ відіграють усе більшу роль як у розв'язанні, так і в перебігу збройних конфліктів [4].

Візуальний бік конфліктів дуже важливий, оскільки саме він найбільше відбивається на масовому сприйнятті подій глядачами. Як вважають дослідники, сприйняття конфліктів значно стереотипізоване й містить у собі емоційну реакцію з почуттям ворожості стосовно однієї сторони та когнітивний аспект – прагнення до спрощення інформації, схематичну оцінку фактів, вибірковість сприйняття [1]. Стереотипне сприйняття інформації залежить від підходу до висвітлення конфліктів засобами масової інформації. Тележурналістам тут особливо складно: вони мають вести репортажі в обмежених часових рамках, і, звичайно, цілісна картина конфлікту може від цього постраждати. Кореспонденти опозиційних сторін найчастіше оцінюють конфлікт із різних точок зору і відбивають його діаметрально протилежно – цей феномен, що спостерігається зазвичай у політиці, дістав назву дзеркальних образів (та ж сама подія по-різному трактується палестинськими й ізраїльськими ЗМІ).

Інформаційно-психологічні операції і раніше були присутні під час ведення воєнних дій, так наприклад(монголи – вели з собою стадо коней для створення ефекту масовості, троянці – підпалювали вночі величезні клубки сіна і пускали їх на греків, китайці – намагалися підкупити впливових людей противника та дестабілізувати ситуацію з середини) та інші, але розвиток інформаційно-комунікаційних технологій та комп`ютерних систем дав початок тому, що ми бачимо зараз.

Останніми роками виникла нова форма воєнного конфлікту, який починається з «мирних» антиурядових акцій, що переростають у жорстке громадянське протистояння, і завершується зовнішньою інтервенцією. Такі конфлікти цілком можна назвати новим типом воєн сучасної епохи. Відомий американський військовий теоретик Френк Хоффман одним з перших зазначив: «…війни сучасної епохи характеризує процес гібридизації, у рамках якого змішуються традиційні форми війни,кібервійни, організованої злочинності, іррегулярних конфліктів, тероризму і т. п.».

Геополітичну ситуацію в сучасному світі не можна назвати стабільною: міжнаціональні суперечності, територіальні конфлікти, миротворчі операції тощо повсякчас виникають в різних точках земної кулі. Обов’язок журналіста загалом і публіциста зокрема – висвітлювати події в гарячих точках професійно, не виходячи за рамки загальних морально-етичних норм подачі військових конфліктів.

У наш час сама поява таких понять, як "інформаційна війна", "медіа агресія", "інформаційна безпека", свідчить не лише про тісний взаємозв’язок засобів масової інформації з конфліктними ситуаціями, але й про те, що у збройних та політичних конфліктах сучасності боротьба на інформаційному рівні не менш важлива, ніж безпосередньо воєнні чи дипломатичні дії. Щоб охарактеризувати нову військову реальність, він запропонував термін «гібридна війна», що дає змогу найбільш точно відобрази-

ти важливі зміни в характері воєн при збереженні їх незмінної природи. Така війна виходить за рамки традиційних понять про неї, вона набуває комбінованого характеру, перетворюючись на клубок політичних інтриг, запеклої боротьби за політико-економічне домінування над країною, за території, ресурси й фінансові потоки [3].

Якщо протягом перших двох третин XX ст. війна переважно впливала на інформаційну сферу, останнім часом бачимо зворотний зв'язок як на макро-, так і на мікрорівні. Перелом в інформаційно-воєнній сфері – це в'єтнамська війна. Американські військовики неодноразово стверджували, що причиною їх поразки стала не так допомога Радянського Союзу та завзятість в'єтнамців, як негативна позиція власної преси. Тоді ж визнали необхідність наявності "інформаційно-психологічного забезпечення бойових дій", себто формування через ЗМІ суспільної думки таким чином, аби будь-які воєнні дії знаходили підтримку серед власних громадян, та й взагалі у більшості мешканців планети.

**Література**

1. Асиметрія міжнародних відносин / за ред. Г. М. Перепелиці, О.М.Субтельногою. – Видавничий дім «Стилос», 2005. – 555 с.

2. Іванов В. Ф., Сердюк В. Є. Журналістська етика. – К.: Вища шк., 2007. – 214-216 с.

3. Циганок О. Ізраїльсько-ліванська війна: рік 2006., - «Червона зірка» від 10.10.2007г. Режим доступу: http://www.redstar.ru/2007/10/10_10/4_02.html.

4. Матеріали інформаційного сайту [Електронний ресурс] http://www.dy.nayka.com.ua/?op=1&z=757.

5. Матеріали інформаційного сайту [Електронний ресурс] http://www.exlibris.ru/media/publications/detail/natsionalnyy_brending_diskussii_vokrug_sushchnosti_yavleniya/.

*УДК 004.056.53*

**Корнійчук М.О.**
студент 3-го курсу
ННІ ІБ Національної академії СБ України
**Семчишина С.В.**
Національна академія СБ України

## ШЛЯХИ ОПТИМІЗАЦІЇ ЗАХИСТУ ІНФОРМАЦІЇ В УКРАЇНІ

Проблеми інформаційної безпеки України в сучасних умовах є надзвичайно актуальними і вимагають поглибленого вивчення.

Загалом система інформаційної безпеки має відбивати стан захищено-

сті національних інтересів саме в інформаційній сфері від зовнішніх та внутрішніх загроз як для самої держави або суспільства, так і для конкретної людини.

Система інформаційної безпеки є одночасно й елементом у системі вищого рівня – міжнародного, національного, місцевого. Але сьогодні низка підсистем, які входять до цієї макросистеми, ще не вивчені на належному рівні, а також не мають комплексного, системного дослідження з виходом на сучасні конструкції та пропозиції. Це стосується проблем інформаційної безпеки в Україні.

Стаття 17 Конституції України передбачає, що «забезпечення інформаційної безпеки – одна з найважливіших функцій держави, справа всього народу». Однак щодо сутності і ознак інформаційної безпеки єдиної точки зору серед науковців немає [1].

Забезпечення інформаційної безпеки – це сукупність заходів, призначених для досягнення стану захищеності потреб особистостей, суспільства і держави в інформації.

Держава здійснює свої заходи через відповідні органи, а громадяни, суспільні організації і об'єднання, що мають відповідні повноваження, у відповідності із законодавством. В основу забезпечення інформаційної безпеки держави повинні бути покладені наступні принципи: 1) законність, дотримання балансу інтересів особистості, суспільства і держави;2) взаємна відповідальність суб'єктів забезпечення інформаційної безпеки; 3) інтеграція систем національної і міжнародної безпеки.

Законодавча база, яка визначає перелік відомостей, що віднесені до державної таємниці, механізм та порядок її захисту повинні розроблюватися, виходячи із наведеного принципу, а також багатосторонніх угод держав, які входять до міжнародної системи інформаційної безпеки. Формування останньої буде, очевидно, справою далекої перспективи, яка ознаменує собою вищий рівень прояву довіри та зацікавленості держав світового співтовариства в забезпеченні виконання на практиці принципу адекватної інформованості. Така система повинна стати підсистемою у системі колективної безпеки [2, с. 3-5].

В Україні створена і діє досить розгалужена система забезпечення безпеки інформації, її захисту. Існує певна законодавча база, яка складається з Законів України «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про державну таємницю» тощо. Діє ряд Указів Президента та Постанов Кабінету Міністрів України, які регулюють конкретні напрями діяльності в галузі захисту інформації.

Функціонує система ліцензування і сертифікації діяльності, зокрема виробництва товарів та надання послуг у галузі технічного і криптографічного захисту інформації.

Органи інформаційної безпеки можуть створюватися (на законодав-

чих засадах) і в недержавних структурах для захисту своїх потреб в забезпеченні необхідною інформацією. Дані органи на основі укладення відповідних угод можуть бути приєднані до єдиної державної системи інформаційної безпеки.

На теперішній час окремі елементи системи інформаційної безпеки створені та функціонують (органи зовнішньої розвідки, інформаційні служби різноманітних міністерств, система технічного та криптографічного захисту інформації держави і т. н.). Проте для їхнього функціонування ще недостатня правова база. Зміст діяльності органів інформаційної безпеки також ще не в повній мірі відповідає покладеним на них завданням. Це пояснюється в першу чергу недостатнім опрацюванням питань, що стосуються форм і способів забезпечення інформаційної безпеки [3, с. 2-3].

Наступним кроком оптиматизації захисту інформації в Україні є забезпечення захисту і контролю національного інформаційного простору, а також забезпечення інформації про країну в світовому інформаційному просторі. Національним інформаційним простором вважається сукупність інформаційних потоків як національного, так і іноземного походження, які доступні з території держави.

Надійно захистити інформаційний простір може лише відкрита символьна система, яка не сконцентрована на собі, а якнайширше розповсюджується, доки не втрачає привабливості для оточуючих. Відсутність відомостей, їх виключно або переважно негативний характер у сучасному світі впливає на зовнішньополітичну і економічну діяльність як держави в цілому, так і на окремих її громадян та їхніх організацій. Саме тому ця проблема набуває загальнодержавного значення, а в разі її нехтування створює загрозу національній безпеці.

Комплексний характер актуальних загроз національній безпеці в інформаційній сфері потребує визначення інноваційних підходів до формування системи захисту та розвитку інформаційного простору в умовах глобалізації та вільного обігу інформації [4].

**Література**

1. Конституція України від 28 червня 1996 року // Відомості Верховної Ради, 1996.

2. Захаров Е. Информационная безопасность или опасность отставания? // Права людини. – 2000. – № 1 . – С. 3-5.

3. Гуцалюк М. Інформаційна безпека України: нові загрози // Бизнес и безопасность. – 2003. – № 5. – С. 2-3.

4. Доктрина інформаційної безпеки України. – [Електронний ресурс]. – Режим доступу: http://www.presedent.gov.ua/documents/472017-21374.

*УДК 32.019.51*
**Люля В.С.**
Національна академія СБ України
**Присяжнюк М.М.**
кандидат технічних наук,
старший науковий співробітник
Національна академія СБ України

# НЕЛІНІЙНІ ТА ПРОКСІ-ВІЙНИ СУЧАСНОСТІ

Провідні країни світу виділяють на оборону значні бюджети, що дають їм змогу тримати мільйонні армії, мати найсучаснішу зброю, в тому числі зброю масового ураження. За цих умов конфлікт між країнами може перетворитися на глобальну війну. Тому виникла потреба пошуку безпечнішого засобу вирішення конфліктів, що не призведе до негативних глобальних наслідків. Таким засобом стала гібридна війна, що являє собою комбіноване військово-політичне, економічне та інформаційне протистояння у вигляді безстатусного, часто прихованого конфлікту. Сучасні технології, специфіка соціальних, економічних та політичних умов розвитку світового співтовариства сприяли появі таких нових понять, як проксі- та нелінійна війна [1].

Останні десятиліття серед фахівців ведуться дискусії не тільки щодо нових типів війни, але й стосовно трансформації поняття «війна», її суті та особливостей. Зважаючи на зростаючу роль інформації у сучасному світі, американський дослідник Маклюен наводить цікаву тезу: «Істинно тотальна війна – це війна за допомогою інформації». Мета нелінійної інформаційної війни – послабити моральні і матеріальні сили супротивника або конкурента та посилити власні. Вона передбачає заходи пропагандистського впливу на свідомість людини в ідеологічній та емоційній галузях. Ліванo-Ізраїльський конфлікт 2006 року відомий в Лівані як Липнева війна, а в Ізраїлі як Друга ліванська війна – є класичним прикладом нелінійної війни, в якій Хезболла боролася із військово сильнішим противником Ізраїлем із використанням класичних військових дій, нерегулярних збройних формувань та інформаційних методів ведення війни, завдавши Ізраїлю, на думку деяких експертів, стратегічної поразки [2].

