**НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ**
**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**

НАЦІОНАЛЬНА АКАДЕМІЯ ПРАВОВИХ НАУК УКРАЇНИ
НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ІНФОРМАТИКИ І ПРАВА

# ІНФОРМАЦІЙНА БЕЗПЕКА: ВИКЛИКИ І ЗАГРОЗИ СУЧАСНОСТІ

ЗБІРНИК МАТЕРІАЛІВ
НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ,
5 квітня 2013 р., м. Київ

Київ
Центр навчально-наукових та науково-практичних видань
Національної академії СБ України
2013

Рекомендовано до друку Вченою радою
Навчально-наукового інституту інформаційної безпеки
Національної академії Служби безпеки України,
протокол № 9 від 27.05.2013 р.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ КОНФЕРЕНЦІЇ

**Співголови:** *Шмоткін О.В.*, кандидат юридичних наук, професор, заслужений юрист України; *Пилипчук В.Г.*, доктор юридичних наук, професор, член-кореспондент НАПрН України.

**Заступники голови:** *Фурашев В.М.*, кандидат технічних наук, старший науковий співробітник, доцент; *Хлевицький В.Б.*, кандидат юридичних наук, старший науковий співробітник.

**Члени організаційного комітету:**

*Бровко В.Д.,* кандидат технічних наук; *Марущак А.І.,* доктор юридичних наук, професор; *Панченко В.М.,* кандидат юридичних наук, старший науковий співробітник; *Остроухов В.В.,* доктор філософських наук, професор; *Мельник С.В.,* кандидат технічних наук; *Леонов Д.Б., Філоненко І.О.*

**Інформаційна безпека: виклики і загрози сучасності** : зб. матеріалів наук.-практ. конф., 5 квітня 2013 року, м. Київ. – К. : Наук.-вид. центр НА СБ України, 2013. – 416 с.

Уміщено матеріали, підготовлені фахівцями та науковцями Служби безпеки України, Науково-дослідного інституту інформатики і права НАПрН України, Військового інституту Київського національного університету імені Тараса Шевченка, Національного авіаційного університету, Національного університету оборони України, інших установ і організацій.

Тези доповідей публікуються в авторській редакції з незначними коректорськими правками.

© НА СБ України, 2013

# ВСТУПНЕ СЛОВО

*Шановні учасники та гості конференції!*

Дозвольте привітати вас з відкриттям нашого наукового форуму, присвяченого з'ясуванню актуальних загроз та викликів інформаційній безпеці й пошуку ефективних шляхів протидії їм.

За умов глобалізації інформаційних процесів, формування світового інформаційного простору, швидкого зростання світового ринку інформації постає нагальна потреба у правовому регулюванні суспільних відносин, пов'язаних із формуванням національного інформаційного простору, забезпеченням інформаційної безпеки держави. Поряд із правовими механізмами захисту національних інтересів в інформаційній сфері значно зростає роль економічних важелів регулювання інформаційних відносин.

Про нерозривний зв'язок економічної та інформаційної безпекових сфер красномовно свідчать підсумки цьогорічного опитування експертів на Всесвітньому економічному форумі у Давосі. На думку респондентів, одними із найбільш серйозних проблем для людства у наступному десятиріччі стануть кібератаки та вірусне поширення неправдивої інформації через сучасні комунікаційні засоби.

Тому сьогодні одним із пріоритетних завдань суб'єктів забезпечення інформаційної безпеки є дотримання балансу між захистом національних інтересів в інформаційній сфері, гарантуванням політичної, економічної та соціальної стабільності у державі та розвитком рівноправного, взаємовигідного міжнародного співробітництва, реалізацією конституційних прав і свобод людини та громадянина на отримання й використання інформації, розбудовою інформаційної інфраструктури країни.

Навколо цього вкрай непростого питання не один рік точиться дискусія у суспільстві, що відбивається насамперед у підходах до формування інформаційного законодавства. Очевидно, що вирішення цієї проблеми потребує часу та глибокого наукового осмислення. На нашу думку, системоутворювальною основою для її розв'язання є формування критеріїв визначення рівня загроз національній безпеці та їх співвідношення з показниками, які характеризують рівень обмежень прав і свобод, що запроваджуються законодавцем у зв'язку з вимогами безпеки.

Цей захід спрямований на інтеграцію зусиль представників різних наукових відомств на вирішення зазначеної проблеми. З метою якісної і плідної співпраці робота конференції планується за напрямками, які представлені такими секціями:

Секція 1. Державно-правові проблеми інформаційної безпеки.

Секція 2. Актуальні питання захисту інформації: технічні та технологічні аспекти.

Секція 3. Протидія сучасним технологіям деструктивного інформаційно-психологічного впливу.

Секція 4. Інформаційна безпека очима молодих дослідників (для студентів та курсантів).

Окремо хотів би звернутися до молодих дослідників. Саме ви є найбільш активними користувачами новітніх технологій. Отже, ви, як ніхто інший, маєте знати їх переваги та уразливі місця. А відтак сподіваємося, що, застосувавши отримані в Академії знання у галузі права, зможете представити нові наукові результати в інтересах забезпечення інформаційної безпеки.

На завершення зауважу, що завдяки унікальному геополітичному розташуванню нашої країни, багатству духовного та історичного спадку українського народу, Україна має стати сильною, непохитною, демократичною, інформаційно розвиненою державою і посісти гідне місце у глобалізованому світі. Тому вважаю, що основною метою реалізації державної політики у сфері забезпечення інформаційної безпеки є виконання двоєдиного завдання: створення розвиненого інформаційного простору і захист національного інформаційного суверенітету.