Проксі-, інформаційні війни або, більш поширена назва, кібервійни – це комп'ютерне протистояння у просторі Інтернету. Воно спрямоване передусім на дестабілізацію комп'ютерних систем і доступу до інтернету державних і фінансових установ, створення безладу та хаосу в житті країн, які покладаються на Інтернет у повсякденному житті. Яскравим прикладом є проксі-війна в Ірані. У червні 2010 року Іран став жертвою кіберата-

ки, коли в комп'ютерну мережу дослідного ядерного центру в Натанзі був занесений комп'ютерний вірус Stuxnet. У результаті чого, за оцінкою газети Business Insider, «атомна програма Тегерану була відкинута щонайменше на два роки назад». Хоча жоден уряд не взяв на себе відповідальність за впровадження вірусу Stuxnet, за рядом оцінок, це була спільна операція США та Ізраїлю. Спеціаліст з інфобезпеки Майкл Гросс назвав цей інцидент «першою відомою кібервійною в історії» [3].

Однією з країн, яка останнім часом активно використовує інструменти гібридної війни, є Російська Федерація. Так, ознаками нелінійної та проксі-війни з боку Росії до України є: ослаблення центральної влади та часткове «безвладдя» на тлі зміни влади; зростання суперечностей (а швидше – актуалізація вже наявних) між Центром і регіонами; незадовільний психологічний і матеріально-технічний стан українських безпекових структур; антагонізм між різними силовими структурами. Особливо активно інформаційно-пропагандистська робота Росії велася саме в Криму протягом усіх років незалежності України [4].

Російські фахівці розробили нову концепцію такого роду війн та застосували її на практиці. Базові складові частини російської стратегії і тактики сучасної гібридної війни сформульовані у 2013 році начальником генерального штабу ЗС РФ В. Герасимовим. Саме на основі цих принципів було спланировано та реалізовано напад на Україну, захоплення Криму та розв'язання війни на Донбасі, в якій військова потужна держава-агресор домовляється із недержавними виконавцями – групами місцевого населення та бойовиками, – зв'язок із якими вона формально цілковито заперечує.

Отже, розглянувши поняття нелінійна та проксі-війна, можна дійти висновку, що вони означають сучасний вид гібридної війни, де в конфлікті використовуються різноманітні засоби нападу та оборони держав, що виходять за рамки конвенційно-визначених варіантів та видів ведення війни.

Сучасне міжнародне право не включає в себе поняття «нелінійна чи проксі-війна», що в свою чергу приводить до відповідних наслідків. Відсутність регулювання цього нововиявленого явища пришвидшує виникнення все нових засобів атаки у війнах, відповідальність за які не можуть понести винуватці через відсутність норм, які зобов'язують сторони.

**Література**

1. Сучасна гібридна війна: нові форми гібридної агресії. [Електронний ресурс]. – Режим доступу: http://racurs.ua/ua/1063-suchasna-gibrydna-viyna-ta-yiyi-vidobrajennya-u-virtualniy-realnosti-chastyna-2.

2. Арзуманян Р.В. Определение войны в 21 веке. Обзор XXI ежегодной конференции по стратегии Института стратегических исследований Армейского военного колледжа, 2011. – 60 с.

3. Hoffman Frank G. Hybrid Warfare and Challenges / F.G.Hoffman // Joint Force Quarterly (JFQ). – 2009. – Issue 52, Forth Quarter.

4. Горбулін В. «Гібридна війна» як ключовий інструмент російської геостратегії реваншу». Дзеркало тижня № 2. 2015, 23 січня. [Електронний ресурс]. – Режим доступу: http://sp.niss.gov.ua/content/articles/files/3-1435911076.pdf.

*УДК 351.746.1*

**Малоокий Я. М.**
Навчально-науковий інститут інформаційної безпеки
Національної академії Служби безпеки України

# ПРОБЛЕМИ НОРМАТИВНО ПРАВОВОГО ВРЕГУЛЮВАННЯ СФЕРИ КІБЕРБЕЗПЕКИ УКРАЇНИ ТА ШЛЯХИ ВИРІШЕННЯ ЦИХ ПРОБЛЕМ

Сучасний світ дедалі стає все більш залежним від стану та розвитку кіберпростору, який проник майже в усі сфери життєдіяльності держави, включаючи державне управління, забезпечення національної безпеки і оборони, безпечне функціонування банківського сектору, сталий розвиток економіки і промисловості, виконання завдань за призначенням в енергетиці та на транспорті.

Недоліки нормативно-правового врегулювання сфери кіберпростору у вигляді неточних формулювань, неузгодженості з іншими документами, часом нерозуміння наслідків тривалої дії певних регуляторних положень призводять до глобальних проблем у забезпечені безпеки громадян і держави у кіберпросторі.

Актуальність даної теми полягає в тому, що сфера кіберпростору в Україні розвивається швидкими темпами, а нормативно-правове врегулювання цієї сфери не поспіває за цим активним розвитком, що породжує низький рівень кібербезпеки України.

Метою моєї роботи є дослідження основного нормативно-правового акта який покликаний врегулювати сферу кіберпростору в Україні, визначення проблем цьому нормативно правовому акті та визначення шляхів вирішення цих проблем.

Відповідно до мети визначено завдання: розглянути Стратегію кібербезпеки України, визначити її недоліки та шляхи виправлення знайдених недоліків.

Основним нормативно-правовим актом який регулює сферу кіберпростору та має за мету забезпечення кібербезпеки в Україні є «Стратегія кібербезпеки України» і в ній яскраво виражена основна проблема сфери кібербезпеки України – невизначеність термінів. Це є основною проблемою на цьому етапі розвитку кіберпростору в України. Будь яка діяльність, в будь якій сфері потребує використання єдиної термінології. В Стратегії використовуються такі терміни: кібератака (11 разів); кіберпростір (26 ра-

зів); кіберзлочинність/кіберзлочин (15 разів); кібербезпека (51 раз); кіберпростір (26 разів); кіберзахист (30 раз); кібершпигунство (2 рази); кіберінцидент (8 разів); кібертероризм (3 рази), але жодного пояснення цих термінів в цій стратегії, або іншому чинному нормативно-правовому акті немає.

Згідно частини 3 Стратегії кібербезпеки України суб'єктами забезпечення кібербезпеки в Україні є: Міністерство оборони України; Генеральний штаб Збройних Сил України; Державна служба спеціального зв'язку та захисту інформації; Служба безпеки України; Національний банк України; Національна поліція України; Розвідувальні органи України та на них покладені різні повноваження по забезпеченню кібербезпеки. Усі повноваження описуються з використанням термінів зазначених вище, а через те що визначення цих термінів відсутнє в жодному нормативно-правовому акті, що чинний сьогодні то і виконання повноважень покладених на суб'єкти не можливі.

Отже стає зрозуміло, що для вирішення цієї проблеми, яка зараз є основною, треба просто визначити термінологію, що дозволить суб'єктам забезпечення кібербезпеки, відповідно до цього нормативно-правового акту, чітко виконувати свої повноваження та забезпечувати кібербезпеки на території України. Депутати Верховної ради України також розуміють цю проблему само тому 05.10.2017 року було прийнято Закон України «Про основні засади забезпечення кібербезпеки України» в якому чітко визначені терміни які зазначались вище, але цей Закон ще не набрав чинності що залишає визначену проблему актуальною і до тепер.

**Література**

1. Указ Президента України Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" // Указ Президента. –2016. – № 96/2016.

*УДК 355.404.52+159.9*

**Мовчан А.Ю.**
аспірант відділу аспірантури і докторантури
Національна академія СБ України
**Слюсарчук І.В.**
доктор юридичних наук, професор
Національна академія СБ України

## ЗАЛУЧЕННЯ ОСОБИ ДО ВИКОНАННЯ ЗАВДАНЬ ПРАВООХОРОННИХ ОРГАНІВ ШЛЯХОМ КОМУНІКАТИВНОГО ВПЛИВУ

Актуальність даної теми зумовлена перш за все глобальними змінами в результаті посилення міждержавних зв'язків у всіх життєво важливих сферах. З розвитком держави постає питання її захисту і оборони.

Сучасний етап розбудови національної державності України характеризується складним політичним та економічним станом розвитку нашої країни. Адже принципово нові загрози, спричинені трансформацією технологій, специфікою соціальних, економічних та політичних умов розвитку сучасного світового співтовариства, впливають на характер та особливості розвитку безпекового середовища, у якому Україні необхідно будувати нову систему відносин між громадянином, суспільством та державою. Вагому роль у забезпеченні національної безпеки відіграє людський фактор. Саме через комунікативний вплив та залучення осіб до виконання службових завдань отримується, опрацьовується та підсумовується важлива інформація з метою запобігання загрозам національній безпеці. Завдяки комунікативному впливу і його особливостям забезпечується захист національних інтересів держави.

Питання полеміки, публічного виступу та переконання, розглядали ще за часів античності Горгій, Сократ, Платон, Демосфен, Аристотель, Цицерон та інші.

Дослідженню комунікативного впливу як прямо, так і опосередковано присвячено низку наукових доробок вітчизняних і зарубіжних учених: О. П. Демиденко (стратегії комунікативного впливу у прагмалінгвальному аспекті), В. І. Розов (комунікативна підготовка співробітників правоохоронних органів), Л. Ф. Компанцева (соціальні комунікації для фахівців сектору безпеки та оборони), В.М.Петрик (технології та засоби маніполювання свідомістю), Ю. Габермас, у центрі своїх філософських роздумів ставив поняття комунікативного розуму, Д. Карнегі займався сучасним практичним напрямком комунікативного впливу на слухача, Шуберт Э.Э. досліджував дискурсні одиниці, рівні, прийоми і принципи мовного впливу в когнітивному аспекті, Р. Ронін розкриває методи та прийоми отримання конфіденційної інформації, її збирання та аналіз, як залучати людей до співпраці та до виконання завдань, які вас цікавлять.

Згадані вище вчені зробили вагомий внесок у розуміння комунікативного впливу, проте, зважаючи на нові завдання, які постають перед сферою забезпечення національної безпеки, доцільність дослідження цієї проблематики буде актуальною й надалі.

Слід зазначити, що протягом останніх десятиліть комунікативний вплив набув значення вирішального інструменту в системі визначення і реалізації зовнішньої політики учасників у міжнародних відносинах.

Як відомо, ще античні дипломати, здійснюючи свої місії до іноземних держав і виконуючи офіційні завдання, часто отримували і таємні інструкції, виконання яких зводилося переважно до збору інформації про країну призначення, потрібної на випадок війни з нею [3, с. 7]. Не нехтували вони також і залученням осіб до виконання завдань задля забезпечення інтересів власної держави.

Мова є потужним засобом комунікативного впливу. Нині комунікативна діяльність безпосередньо впливає на формування зовнішньополітичного курсу кожної держави. Крізь призму слова здійснюється вагомий вплив на суспільство, на перебіг подій у країні та світі. Задля забезпечення національної безпеки комунікативний вплив застосовується як засіб залучення осіб до виконання завдань у цій сфері.

Фахівці на основі критерію використання мовленнєвих засобів виділяють наступні методи впливу: переконання, примушення, навіювання і інформування. Переконуючий вплив у професійному спілкуванні досягається за допомогою аргументації. «Аргументація – це логіко-комунікативний процес, спрямований на обґрунтування позиції однієї людини з метою наступного її розуміння й прийняття іншою людиною» [4, с. 39].

Проте не завжди поставленої мети можна досягнути методом переконання, в такій ситуації комунікативний вплив набуває дещо іншої форми і використовується інший мовленнєвий засіб – примушення. В.І.Розов надає наступне визначення даного терміну: «Примушення – це такий вид психологічного впливу, який відкрито пригнічує здатність до опору. Це дозволяє досягати мети, що суперечить бажанням, намірам і інтересам людини» [4, с. 48].

Під навіюванням або сугестією розуміють форму психологічного впливу, при якому передання інформації відбувається за допомогою частково неусвідомлюваного, направленого сигналу на вербальному чи невербальному рівнях. «Як комунікативна технологія сугестія має нейтральний характер, її позитивність чи деструктивність визначається метою, цілями та результатом комунікативних дій. Навіювання є основним способом маніпулювання свідомістю» [2, с. 244-245]. Є. Л. Доценко зазначає, що маніпуляція – це вид психологічного впливу, майстерне використання якого призводить до прихованої появи у іншої людини намірів, які не співпадають з його актуально існуючими бажаннями [1, с. 59].

Як ми бачимо ці методи можуть бути використані задля досягнення поставленої мети. Адже залучаючи людину до співробітництва зі спецслужбами треба викликати у неї свідоме бажання допомогти державним органам. Щирість і відвертість у зверненні потужним чином впливають на сприйняття інформації. Метою комунікативного впливу як засобу залучення особи до виконання завдань у сфері забезпечення національної безпеки є спонукання об’єкта прийняти таке рішення, або вчинити ті дії, які необхідні для правоохоронного органу, надання посильної допомоги, правильне та неухильне виконання певного роду завдань, отримання інформації, задля того, щоб тримати певну ситуацію під контролем.

**Література**

1. Доценко Е. Л. Психология манипуляции: феномены, механизмы и защита / Е. Доценко. – М. : Издательство МГУ, 1997. – 344 с.

2. Компанцева Л.Ф. Соціальні комунікації для фахівців сектору безпеки та оборони : підруч. : у 2 т. Т. 1 / Л. Компанцева. – К.: Вид-во НА СБ України, 2016. – 267 с.

3. Пик С. М. Таємна дипломатія і розвідка у міжнародних відносинах : навч. посібник / С. Пик. – Львів : ЛНУ імені Івана Франка, 2012. – 514 с.

4. Розов В.І. Комунікативна підготовка співробітників правоохоронних органів: навч. посіб. / В. Розов. – К. : Центр учбової літератури, 2015. – 160 с.

*УДК 35.077*

**Осьмак А.С.**
кафедра інформаційної політики
та цифрових технологій НАДУ

# ПЕРСПЕКТИВИ РОЗВИТКУ СТРАТЕГІЧНОЇ КОМУНІКАЦІЙНОЇ СКЛАДОВОЇ ПУБЛІЧНОГО ВРЯДУВАННЯ В УМОВАХ ЦИФРОВІЗАЦІЇ СУСПІЛЬСТВА

Сучасні глобалістичні виклики України, реформування публічного врядування в Україні та курс на цифровізацію суспільства, який визначено в «Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки», яка в т.ч. передбачає стимулювання розвитку відкритого інформаційного суспільства як одного з істотних факторів розвитку демократії в країні [1], передбачають необхідність змін у систему комунікативної взаємодії між різними ланками громадянського суспільства та інститутами публічної влади. Однією із складових інформаційної сфери стратегічних комунікацій в яких реалізується державна політика є, крім всього іншого – сфера цифрового урядування (державна політика з питань цифрового урядування; державна політика сприяння розвитку громадянського суспільства в Україні) [2].

Для розуміння перспектив розвитку комунікаційних систем, необхідно розглянути етапи розвитку та проаналізувати перспективи трансформації цифрових комунікативних систем.

Першим, хто сформулював підходи та відмінності розвитку цифрових комунікаційних систем став Тімоті О'рейллі. Він вперше застосував термін Веб 2.0 (Web 2.0) сформулював основні принципи побудови комунікаційних систем та відмінності в противагу попередніх організаційних підходів, які отримала термін Веб 1.0. [3]. Ревізія Веб 1.0 дозволив більшості веб-користувачів виступати лише як споживач контенту. Так було виділено три основних фактори Веб 1.0: веб-сайти 1.0, які є статичними; корисна інформація представлена користувачеві таким чином, що можливе тільки її зчитування; додавання або зміни інформації користувачем неможлива, що означає відсутність взаємодії між користувачем та сайтом.

Принциповою відмінністю технології Веб 2.0 є можливість не лише переглядати статичні веб-ресурси мережі, а й завантажувати власну інформацію, здійснювати обмін цифровими інформаційними ресурсами з іншими користувачами, діяти спільно з метою їхнього накопичення, брати участь в обговореннях тощо.

Так, разом зі зміною технологічних підходів потрібно провести відповідні зміни і в системі публічного врядування. Веб 2.0 передбачає наявність нової методики проектування державних інформаційних систем. Портали органів влади мають стати тим краще, чим більше людей ними користуються. Особливістю таких методик повинно бути можливість розширення за рахунок залучення громадян і бізнесу як до інформаційного наповнення і багаторазової його вивірки. В такій системі держава задає інформаційний привід, а громадяни отримують всі можливості його обговорення, дозволяють їм вільно додавати свої коментарі та думки з тих чи інших проблем без шкоди для достовірності вихідної інформації. Передбачається підвищення соціальної активності суспільства в усіх напрямках діяльності влади [4]. Перехід на новий комунікаційний рівень з метою активізації спілкування з громадянами повинен змінити поняття «цифровий уряд» на «уряд 2.0» (Gov 2.0), в якому широко застосовуються ідеї Веб 2.0. Використання технологій Веб 2.0 дозволить держорганам змінити характер взаємодії, поліпшити свою діяльність [5].

Подальшим розвитком стратегічних комунікацій є перехід до концепції Веб 3.0 з подальшою перспективою розвитку цієї стратегії до рівня Нейронет (NeuroNet, NeuroWeb, Brainet). Суттю Веб 3.0 є соціокультурне поняття, яке дозволить професіоналам створювати високоякісний контент і сервіси, на технологічній платформі Веб 2.0. Разом з формуванням філософії Веб 3.0 визначаються і основні принципи побудови платформи «Уряд 3.0» (Gov 3.0).

«Уряд 3.0» - нова парадигма для публічного врядування. Вона передбачає пряму доставку індивідуальних публічних послуг, шляхом надання доступу та перерозподілу цифрових даних на основі смарт-сервісів. При цьому передбачається новий рівень комунікації та співпраці між урядовими департаментами. Завданням таких систем і підходів є переорієнтацію публічного врядування на сервісні функції, компетентність і прозорість [6].

Аналіз, розвиток та впровадження сучасних комунікативних технологій дозволить забезпечити максимальну ефективність комунікаційної складової в діяльності органів публічного врядування.

**Література**

1. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/67-2018-%D1%80.

2. Поняття та сутність стратегічних комунікацій у сучасному українському державотворенні. / Кушнір О. В. – Режим доступу: http://goal-int.org/ponyattya-ta-sutnist-strategichnix-komunikacii-u-suchasnomu-ukrainskomu-derzhavotvorenni/.

3. Key differences between Web 1.0 and Web 2.0. / Graham Cormode, Balachander Krishnamurthy – Mode of access: http://firstmonday.org/article/view/2125/1972#author – Title from the screen.

4. Web 2.0 выходит на государственный уровень / Павел Григорьев – Режим доступу:: https://ecm-journal.ru/docs/Web-20-vykhodit-na-gosudarstvennyjj-uroven.aspx.

5. Tech-savvy governments to embrace Web 2.0. – Mode of access: http://www.zdnet.com/article/tech-savvy-governments-to-embrace-web-2-0/ – Title from the screen.

6. What Is Government 3.0? – Mode of access: http://www.mois.go.kr/eng/sub/a03/Government30/screen.do – Title from the screen.

*УДК 349, 323, 355/359*

**Преловський К.В.**
здобувач аспірантури і докторантури
Національна академія СБ України

## ІНФОРМАЦІЙНА БЕЗПЕКА ЯК ОДНА ІЗ СКЛАДОВИХ НАЛЕЖНОГО ФУНКЦІОНУВАННЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ БАНКІВСЬКОЇ СИСТЕМИ УКРАЇНИ

Запорукою процвітання будь-якої країни є розвиток та безперебійне функціонування її банківської системи. В сучасному світі технологій саме банківська система забезпечує необхідний паритет між життям суспільства «у кредит», розвитком бізнесу та отриманням податків для поповнення бюджету країни.

Так, у більшості високорозвинених країн світу (США, ФРН, Великобританія, Австралія тощо) для забезпечення нормального функціонування об’єктів, пошкодження, втрата або мінімальне порушення повсякденного режиму роботи яких призведе до значних негативних наслідків для національної безпеки, розроблено термін «критична інфраструктура» [1]. В Україні до об’єктів критичної інфраструктури віднесено підприємства та установи (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), продовольство, охорона здоров’я, комунальне господарство, що є стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення [2].

Як відомо, під інформаційною безпекою розуміється стан захищеності систем обробки і зберігання даних, при якому забезпечено

конфіденційність, доступність і цілісність інформації, або комплекс заходів, спрямованих на забезпечення захищеності інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки, запису чи знищення [3].

Банківська система України, окрім здійснення фінансових операцій, є найактуальнішою та однією з найбільших баз даних, що містить інформацію щодо установчих даних клієнтів, складу їх сімей, номерів мобільних телефонів, адрес проживання та реєстрації, тощо. Крім того, в банківській системі наявний ще один підвид інформації - банківська таємниця (bank secrecy). Банківська таємниця це – інформація щодо діяльності та фінансового стану клієнта, яка стала відомою банку в процесі обслуговування клієнта та взаємовідносин з ним чи третім особам при наданні послуг банку і розголошення якої може завдати матеріальної чи моральної шкоди клієнту. Відповідно до Закону України «Про банки і банківську діяльність» до банківської таємниці відносять відомості та інформацію: 1) про банківські рахунки клієнтів, у тому числі кореспондентські рахунки банків у Національному банку України; 2) про операції, проведені на користь чи за дорученням клієнта, та здійснені ним угоди; 3) про фінансово-економічний стан клієнтів; 4) про системи охорони банку та клієнтів; 5) про організаційно-правову структуру юридичної особи – клієнта, її керівників, напрями діяльності; 6) стосовно комерційної діяльності клієнтів чи комерційної таємниці, будь-якого проекту, винаходів, зразків продукції та інша комерційна інформація; 7) щодо звітності банку, за винятком тієї, що підлягає опублікуванню; 8) про коди банків для захисту інформації [4].

Слід зазначити, що станом на жовтень 2017 в Україні зареєстровано понад 42 млн. держателів платіжних карток, для обслуговування яких вироблено понад 60 млн. пластикових карток, з яких активними є 34 млн. Також, згідно аналізу розрахунків НБУ встановлено, що у 2011 році частка безготівкових платежів в Україні становила 8%, а за підсумками 2016 року вона перевищила 35% і у подальшому спостерігаються тенденції ще більшого переходу від готівкових розрахунків до безготівкових [4].

Вищезазначене свідчить про те, що захист банківської таємниці є одним з ключових об’єктів критичної інфраструктури банківської системи України.

Доцільно зазначити приклади ураження банківської системи України через інформаційні системи. Так, у червні 2017 банківська система України була уражена комп’ютерними вірусами «Wanna.Cry» та «PetYa». Спочатку через телекомунікаційні мережі віруси були направлені на інфікування систем ДФС України. Після ураження комп’ютерних систем ДФС України вірус перенісся до приватних підприємств, а вже далі поразив безпосередньо банки і інші організації та установи. Фактично гроші та персональні дані з банків викрадені не були, адміністративні будівлі не по-

шкодженні, уражено лише програмне забезпечення комп'ютерів обладнаних з операційною системою «Windows» (банківські установи з іншими операційними системами вражені не були), котре і призвело до припинення можливості здійснення електронних розрахунків та переводів.

Ще одним прикладом ураження банківської системи України є масові інформаційні вибухи у ЗМІ в 2014 році, направлені на залякування населення інформацією про ліквідацію ряду банків та девальвацією гривні. У зв'язку із запізненим реагуванням на дані інформаційні атаки, населення почало панічно знімати депозити з банківських установ. Це в свою чергу призвело до стрімкого падіння курсу гривні відносно долара США та прояву недовіри до банків. В результаті, населення почало тримати гроші «у матрацах» що призвело до подальшого дефіциту долару США, необхідного для здійснення міжнародних розрахунків, а через це – ще більшого його подорожчання. Наступною стадією стала неспроможність банків виплатити дострокові депозити своїм вкладникам, що завершилось запровадженням тимчасових адміністрацій та ліквідацією банківських установ.

**Література**

1. Єрменчук О. П. Нормативно-правове регулювання діяльності у сфері захисту національної критичної інфраструктури: аналіз та узагальнення нормотворчої практики США. / О. П. Єрменчук // Науковий вісник ДДУВС. – 2017. – № 3.

2. Постанова Кабінету Міністрів України від 23 серпня 2016 р. № 563.

3. Вікіпедія [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/інформаційна_безпека.

4. Офіційний сайт Національного банку України, [Електронний ресурс], Режим доступу: https://bank.gov.ua/.

*УДК 316.77*

**Пуркар Д.П**.
студент 3-го курсу
ННІ ІБ Національної академії СБ України
**Шепета О.В.**
кандидат юридичних наук, доцент
Національна академія СБ України

## СОЦІАЛЬНЕ ЗНАЧЕННЯ ДІЯЛЬНОСТІ ПРЕСИ У СФЕРІ ПРАВОВОГО ІНФОРМУВАННЯ ГРОМАДЯН

Сьогодні в Україні відбувається процес становлення нової політико-правової системи. Глибокі економічні, політичні, соціальні, культурні, ду-

ховні, інформаційні та інші перетворення, що знаходять свій розвиток у нашій державі на сучасному етапі, суттєво впливають на суспільну свідомість українських громадян і, зокрема, на правову культуру і правову свідомість як невід'ємні елементи формування громадянського суспільства та правової держави. Радикальна перебудова правового життя вирішальною мірою відбивається на стані правового розуміння, законності, правопорядку, правотворчої і правозастосовної практики, юридичної культури, прав та свобод людини і громадянина.

У ситуації суттєвого реформування правової системи зростає роль правової культури, а, відповідно, й інформаційної культури як її частини. Однією з найважливіших умов та засобом забезпечення підвищення рівня правової культури населення є структура відносин та засобів правового інформування. Водночас, це є невід'ємною складовою формування структури громадянського суспільства [1].

Враховуючи значний вплив засобів масової інформації на суспільство, доцільним вбачається дослідження ролі преси, як окремого виду ЗМІ, на стан правової поінформованості громадян України. Досліджується сфера правового інформування як складовий елемент правової свідомості громадян, який впливає на рівень усвідомленості та правомірності поведінки, виконання людиною своїх громадянських обов'язків та можливість цивілізованого користування правами і свободами, а це значною мірою залежить від рівня її правової поінформованості.

Значущість для суспільства правового інформування підкреслюється тим, що засоби масової інформації є історично сформованою потужною ідеологічною зброєю. Тому, якщо вони підпорядковані лише одній (все одно якій) соціальній групі людей, тим більше людей, які мають реальну владу в країні, як правило, створюють монополію на інформацію, а отже, ймовірні, і навіть неминучі, всілякі викривлення в розумах і політиці, і як наслідок, спотворення правових категорій. Відзначається, що діяльність друкованих періодичних ЗМІ щодо поширення ненормативної правової інформації, крім суто інформативної функції, забезпечує більшу "прозорість", демократичність функціонування органів державної влади у здійснюваних ними управлінських формах.

Правове інформування ЗМІ може бути визначене як інститут інформаційного права, як сукупність норм, що регулюють систему заходів, що здійснюються засобами масової інформації стосовно поширення інформації про правову дійсність у державі, змістом якої є чинне законодавство і право, правова ідеологія, а також відомості про правові форми діяльності держави. Нормативне правове інформування розуміється як діяльність відповідних ЗМІ (наприклад, преси) щодо поширення відомостей про нормативно-правові акти, що видаються органами державної влади різних рівнів, а також органами місцевого самоврядування, а ненормативне пра-

вове інформування – як діяльність певних ЗМІ щодо поширення відомостей про правотворчу, правозастосовну, інтерпретаційно-правову, судову, контрольно-наглядову, правоохоронну, установчу діяльність держави, а також про науково-правову сферу життєдіяльності суспільства.

Провідною державною структурою, що забезпечує на систематичній основі доведення до населення інформації про тексти нормативно-правових актів різного рівня є Міністерство юстиції України.

Згідно з законодавством право на інформацію забезпечується:

– створенням механізму реалізації права на інформацію;

– створенням можливостей для вільного доступу до статистичних даних, архівних, бібліотечних і музейних фондів, інших інформаційних банків, баз даних, інформаційних ресурсів;

– обов'язком суб'єктів владних повноважень інформувати громадськість та засоби масової інформації про свою діяльність і прийняті рішення;

– обов'язком суб'єктів владних повноважень визначити спеціальні підрозділи або відповідальних осіб для забезпечення доступу запитувачів до інформації;

– здійсненням державного і громадського контролю за додержанням законодавства про інформацію;

– встановленням відповідальності за порушення законодавства про інформацію.

Право на інформацію може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку, з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя [2].

**Література**

1. Становлення і розвиток друкованих засобів масової інформації новітньої України // [Електронний ресурс]. – Режим доступу: http://revolution.allbest.ru/history/00443222_0.html.

2. Стан і перспективи розвитку друкованих засобів масової інформації // [Електронний ресурс]. – Режим доступу: http://studopedia.su/12_66236_stan-i-perspektivi-rozvitku-zasobiv-masovoi-informatsii-v-ukraini.html.

*УДК 343.32*
**Рагнєв А.О.**
курсант
Національна Академія СБ України

# СУЧАСНІ ФЕНОМЕНИ СПРИЙНЯТТЯ ІНФОРМАЦІЇ ЯК ЕФЕКТИВНИЙ ВАЖЕЛЬ ВПЛИВУ НА СВІДОМІСТЬ ЛЮДИНИ

Ми живемо в час інформаційного суспільства. І це означає, насамперед, не глобальне поширення інформаційних технологій, а зовсім інший, новий рівень сприйняття інформації, з якою ми зіштовхуємося в повсякденному житті. Ми живемо в безмежному океані інформаційних потоків, «споживаючи тони контенту» та не усвідомлюючи як на нас впливає його зміст.

Тим не менш, природа не залишила цей нюанс непродуманим. Наша психіка адаптувалася до такого інформаційного оточення шляхом звичайної фільтрації того, що ми «споживаємо» в інформаційному плані.

По-перше, це так звана «інформаційна бульбашка» – певна свідома інформаційна ізоляція, яка є результатом власного вибору людини, відповідно до її інтересів. Проте, особа може і не усвідомлювати цього. Термін «інформаційна бульбашка», або «бульбашковий фільтр» уперше увів Ілая Парайзер і пояснив його як «персональну екосистему інформації, яка обслуговується певними алгоритмами» [1]. Також він описує явище використання цього феномену соціальними мережами та пошуковими машинами для вибіркового формування контенту, який є більш прийнятним для конкретної особистості, для подачі його у її «споживання».

По-друге, іншим механізмом пристосування до сучасного темпу життя є феномен «кліпового мислення», тобто мислення миттєвого сприйняття, сприйняття тут і тепер, навіть можна сказати, що це не мислення, а миттєва реакція на якийсь об’єкт, що заважає людині бути цілісною [2]. Вперше термін «кліпова культура», як принципово нове явище, був відзначений американським футурологом Е. Тоффлером, який окреслив його у концепції поняття кліпової культури [3]. Цей феномен можна пояснити на прикладі відомої соціальної мережі Instagram. Коли особа гортає стрічку новин, вона бачить великі фото із прихованими під ними підписами. Саме так більшість людей сьогодні сприймає інформацію. Тобто для аналізу пропонується лише загальний образ, текст аналізується лише поверхово, усвідомлюються лише загальні риси і таким чином створюється уявлення про світ. Більш того, це все робиться у поспіху, через страх пропустити ще щось цікаве. Хоча, якщо на секунду зупинитися і спробувати відтворити те, що запам’яталося за останні кілька годин, - результат не буде приголомшувати обсягами відтвореного.

Це показник того, що по-перше, сучасна людина бачить світ поверхово, через образи, які їй подають ЗМІ. У своїй книзі «Третя хвиля» Е. Тоффлер відтворює це явище таким чином: «…на особистісному рівні нас осаджують і засліплюють суперечливими фрагментами образного ряду, що до нас і не відносяться, які вибивають грунт з-під ніг наших старих ідей, обстрілюють нас розірваними, позбавленими сенсу «кліпами», миттєвими кадрами» [3; 160]. Герберт Маркузе, теж негативно описав вплив інформаційних технологій на сучасну людину, яку він описує як одновимірну, тобто позбавлену можливості мислити панорамно і критично [4; 115]. Підсумовуючи погляди дослідників, можна зробити висновок, що сьогодні формується тип людини-споживача, у якої майже повністю знижений рівень об'єктивного сприйняття дійсності.

Крім того, завдяки цьому, сучасна людина стає легкою мішенню для будь-яких маніпуляцій. Комбінація «бульбашкового фільтру» та «кліпового» мислення робить свідомість людини відкритою для зовнішніх модифікацій або, як кажуть програмісти, повністю «open-source» та «open-code».

Основним фактором тут є те, що через відсутність критичного мислення у маніпулятора з'явилася можливість модифікувати контент інформаційного оточення, що сприймає конкретна особистість або група людей. При цьому, ще легше це стає зробити, якщо людина вважає це нормою. Таким чином змінюється сприйняття дійсності.

Наприклад, особа цікавиться інформацією про новинки кінометражу, переглядає новини про це цілодобово. Шляхом нескладних маніпуляцій, поступово до контенту, який потрапляє до поля зору особи, буде додаватися інформація про риболовлю. Спочатку «випадкові» словосполучення, потом фото, потом афіші, потім посилання на статті, які релевантно пов'язують кіноакторів та риболовлю. З часом, особа «сама» почне читати такі статті і цікавитися риболовлею. Це банальний приклад, який чудово ілюструє механізм, який використовують стосовно населення зацікавленні в цьому структури.

Шляхи подолання цієї проблеми – у формуванні інформаційної культури та критичного мислення в населення. Але питання їх реалізації та контролю залишається відкритим та майже риторичним.

**Література**

1. Elie Pariser The Filter Bubble: What the Internet Is Hiding from You / Elie Pariser [Електронний ресурс] – Режим доступу: www.lse.ac.uk

2. Гриценя О. Феномен «кліповості» у парадигмі сучасної інформаційної культури / О. Гриценя [Електронний ресурс] – Режим доступу: www.kulturolog.org.ua

3. Тоффлэр Э. Третья волна / Э. Тофлэр. – М.: АСТ, 1999. – 664с.

4. Маркузе Г. Одновимірна людина. Дослідження ідеології розвинутого індустріального суспільства [глави з книги] / пер. В.Курганський // Сучасна зарубіжна соціальна філософія: Хрестоматія. – Київ: «Либідь», 1996. – С. 87-134.

*УДК 340.13 342.7 342/9*
**Роллер В.М.**
Військовий інститут КНУ ім. Тараса Шевченка

# ДОТРИМАННЯ ПРИНЦИПУ ПРОПОРЦІЙНОСТІ ПРИ ЗДІЙСНЕННІ ЗАХОДІВ ПРОТИСТОЯННЯ РОСІЙСЬКІЙ ПРОПАГАНДІ

З 2014 року між Україною та Російською федерацією йде неоголошена війна. Протистояння відбуваються не тільки на полі бою, а й у інформаційному просторі. Багато хто вважає, що інформаційна війна проти України була розпочата набагато раніше, ніж фактична військова інтервенція.

За час ведення гібридної війни здобуто багато нових знань про інформаційну війну, методи її ведення та способи підвищення інформаційної культури громадян, для зменшення впливу на їх свідомість та погляди. Органами державної влади вживаються заходи щодо зменшення російської пропаганди на території нашої Батьківщини.

У рамках реагування та боротьби з агресією Російської Федерації у 2017 році видано Указ Президента України від 15 травня 2017 року № 133/2017 Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року "Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)". У відповідності до цього Указу Президента на три роки, введено заборону інтернет-провайдерам надавати послуги з доступу користувачам мережі Інтернет до ресурсів сервісів «Mail.ru» (www.mail.ru) та соціально-орієнтованих ресурсів «Вконтакте» (www.vk.com) та «Одноклассники» (www.ok.ru).

Розглянемо такі заходи з точки зору українського законодавства. Конституція України у статті 34 визначає: "Кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань. Кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб - на свій вибір.

*Здійснення цих прав може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку* з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя".

В той же час Законом України " Про інформацію " визначено: " Кожен має право на інформацію, що передбачає можливість вільного одержання, використання, поширення, *зберігання та захисту інформації, необхідної для реалізації своїх прав, свобод і законних інтересів"*.

У статті 11 цього ж Закону визначено: “Інформація про фізичну особу (персональні дані) - це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Не допускаються збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та захисту прав людини. До конфіденційної інформації про фізичну особу належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров’я, а також адреса, дата і місце народження. *Кожному забезпечується вільний доступ до інформації, яка стосується його особисто, крім випадків, передбачених законом”.* Тобто, інформаційні права громадян захищені державою, та можуть бути обмежені також лише у випадках визначених законом.

Отже, у правовому полі виникає ситуація, коли на вагах з однієї сторони інтереси держави - у вигляді протистояння російській пропаганді у соціальних мережах, а з іншої сторони право громадян за доступ до особистих даних та їх захист. Забороняючи інтернет-провайдерам надавати послуги з доступу користувачам мережі Інтернет до соціально-орієнтованих ресурсів «Вконтакте» (www.vk.com) та «Одноклассники» (www.ok.ru), держава залишає громадян незахищеними від злому їх персональних аккаунтів у цих мережах та кіберзлочинності. У відсутності доступу до аккаунту громадянин не має можливості контролювати дії з аккаунтом, використання інформації, розміщеної на цих аккаунтах, а також інформації, що використовувалась при реєстрації на цих сайтах (номери телефонів, поштові адреси та паролі). Крім того, оскільки ці мережі засновані на території Росії, їх сервери переважно знаходяться на цій же території, що дає полегшений доступ російським спецслужбам, до даних, які знаходяться на цих серверах.

Отже, при прийняті рішень, щодо заборони чи обмеження доступу до аккаунтів у соціальних мережах необхідно враховувати принцип пропорційності, тобто, користь у забороні використання цих сайтів та обмеження пропаганди має бути більшою, ніж ймовірна шкода персональним даним чи інформації розміщеній у аккаунті користувача, доступ до якого закрито чи обмежено.

**Література**

1. Конституція України: [прийнята на п’ятій сесії Верховної Ради України 28 червня 1996 р., у редакції від 30.09.2016 р.]/База даних «Законодавство України /ВР України. URL: http://zakon0.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.

2. Про інформацію: [закон України : офіц. текст : у редакції від 01.01.2017] / База даних «Законодавство України /ВР України. URL: http://zakon3.rada.gov.ua/laws/show/2657-12.

3.Указ Президента України № 133/2017 Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року " Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій) "[Указ, від 15.05.2017 року] /База даних «Законодавство України /ВР України. URL:http://www.rnbo.gov.ua/documents/445.html.

4. Ю. Євтошук /Принцип пропорційності у практиці Конституційного Суду України, Вісник Конституційного Суду України № 1/2011 URL: http://www.irbisnbuv.gov.ua/cgibin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/Vksu_2011_1_15.pdf.

*УДК 004.56*

**Романова Т.В.**
Національна академія СБ України
**Гулак Г.М.**
кандидат технічних наук, доцент
Національна академія СБ України
**Кащук В.І.**
Національна академія СБ України

# РОЗВИТОК ТЕХНОЛОГІЙ КРИПТОВАЛЮТ ТА ЇХ ВПЛИВ НА ЗДІЙСНЕННЯ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ

Сучасний світ отримав нову технологію, яка несе нові можливості та нові ризики – криптовалюту. Для різних підвидів цієї технології криптовалюта, за суттю, це низка взаємопов’язаних інформаційних ресурсів, які утворюються шляхом застосування криптографічних перетворень - «блокчейн».

З технічного погляду робота в «блокчейн» будується просто: користувачі вносять необхідні дані (у випадку з біткойнами – це дані про транзакції), які потім потрапляють у блоки, створювані так званими майнерами, одного разу потрапивши до блоку, запис вважається дійсним і залишається незмінним.

Внесені дані неможливо стерти, видалити або підмінити. При цьому кожен користувач має доступ до повної копії всіх блоків, що пояснюється мережевим характером технології, а також дає можливість звіряти отриману інформацію на предмет відповідності даним, наявним у користувача. Ця особливість системи визначається використанням спеціальних алгоритмів шифрування. Такі властивості технології "блокчейн" зумовлюють можливість їх використання в різних галузях.

Основна перевага «блокчейну» полягає в тому, що відпадає потреба у послугах таких посередників, як платіжні системи, внаслідок чого підвищується швидкість обробки операцій і знижується вартість для кінцевого споживача.

Використання технології "блокчейн" має великий потенціал з погляду спрощення та підвищення ефективності у різних сферах діяльності і, насамперед, фінансовій, за рахунок створення принципово нової інфраструктури фінансових сервісів.

Водночас, попри очевидні переваги технології "блокчейн", перейти на нову технологію вдасться не так швидко.

На це є кілька причин, перш за все невизначеність у правовій та регуляторній сферах. Крім того, широкомасштабне впровадження цієї технології потребуватиме значних зусиль у частині стандартизації та уніфікації. Потрібно побудувати багаторівневу інфраструктуру "блокчейн" і зміцнити довіру до неї споживачів і регуляторів.

Отже, блокчейн – це технічне рішення, яке кардинально змінює основні підходи до здійснення онлайн-аукціонів, забезпечуючи учасникам максимальний доступ до інформації та захист даних.

Блокчейн фактично надає змогу кожному бажаючому перевірити хронологію дій, здійснених усіма учасниками під час аукціону і переконатися, що нічого не було зроблено заднім числом.

Варто врахувати, що нині технологія, попри її переваги, має водночас і недоліки, зокрема вона не відповідає багатьом критеріям безпеки, оскільки сам механізм роботи "блокчейн" передбачає, що внесені дані перебувають у публічному доступі.

За умови глобального характеру мережі й доступності даних на всіх континентах створюється цілком відчутний простір для цілеспрямованих махінацій, навіть за наявності потужних алгоритмів, що забезпечують анонімність користувачів і непідробність записів.

Серйозною проблемою роботи "блокчейн", яка впливає на здійснення правоохоронної діяльності, є управління анонімністю, протидія відмиванню грошей, шахрайству. Іншими словами, не зовсім зрозуміло, як зв’язати криптографічних користувачів із користувачами з реального світу.

Регулювання схем віртуальної валюти у США здійснюється у межах консервативної політики. У червні 2015 р. Нью-Йоркським департаментом фінансових послуг затверджено вимоги до "біт-ліцензій" (BitLicense) щодо регулювання організацій, які працюють з біткоінами, які розроблялися протягом двох років: заходи, спрямовані на забезпечення захисту прав споживачів, запобігання відмиванню грошей і посилення вимог до кібербезпеки при роботі з криптовалютами. При цьому немає суттєвих відмінностей у підходах у випадку з BitLicense та ліцензуванням для традиційних операторів грошових переказів.

Ряд країн, утому числі КНР, не підтримав нову грошову технологію. Центральний банк Китаю заборонив фінансовим інститутам здійснювати транзакції з цією валютою, а Народний банк Китаю оголосив, що фінансові установи та страхові компанії не можуть встановлювати ціни в біткоінах, купувати чи продавати віртуальну валюту або страхувати продукцію, пов'язану з біткоінами. Водночас використання приватними особами біткоінів у Китаї не забороняється. У жовтні 2015 р. у заяві для преси міністр фінансів Російської Федерації запропонував чотири роки позбавлення волі за випуск криптовалют, хоча офіційно в РФ операції з криптовалютою не заборонені. Ініціатива отримала підтримку декількох державних органів, у тому числі Міністерства економічного розвитку, Федеральної служби з контролю за обігом наркотиків. Крім того, Державна Дума заявила, що криптовалюта перешкоджає економічній стабільності Росії.

**Література**

1. Волосович С. В. Віртуальна валюта: глобалізаційні виклики і перспективи розвитку / С. В. Волосович // Економіка України. – 2016. – № 4. – С. 68-78.

2. Кузнецов Ю. Обережно: шпигуни поруч! / Юрій Кузнецов // Військо України. – 2014. – № 8. – С. 44-47.

3. Задірака В.К. Сучасні методи розв'язання задач інформаційної безпеки / В. К. Задірака // Вісник Національної академії наук України. – 2014. – № 5. – С. 65-69.

4. Сейтим Айганым. Анализ криптовалюты "Биткоин" на соответствие основным функциям денег / Айганым Сейтим // Актуальні проблеми економіки. – 2016. – № 4. – С. 286-293.

*УДК 325.744*

**Саган О.В.**
аспірантка Національного інституту
стратегічних досліджень при Президентові України

## СОЦІАЛЬНІ МЕРЕЖІ ЯК ІНСТРУМЕНТ ІНФОРМАЦІЙНОЇ ВІЙНИ

Швидкий прогрес та інформаційна революція дали змогу удосконалити й механізми війни, оскільки вивели її на новий рівень. Мова йде про так звану інформаційну війну, особливістю якої є латентний (прихований) характер. Враховуючи складність та багатогранність цього явища існує багато його визначень. Зокрема, у книзі Прокоф'єва "Інформаційна війна і інформаційна злочинність" визначається: інформаційна війна – це дії, початі для досягнення інформаційної переваги шляхом завдання шкоди інформації, процесам, що базуються на інформації і інформаційних систе-

мах супротивника при одночасному захисті власної інформації, процесів, що базуються на інформації і інформаційних системах. Зважаючи на роль інформації у сучасному світі, американський дослідник Маклюен виводить цікаву тезу: "Істинно тотальна війна - це війна за допомогою інформації". Очевидно, що інформаційна війна - складова частина ідеологічної боротьби [1].

Оскільки при розробці інформаційної зброї особлива увага приділяється психологічним особливостям людини та соціуму, соціальні мережі стали одним з найбільш важливих інструментів цього різновиду війни. Такий вибір пояснюється тим, що вони забезпечили легкий доступ до великих масивів інформації, а також стали ідеальним знаряддям для здійснення впливу та моделювати поведінки. Сам того не підозрюючи, користувач соціальної мережі стає абсолютно незахищеним перед вторгненням у його особисте життя. Наприклад, вчені Кембриджського університету виявили, що навіть те, як користувач ставить «лайки» у Facebook, може багато розповісти про нього, адже сучасні комп'ютерні програми дозволяють отримати усю інформацію з соціальних мереж і здійснити її аналіз [2].

Популярність соціальних мереж зростає з кожним роком, про що свідчить постійно зростаюча кількість користувачів. Відповідно до останніх даних, кількість користувачів "Facebook" перевищила один мільярд, трохи поступаються йому "Twitter" та "Google +" з приблизною кількістю учасників більше 200 мільйонів [3]. Понад мільярд людей активно використовують прямі мобільні платформи обміну повідомленнями, зокрема WhatsApp, Line, Facebook Messenger, Skype, Telegram тощо. Разом з тим зростають тенденції використання соціальних мереж з метою негативного інформаційно-психологічного впливу на обрані цільові аудиторії та збору інформації. Особливістю соціальних мереж є те, що через них негативний інформаційний вплив часто здійснюється приховано і має тривалий характер, оскільки триває до моменту виявлення та прийняття мір протидії [4].

Отже, з метою ефективного протистояння інформаційній війні у соціальних мережах виникає необхідність дослідити найбільш ефективні прийоми її ведення. Такими прийомами інформаційних атак є: *дезінформація* або надання хибної інформації - здійснюється з метою введення противнику або цільовій групі, що визначені як мішень для атаки; *залякування* або транслювання інформації що має на меті порушення рівноваги та формування тривожних або панічних настроїв - для відволікання уваги від реальних цілей та намірів противника та представників цільових груп-мішеней; *схематизування* або графічно-кількісна подача даних у доступному для представників цільової групи форматі - для спрощення та прискорення сприйняття інформації її отримувачами; *глузування* або виставлення противника та його можливостей в комічному світлі - під час підготовки до ведення активних дій в оф-лайн форматі, та в якості нейтралізації передбачень щодо потенційних можливостей противника; *вклинювання* або використання інформаційних повідомлень противника шляхом додавання до них певної інформації і корекції повідомлення у потрібному рус-

лі - для посилення ефективності та атакуючого потенціалу; *фальшування* - в соціальних мережах цей прийом зазвичай використовують для того, щоб на фоні повідомлення ЗМІ, яке не викликає сумніву, подати приховані меседжі або психологічні установки [5].

Звичайно, соціальні мережі можуть бути також використані з метою завчасного виявлення негативних явищ, зокрема таких як підготовка масових заворушень чи злочинної діяльності. Відповідно до досліджень Університету Кардіффа, даний сервіс показав здатність прогнозувати масові акції та інші події значно швидше, ніж поліція з випередженням навіть до однієї години. Що ж стосується можливостей збору інформації, слід зазначити, що з соціальними мережами пов'язаний новий вид розвідки - розвідки у соціальних мережах - "social media intelligence" або "SOCMINT", який в повній мірі використовується як силовими, так і різноманітними цивільними структурами [4].

Руйнування, які здатні завдати інформаційні війни у суспільній психології, психології особи, за масштабами і за значенням цілком співмірні, а часом можуть перевищити наслідки збройних війн. Інформаційна війна, яку протягом останніх років розгорнула проти України Росія цілком показала важливість інформаційної безпеки для всіх сфер життєдіяльності держави та деструктивну силу, яку може чинити інформація.

**Література**

1. Бабенко Ю. інформаційна зброя – зброя масового знищення! // https://www.pravda.com.ua/rus/articles/2006/04/20/4399050/.

2. Гвоздик О. Соціальні мережі – вільний обмін думками чи маніпулювання свідомістю? // http://xpress.sumy.ua/article/society/5700.

3. List of virtual communities with more than 100 million active users // http://en.wikipedia.org/wiki/List_of_virtual_communities_with_more_than_100_million_active_users.

4. Попова Т. Соціальні мережі, кібератаки та гібридні війни //https://www.radiosvoboda.org/a/28598299.html.

5. Курбан О.В. Інформаційні війни у соціальних он-лайн мережах : [монографія] / О.В.Курбан. – К.: Київ. ун-т ім.. Б.Грінченка, 2017. – 392 с.

*УДК 32.019.51*

**Селіна М.Б.**
Національна академія СБ України

## СТРАТЕГІЧНІ КОМУНІКАЦІЇ ЯК УМОВА РЕАЛІЗАЦІЇ НАЦІОНАЛЬНИХ ІНТЕРЕСІВ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Сучасна ситуація в Україні характеризується посиленням інформаційної боротьби в усіх сферах суспільно-політичного життя. За умов загострення суспільно-політичної кризи всередині країни Україна стає

об’єктом інформаційних впливів ззовні, спільною рисою яких є їх негативізм, спрямованість на формування у користувачів інформаційного продукту негативного ставлення до політичних рішень та їх суб’єктів – владних інститутів, а деколи й до принципу порядку загалом [2, с. 354].

Зважаючи на це, у процесі забезпечення національної безпеки України актуальним стає питання використання сучасних інформаційно-комунікативних технологій з метою нейтралізації загроз в інформаційній сфері. Одним з ефективних інструментів протидії зовнішнім та внутрішнім загрозам в інформаційній сфері, а також розбудови іміджу України в світі є стратегічні комунікації.

Наразі відсутнє єдине визначення «Стратегічних комунікацій», а серед науковців та практиків ведуться дискусії навкруги трактовки цього терміну.

Термін «Стратегічні комунікації» в його сучасному розумінні з’явився у військових колах США у 2001 році [6]. Вже починаючи з 2006 року його розпочали використовувати в офіційних документах США та трактувався як сфокусовані зусилля США, спрямовані на розуміння специфіки цільових аудиторій і роботу з ними для створення, укріплення і збереження урядом США сприятливих умов для подальшого просування національних інтересів і цілей шляхом скоординованої інформації, комплексних планів, програм дії, а також синхронізації з іншими елементами національної влади [5].

Положеннями Воєнної доктрини України «стратегічні комунікації» визначаються як скоординоване й належне використання комунікативних можливостей держави - публічної дипломатії, зв’язків із громадськістю, військових зв’язків, інформаційних і психологічних операцій, заходів, спрямованих на просування цілей держави [1].

На думку Л.Компанцевой «Стратегічні комунікації» - забезпечення взаємодії та вибудовування довгострокових формальних і неформальних зв’язків між різними структурами, інститутами, людьми: державою і громадянським суспільством; органами влади і інститутом сектору безпеки і оборони; силовими відомствами і громадянським суспільство; силовими відомствами і ЗМІ; співробітниками сектору безпеки і оборони [3, с. 204].

В. Ліпкан розуміє «стратегічні комунікації», як узгоджені та скоординовані урядом держави можливості інституціональної структури та інститутів громадянського суспільства, спрямовані на розуміння цільової аудиторії з метою створення, зміцнення, збереження та розвитку сприятливих умов для просування з урахуванням національних цінностей легітимованих національних інтересів, політики та цілей держави через використання узгоджених концепцій, стратегій, доктрин і програм, планів, тем, меседжів, смислів, наративів і продуктів, поєднані та синхронізовані з діями, можливостями, спроможностями та потенціалом усіх елементів системи державного управління [4].

Комплекс заходів, спрямованих на керування цільовими аудиторіями як всередині країни, так і за її межами, який складається з трьох частин – зв'язків з громадськістю, публічною дипломатією і інформаційних операцій [7].

Незважаючи на наявність термінологічних проблем, аналізуючи наявні визначення, на нашу думку можна дійти висновку, що більшість дослідників головним чином називають три складові стратегічних комунікацій: публічну дипломатію, зв'язки з громадськістю та інформаційні операції, при цьому суть стратегічних комунікацій полягає у керуванні цільовими аудиторіями з метою зміни їх поведінки та донесення до них інформації, необхідної для країни-суб'єкта використання стратегічних комунікацій.

Таким чином, у сучасних умовах, ускладнених зовнішньою інформаційною та військовою агресією, стратегічні комунікації можуть стати ефективним інструментом підвищення рівня взаємодії між державними органами і громадськістю, а також ж надає можливості за допомогою інформації формувати суспільну думку у необхідному для розвитку держави напрямі. Тобто використання стратегічних комунікацій стає чи не головною передумовою реалізації національних інтересів у сфері інформаційної безпеки держави.

**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».

2. Власюк О.С. Національна безпека України: еволюція проблем внутрішньої політики : Вибр. наук.праці/ О.С.Власюк. – К.: НІСД, 2016. – 528 с.

3. Компанцева Л.Ф. Соціальні комунікації для фахівців сектору безпеки і оборони : підруч.: у 2 т. Т. 1 / Л.Ф. Компанцева. – К.: Нац. акад. СБУ, 2016. – 267 с.

4. Ліпкан В. А. Поняття та структура стратегічних комунікацій на сучасному етапі державотворення. http://goal-int.org/ponyattya-ta-struktura-strategichnix-komunikacij-na-suchasnomu-etapi-derzhavotvorennya/.

5. Quadrennial Defense Review Report. 2006. February 6. The Secretary of Defense. 1000 Defense Pentagon. Washington. – P. 92.

6. Paul Ch. Report of the Defence Science Board Task Force on Managed Dissemination. 2001.

7. Tatham S.A. Strategic Communication: A Primer Academy of the United Kingdom, 2008. – P. 2.

*УДК 351.002.8*
**Сіренко Г.Г.**
аспірант кафедри інформаційної політики
та цифрових технологій Національної академії
державного управління при Президентові України

# ОСОБЛИВОСТІ ОРГАНІЗАЦІЇ ПІДБОРУ ТА ПІДГОТОВКИ КАДРІВ ПІДРОЗДІЛІВ КІБЕРЗАХИСТУ ОРГАНІВ ПУБЛІЧНОЇ ВЛАДИ В СУЧАСНИХ УМОВАХ ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНОГО ПРОСТОРУ УКРАЇНИ

Зважаючи на глобалізацію інформаційних процесів, їх інтеграцію в різні сфери суспільного життя провідні держави світу приділяють посилену увагу створенню та удосконаленню ефективних систем захисту від зовнішніх і внутрішніх загроз кібернетичного характеру. На цей час кіберзахист є одним із пріоритетних напрямів державної політики в Україні.

Так Стратегією кібербезпеки України, затвердженою Указом Президента України від 15.03.2016 № 96/2016, однією із необхідних запорук створення умов для безпечного функціонування кіберпростору відзначається забезпечення кіберзахисту державних електронних інформаційних ресурсів [3].

Статтею 1 Закону України «Про основні засади забезпечення кібербезпеки України» (далі – Закон) поняття кіберзахисту визначено як сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем. Функція кіберзахисту відповідно до Закону нерозривно пов'язана із досягненням безпеки кіберпростору. Основними суб'єктами національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України [1].

Зважаючи на зазначене на цей час є важливим комплектування новоутворених підрозділів кіберзахисту якісними кадрами та подальший їх належний професійний розвиток.

Статтею 8 Закону забезпечення функціонування національної системи кібербезпеки здійснюється у тому числі шляхом підготовки відповідних фахівців через державне замовлення, підвищення їх кваліфікації та проведення обов'язкової періодичної атестації (переатестації) персоналу, відповідального за забезпечення кібербезпеки об'єктів критичної інфраструктури, з урахуванням міжнародних стандартів.

Щодо існуючих на цей час внормованих вимог до посад, які можливо використати при підборі кадрів до підрозділів кіберзахисту, то у випадку заміщення вакантних посад державних службовців використовуються загальні вимоги до кандидатів зазначені у Законі України «Про державну службу». Але вони можуть бути застосовані тільки до кандидатів на посади державних службовців та носять занадто загальний характер, не враховуючи особливості майбутньої професійної діяльності [2].

За результатами аналізу досліджень вітчизняних науковців з цієї теми слід відзначити праці І.В. Діордіца, у яких він надає наукове обґрунтування кваліфікаційних вимог до фахівців із кібербезпеки, відстежує алгоритм розроблення кваліфікаційних вимог в аспекті освітньої діяльності. Водночас науковець робить висновок, що практиці підбору кадрів бракує науково обґрунтованих кваліфікаційних характеристик фахівців, без яких забезпечення безпеки в інформаційно-комунікативному просторі стає доволі проблематичним [4].

Також тему підбору кадрів до підрозділів інформаційної безпеки частково висвітлено у працях В.Л. Бурячка. Автор зауважує, що підвищення компетентності фахівців різних сфер діяльності у питаннях кібербезпеки можливе за рахунок: розроблення і впровадження програми навчання фахівців у галузі кібербезпеки, здатних до прогнозування можливих ризиків від кібернападів та оцінювання їх наслідків; реалізації механізмів набору персоналу необхідної кваліфікації для забезпечення кібербезпеки державних ІТ-систем і мереж тощо [5].

Крім зазначеного науковець вказує, що створенню дієздатної системи протидії внутрішнім і зовнішнім загрозам власному інформаційному та кіберпростору Україні заважає низка проблем, у тому числі незадовільне кадрове забезпечення кваліфікованими фахівцями , правоохоронних органів та силових структур України, що спеціалізуються на проблемах кіберзахисту.

Таким чином на цей час важливим є теоретичне обґрунтування та практичне визначення кваліфікаційних вимог до спеціалістів сфери кіберзахисту, розроблення методів підбору кадрів з урахуванням особливостей професійної сфери. Зазначене допоможе здійснювати якісніший підбір кадрів підрозділів кіберзахисту, визначить пріоритети у роботі служб персоналу.

**Література**

1. Про основні засади забезпечення кібербезпеки України / Закон України від 05.10.2017 № 2163-VIII // Урядовий кур’єр від 15.11.2017 – 2017 р., № 215;

2. Про державну службу / Закон України від 10.12.2015 № 889-VIII // Урядовий кур’єр від 03.02.2016 – 2016 р., № 21.

3. Про Стратегію кібербезпеки України / Указ Президента України від 15.03.2016 № 96/2016 // Урядовий кур'єр від 18.03.2016 – 2016 р., № 52.

4. І.В. Діордіца, Кваліфікаційні вимоги до компетенцій фахівців із кібербезпеки: стаття // Підприємництво, господарство і право 2/2017.

5. 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, В. Б. Толубка. – К.: ДУТ, 2015. – 288 с.

*УДК 351.002.8*

**Сорока С.А.**
Національна академія державного управління
при Президентові України

## СТАНОВЛЕННЯ ТА РОЗВИТОК НОРМАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ СФЕРИ КІБЕРБЕЗПЕКИ В УКРАЇНІ

Виклики сьогодення потребують повноцінного нормативно-правового регулювання сфери кібербезпеки держави, його відповідності політичним реаліям, рівню технологічного розвитку, нормам міжнародного права, а також ефективному захисту національних інтересів України. Наявність потенційних і реальних загроз у сфері кібербезпеки негативно впливає на суспільний розвиток українського суспільства та реалізацію його євроінтеграційних прагнень.

Внаслідок посилення ролі та значення інформації в життєдіяльності суспільства, розвитку та доступності технологій, все більшої актуальності в системі Національної безпеки України набуває забезпечення її інформаційної складової, зокрема кібербезпеки держави. Саме тому, в статті 17 Конституції України закріплюється, що захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу [1].

Загалом вітчизняне законодавство в сфері інформаційної безпеки почало інтенсивно розвиватись на початку та особливо в середині 90-х років XX століття. Саме в цей період були прийняті основоположні нормативно-правові акти, серед яких закони України «Про інформацію» [2], «Про державну таємницю» [3], «Про науково-технічну інформацію» [4] та інші.

Однак, лише після революції Гідності питанням інформаційної безпеки, а особливо кібербезпеки приділяється більше уваги. Так, Указом Президента України було оприлюднене рішення Ради національної безпеки і оборони України від 28 квітня 2014 р. «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної без-

пеки України» [5]. Указом Президента України від 25 лютого 2017 року № 47/2017 уведено в дію рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» [6].

Але разом з розвитком новітніх технологій зростали і масштаби кібератак, кіберзлочинності та кібертероризму. Варто пригадати найбільшу за всю історію України кібератаку на комп'ютерні системи фінансових установ, енергетичних підприємств, засобів масової інформації, об'єктів транспорту та інфраструктури, телекомунікаційних мереж та інших великих організацій. Вірус Petya. А частково паралізував роботу транспортних підприємств: аеропорту «Бориспіль», на сайті якого перестала оновлюватися інформація про розклад рейсів, і столичного метрополітену, зробивши неможливою оплату за проїзд безконтактними банківськими картами. Ускладнилася робота банків: державного «Ощадбанку» та низки комерційних банків. Впали системи «Укренерго», «Укрпошти» і «Нової пошти», «Укрзалізниці», «Укртелекому», великих мережевих супермаркетів, засобів масової інформації, зокрема телеканалів.

Завдяки безпосередньої участі провідних фахівців Державної служби спеціального зв'язку та захисту інформацій України (Адміністрації Держспецзв'язку) та за участі міжнародних експертів (США, Канади, Європейського союзу) було розроблено Закон України «Про основні засади забезпечення кібербезпеки України» (далі – Закон), який згодом було ухвалено вітчизняним парламентом та набирає чинності 9 травня 2018 року. Цей Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки. Суб'єктом, що забезпечує формування та реалізацію державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, визначено Державну службу спеціального зв'язку та захисту інформації України [7].

Проте необхідно зауважити, що досі в Україні не прийнято закону, який би визначав концепцію державної інформаційної політики України. Відповідно, в країні не існує єдиного плану, єдиної державної позиції чи стратегії розвитку інформаційної галузі, а отже, і забезпечення інформаційної і кібербезпеки держави.

У швидкоплинному перебігу подій суспільного життя, з революційними процесами у розвитку інформаційних технологій значна частина чинних нормативних актів як внутрішньодержавних, так і міжнародних поступово втрачає актуальність, відповідність процесам, які ними норму-

ються, і потребує уточнень та доопрацювань. Розвиток інформаційної діяльності створює необхідність правового урегулювання нових аспектів цієї діяльності. Потребує досконалого нормативно-правового обґрунтування питання організації ефективного протистояння кіберзлочинності в умовах активізації глобальних впливів, нових цифрових технологій. Комплекс відповідних правових актів має постійно вдосконалюватися із урахуванням відповідного міжнародного законодавства, його еволюції і вітчизняної законотворчої практики, що має бути на варті інтересів національної інформаційної діяльності.

Для вирішення насущних проблем сфери кібербезпеки України основні зусилля необхідно направити на створення ефективної системи захисту національного інформаційного простору, подолання колізій та прогалин у чинному інформаційному законодавстві, попередження порушення інформаційних прав і свобод людини та громадянина, ухвалення Закону України "Про Національну безпеку України".

**Література**

1. Конституція України : закон України від 28 червня 1996 р. № 254к/96 // Відомості Верховної Ради України. – 1996. – № 30. – Ст. 141.

2. Про інформацію: закон України від 2 жовтня 1992 р. № 2657-XII// Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650.

3. Про державну таємницю: закон України від 21 січня 1994 р. № 3855-XII// Відомості Верховної Ради України. – 1994. - № 16. – Ст. 93.

4. Про науково-технічну інформацію: закон України від 25 червня 1993 р. № 3322-XII// Відомості Верховної Ради України. – 1993. – № 33. – Ст. 345.

5. 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": указ Президента України від 01 травня 2014 р. № 449 // Офіційний вісник Президента України. – 2014. – № 16. – Ст. 982.

6. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: указ Президента України від 29 грудня 2016 р. № 47 // Урядовий кур’єр. – 2017. - № 38. – Ст. 98.

7. Про основні засади забезпечення кібербезпеки України: закон України від 05 жовтня 2017 р. № 2163-XIX// Відомості Верховної Ради України. – 2017. – № 45. – Ст. 403.

*УДК 343.953*
**Тарасюк А. В.**
аспірант відділу аспірантури і докторантури
Національна академія СБ України

# ВИКОРИСТАННЯ МЕТОДУ ПРОФАЙЛІНГУ СПІВРОБІТНИКАМИ ПРАВООХОРОННИХ ОРГАНІВ ДЛЯ ВИРІШЕННЯ ПРОБЛЕМ У СФЕРІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

У даних тезах розглянуті актуальні проблеми використання методу профайлингу для забезпечення інформаційної безпеки України. Надана комплексна оцінка перспектив застосування вказаного методу з точки зору науково-теоретичних положень та прикладних основ науки оперативної психології.

Професійне спілкування співробітників правоохоронних органів є обов'язковим та важливим елемент їх службової діяльності, у процесі якого здійснюється організація взаємодії з різними категоріями осіб. Таке спілкування має свою специфіку, зумовлену професійною метою, обсягом наявної інформації, умовами взаємодії, ймовірністю виникнення негативних психічних станів (стресу, нервово-психічного напруження, тривожності, агресивності тощо) та індивідуально-психологічними особливостями співрозмовників [1, с. 31].

Для ефективного вирішення покладених завдань із забезпечення інформаційної безпеки співробітники правоохоронних органів мають бути добре обізнаними із методами і способами психології та вдало використовувати їх у своїй безпосередній роботі.

Як свідчить практика, найчастіше дуже складно достовірно проаналізувати глибині мотиви людської поведінки, у тому числі і поведінки об'єктів, що проходять за контррозвідувальними чи оперативно-розшуковими справами, без якісного знання психології особистості, психологічних механізмів та мотивів, соціально-психологічних явищ і процесів. Проте психологічним аспектам у забезпеченні інформаційної безпеки правоохоронними органами не надається належної уваги, не дивлячись на те, що дефіцит спеціальних психологічних знань найчастіше не дозволяє правоохоронцям якісно здійснювати свою службову діяльність.

Одним із проблемних аспектів психологічного забезпечення інформаційної безпеки держави є процес діагностики та оцінки індивіда. У вказаному контексті з тих, що проводяться у теперішній час, науково-практичних дослідженнях можна виокремити методику складання психологічного профілю (профайлинга) як перспективний напрямок підвищення ефективності професійної діяльності правоохоронних органів [1, с. 237].

На думку Е.С. Черкасовой, терміном «профайлинг» позначається два різнопланових контексти діяльності правоохоронних органів. Перший контекст – створення психологічного профілю неустановленого об'єкта, причетного до правопорушення, на основі якого цей об'єкт підлягає встановленню та притягненню до відповідальності за скоєний злочин. Другий контекст – технології спостереження і опитування пасажирів у ході огляду при проходженні реєстрації на рейс, з метою виявлення потенційно небезпечних осіб перед авіаперельотом. Даний напрямок активно реалізується в авіаційній безпеці з залученням фахівців-психологів зі спеціалізацією у галузі біхевіоризму (напрямок наукового психологічного знання в області поведінки) [2, с. 5].

Сучасні дослідження у визначенні терміну «профайлинг» містять у собі об'єднання психологічних методів і методик оцінки мотиваційної диспозиційної сторони особистості та прогнозування поведінки людини на основі аналізу найбільш інформативних ознак. Сукупність характеристик зовнішності, невербальної, вербальної поведінки, мотивація, планування і реалізації злочинного діяння забезпечувати якісне наповнення даного терміну, дозволяючи складати психологічний профіль (портрет) особистості [1, с. 239].

Ефективне досягнення цілей з забезпечення інформаційної безпеки держави, пов'язаних з застосуванням методу психологічного профайлинга, буде неможливим без створення функціонування системи науково-методичного забезпечення службової діяльності правоохоронних органів. Погоджуючись з думками деяких науковців вважаємо, що використання вищезгаданого напрямку на рівні професійної компетенції в процесі виявлення, попередження та запобіганні протиправних дій об'єктів службової зацікавленості, внести свій вклад у підвищення ефективності професійної діяльності у напрямку забезпечення інформаційної безпеки правоохоронними органами України.

**Література**

1. Коробков В.А., Ведин А.В. Основные направления применения в оперативно-розыскной деятельности методики составления психологического профиля. URL: http://cyberleninka.ru (дата звернення 27.02.2018).

2. Черкасова Е.С Психологический портрет лица, совершившего насильственное приступление, профайлинг как современное направление психологической науки. URL: http://www.rusnauka.com/26_WP_2013/ Psihologia/7_144300.dok.htm (дата звернення 27.02.2018).

*УДК 35.746.1*
**Фецан В. В.**
магістр
Національна академія СБ України
**Тугарова О.К.**
кандидат юридичних наук, доцент
Національна академія СБ України

# СУТНІСТЬ, НАПРЯМИ ТА ЗАВДАННЯ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ

Термін “політика” походить від давньогрецького слова polis (місто-держава) і розуміється як діяльність самоуправління в полісі (місто, держава), «мистецтво управління» державою і суспільством). У словниках термін «політика» визначається як загальний напрямок, характер діяльності держави [1].

Державна інформаційна політика є важливою складовою зовнішньої та внутрішньої політики країни й охоплює всі сфери життєдіяльності суспільства.

Державна інформаційна політика – це сукупність напрямів та способів діяльності держави з контролю, регулювання та планування процесів у сфері одержання, зберігання, оброблення, використання та поширення інформації. Держава регулює розподіл інформаційних ресурсів, встановлює пріоритети для забезпечення національних інтересів, загальні принципи інформаційної діяльності та ін. Саме інформаційна політика стає основним засобом вираження позиції держави і управління інформаційними процесами під час переходу країни в іншу формацію – до інформаційного суспільства [2, с. 101-102].

Основними напрямами державної інформаційної політики є: формування та захист державних інформаційних ресурсів; забезпечення умов для розвитку інформаційних ресурсів; створення умов для якісного та ефективного інформаційного забезпечення громадян, органів державної влади та місцевого самоврядування, організацій та суспільних об’єднань на основі державних інформаційних ресурсів; створення та розвиток центральних й регіональних інформаційних мереж та систем, забезпечення їх сумісності та взаємодії в єдиному інформаційному просторі держави; сприяння формуванню ринку інформаційних ресурсів та послуг, інформаційних систем та технологій, засобів їх забезпечення; формування та реалізація єдиної науково-технічної промислової політики в сфері інформатизації; створення та вдосконалення системи інвестування й механізму стимулювання розробки та реалізації проектів інформатизації; розвиток зако-

нодавства у цій сфері, захисту інформації та інформаційних процесів у цілому; сприяння міжнародному співробітництву в галузі інформації й гарантування інформаційного суверенітету.

Основні акценти державної інформаційної політики повинні базуватись на: забезпеченні права на достовірну, повну та своєчасну інформацію, свободу слова та інформаційної діяльності, недопущення втручання в зміст та внутрішню організацію інформаційних процесів, крім випадків, визначених законодавством; збереженні та вдосконаленні національного інформаційного продукту та технологій, забезпеченні інформаційної та національної культурної ідентифікації країни у світовому інформаційному просторі; гарантуванні державної підтримки та розвитку ресурсів науково-технічної продукції та інформаційних технологій.

Загальноприйняте визначення інформаційної політики у вузькому розумінні будується навколо питання доступу до урядової інформації. Але вперше урядами країн було використано поняття «інформаційна політика» у період Першої світової війни для позначення пропагандистської діяльності. І тільки у 1970-1980х рр. уряди різних країн зайнялися розробкою цілісної категорії «державна інформаційна політика».

Загалом наукові підходи до визначення сутності поняття «державна інформаційна політика» дуже різняться: від глобального керівництва інформаційною сферою до звуженого розуміння інформаційної політики як процесу забезпечення діяльності засобів масової інформації.

Оскільки зазначені питання виникли в умовах зародження та становлення інформаційного суспільства, сьогодні вони набувають дедалі більшої актуальності, що пов’язано з переходом діяльності сучасної держави в транскордонний цифровий вимір, збільшенням ролі та впливу інформації на забезпечення національної та міжнародної безпеки, а відтак необхідністю удосконалення державної інформаційної політики.

Загалом, напрями державної інформаційної політики повинні базуватися на національних інтересах України і враховувати наявні загрози в інформаційній сфері . Основні завдання державної інформаційної політики у розрізі прийняття та удосконалення нормативно-правових актів повинні включати: створення розвиненого інформаційного середовища; ефективне формування й використання національних інформаційних ресурсів, забезпечення вільного доступу до них; розвиток інформаційних та телекомунікаційних технологій; модернізація інформаційної інфраструктури; розвиток незалежних ЗМІ й забезпечення громадян суспільно важливою інформацією; сприяння міжнародному співробітництву в інформаційній сфері та утвердження інформаційного суверенітету держави; запобігання загрозі заподіяння шкоди життєво важливим інтересам особи, суспільства та держави в процесі інформаційної діяльності.

**Література**

1. Великий тлумачний словник сучасної української мови / уклад. і голов. ред. В.Т.Бусел. – К. : ВТФ “Перун”, 2005. – 1725 с.

2. Бєляков К.І. Інформатизація в Україні: проблеми організаційного, правового та наукового забезпечення: моногр. / К.І. Бєляков. – К.: КВІЦ, 2008. – 576 с.

*УДК 005.7:355/359*

**Щербина Д.С.**
Державний науково-дослідний інститут
спеціального зв’язку та захисту інформації
Державної служби спеціального зв’язку
та захисту інформації України

# ПІДГОТОВКА ФАХІВЦІВ ЯК ПРОБЛЕМА У СФЕРІ БЕЗПЕКИ ІНФОРМАЦІЇ ДЕРЖАВИ

У сучасному суспільстві важливу роль відіграє інформаційна складова державних відносин. Отже, існує необхідність збереження, державних таємниць та службової інформації була на вищому рівні. Для цього потрібні професіонали, здатні захищати інформацію на усіх рівнях її обігу. Таких фахівців готують в спеціальних вищих навчальних закладах, наприклад: Академія служби безпеки України, Інститут спеціального зв’язку та захисту інформації «КПІ» ім. І. Сікорського та інші. Ціль таких ВНЗ - навчити захищати інформаційний простір України, інформацію з грифами таємності, забезпечувати стабільний та безпечний обіг інформації органів державної влади, оберігати кіберпростір держави, тощо. Саме ці заклади повинні мати передове навчання та високу підтримку держави.

На даний час, виникла проблема у недосконалості заходів для комплексної підготовки майбутніх фахівців протистояти сучасним загрозам, а також для підвищення кваліфікації вже працюючого персоналу. Недостатнє фінансування, застаріла та дуже обмежена матеріально-технічна база та погано вмотивовані викладачі, ці фактори суттєво знижують кількість висококваліфікованого персоналу. В подальшому, це призводить до неможливості захищатися від вірусних атак, перехоплення та викрадення державних таємниць, втручання чужих держав у інформаційний простір України, ЗМІ підконтрольні іноземцям, вплив на населення через інформаційних агентів, незахищені урядові інформаційні джерела і т. д.

Існування внутрішніх та зовнішніх загроз повинно підштовхувати державу в підтримці науковців у сфері захисту інформації та кіберзахисту. Адже, саму наука рухає прогрес у сфері технологій. Тому необхідно постійно вдосконалювати методи підготовки відповідно міжнародним стан-

дартам, корегувати навчальні програми у навчальних закладах, для якіснішої освіти фахівців. Нині, інформація – це один із стратегічних національних ресурсів держави, тому важливо її захищати відповідно за сучасними нормами. Отже, у зміст навчання фахівців мають бути додані сучасні знання у сфері технологій, інформаційного простору та безпеки інформації. Також, варто оновлювати програми навчання відповідно із розвитком технологій у всьому світі.

Неабияку, роль у розвитку в сфері забезпечення інформаційної безпеки, відіграють міжнародні взаємодії. Адже, обмін знаннями – значний внесок додає у вітчизняну науку. Нові ідеї, системи, програми, комплекси, винаходи, ноу-хау, все це необхідно знати і вивчати для подальшого прогресу. На сьогодні, вже не одна країна у світі використовує систему блокчейн (англ. blockchain) в багатьох сферах державного життя. Це розподілена база даних, яка підтримує перелік записів, так званих блоків, що постійно зростає. Така технологія дозволяє, щоб дану базу було повністю захищено від підробок та переробок. Сфери застосування технології різноманітні: захищений документообіг, створення платформ для надання адміністративних послуг, банківські операції і т.д. Велика Британія, Естонія, Фінляндія, США – ці країни вже використовують дану систему у своїх державних установах та сфері національної безпеки. Тож, чому Україні не використати досвід інших країн та не впроваджувати сучасні системи, для захисту інформації в державі?

**Література**

1. Закон України "Про інформацію", прийнятий Верховною Радою України 2 жовтня 1992 р. // ВВР України. - 1992. - № 48. - Ст. 651; Із змінами від 6 квітня 2000 р. – 2000. – № 27. – Ст. 213; від 7 лютого 2002 р. – ВВР. – 2002. – № 29. – Ст. 194; від 3 квітня 2008 р. – ВВР. – 2003. – № 28. – Ст. 214.

2. Закон України "Про Державну службу спеціального зв’язку та захисту інформації" від 23 лютого 2006 р. // ВВР України. – 2006. – № 30. – Ст. 258.

3. Інформаційна безпека сучасного суспільства: навч. посіб. / за заг. ред. А. І. Міночкіна. – К.: ВІГІ НТУУ "КГП", 2006. –188 с., Інформаційна безпека держави у контексті протидії інформаційним війнам : навч. посіб. / за заг. ред. В. Б. Толубка. – К.: НАОУ, 2004. – 315 с.

## ЗМІСТ

## РОЗВИТОК СТРАТЕГІЧНИХ КОМУНІКАЦІЙ ЯК ПЕРЕДУМОВА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

## УДОСКОНАЛЕННЯ СИСТЕМИ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ ТА СЛУЖБОВОЇ ІНФОРМАЦІЇ УКРАЇНИ З УРАХУВАННЯМ ДОСВІДУ ПРОВЕДЕННЯ АТО

## ПОГЛЯД НА ПРОБЛЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ МОЛОДИХ УЧЕНИХ І СТУДЕНТІВ

Наукове видання

# АКТУАЛЬНІ ПРОБЛЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ

## IX Всеукраїнська науково-практична конференція

Збірник тез наукових доповідей
(Київ, 30 березня 2018 року)

*Електронна версія*

Авторська редакція

Технічне редагування, макетування *Т. О. Коркач*

Формат 60x84/16.
Ум. друк. арк. 24,03. Обл.-вид. арк. 23,71.

Видавець і виготовлювач
Національна академія Служби безпеки України,
вул. М. Максимовича, 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