Запрошую всіх учасників конференції до співпраці, конструктивного діалогу та плідної наукової дискусії.

Бажаю успіхів та дякую за увагу!

*Перший проректор*
*Національної академії СБ України,*
*кандидат юридичних наук,*
*старший науковий співробітник*
*Довгань О.Д.*

# ПЛЕНАРНІ ДОПОВІДІ

*Бурячок В.Л.,*
*кандидат технічних наук,*
*старший науковий співробітник,*
*військова частина А1906 Міністерства оборони України*

*Гнатюк С.О.,*
*кандидат технічних наук,*
*Національний авіаційний університет*

*Корченко О.Г.,*
*доктор технічних наук, професор,*
*Національний авіаційний університет*

## ХАРАКТЕРНІ ОЗНАКИ ТА ПРОБЛЕМНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Неконтрольоване поширення та необмежене застосування інформаційного і кіберпросторів [1, 2] протягом останніх десятиріч:

1) призвело до *уразливості інформаційної сфери* більшості країн світу *для стороннього кібернетичного впливу;*

2) визначило політичну необхідність *контролю і подальшого регулювання відносин* у цій царині;

3) дало підстави стверджувати про *особливу актуальність:* процесів *пошуку, збирання й добування інформації* у відкритих, відносно відкритих і закритих електронних джерелах; заходів із *забезпечення конфіденційності, цілісності та доступності* власного ІР, а також *протидії цілеспрямованому впливу з боку потенційно можливих кібернетичних втручань і загроз.*

Зважаючи на це та враховуючи постійно зростаючий потенціал використання мережі Internet у військових цілях, провідні країни світу – США, Японія, Франція, Велика Британія, Росія, Китай та багато інших протягом останніх років активно модернізують власні сектори безпеки [1] й, передусім, безпеки кібернетичної, відводячи при цьому головну роль проблемі завоювання інформаційної переваги в управлінні військами (силами) і зброєю, а також удосконаленню нормативно-правової бази. У практику збройної боротьби вони активно впроваджують концепцію інформаційного протиборства, яка передбачає ведення активних розвідувальних дій щодо об’єкта нападу або потенційного порушника та дій, спрямованих на

захист національних інтересів від впливу внутрішніх і зовнішніх кібернетичних втручань та загроз. Наслідком таких дій невдовзі можуть стати так звані кібернетичні війни [3], основними методами ведення яких на тактичному рівні вже нині визнані кібератаки, а на стратегічному та спеціальному рівнях – кібероперації. Практично всі вони в умовах сьогодення досягають очікуваного від них результату. Підтвердженням цьому є атаки, спричинені вірусами Stuxnet і Hydraq – двома найпомітнішими кіберподіями 2010 року, троянськими вірусними програмами Duqu та Flame (2011 рік), Mahdi та Gauss (2012 рік), а також події навколо сайту Wikileaks, які кардинально змінили межі загроз та показали усьому світу, що можливості кіберзброї можуть бути досить вражаючими, а протидія її негативному впливу може виявитися вкрай складним завданням для сторін, що захищаються.

Такий стан справ дає підстави стверджувати, що відсутність надійної системи кібернетичної безпеки (*стан захищеності кіберпростору в цілому або окремих об'єктів його інфраструктури та засобів їх взаємодії від ризику стороннього кібернетичного впливу*) може призвести до втрати політичної незалежності будь-якою державою світу, тобто до фактичного програшу нею війни невійськовими засобами та підпорядкування її національних інтересів інтересам іншої (протиборчої) сторони (рис. 1) [1, 2].


Рис. 1. Складові кібернетичної безпеки

Характерними ознаками, які нині визначають поняття кібербезпеки, є *сукупність активних захисних і розвідувальних дій, що в процесі інформаційного протиборства зусиллями поодиноких інсайдерів або організованих кіберугруповань розгортаються навколо інформаційного ресурсу (ІР), інформаційно-комунікаційних технологій (ІКТ) та інформаційно-телекомунікаційних систем (ІТС)* [4], та які спрямовані на досягнення і утримання потенційними протиборчими сторонами переваги у протидії новим загрозам безпеці для власних об'єктів критично важливої інформаційної і кіберінфраструктури. Останнім часом такі дії займають чільне місце у геополітичній конкуренції переважної більшості країн світу, що, у свою чергу, зумовлює нові завдання їх збройних сил й виводить на пер-

ший план проблеми так званого інформаційного протиборства. Серед причин такої ситуації можна назвати:

– *відсутність або недосконалість нормативно-правової бази,* яка б забороняла застосування інформаційної і кіберзброї, проведення інформаційних і кібероперацій, а також встановлювала б відповідальність протиборчих сторін за здійснення злочинів у ІТ сфері;

– *формування* окремими державами власних доктрин і стратегій *наступальних та підривних дій в інформаційному і кіберпросторах;*

– *створення та застосування* спеціальних сил і засобів *негативного впливу на критично важливу інформаційну і кіберінфраструктуру;*

– *проникнення ІТ в усі сфери державного й громадського життя,* побудова на їх основі систем державного і військового управління;

– *розвиток державних проектів і програм у сфері інформатизації* (електронний документообіг, міжвідомча електронна взаємодія, універсальні електронні карти, надання державних послуг в електронній формі), спрямованих на формування інформаційного суспільства, тощо.

Україна як самодостатня і суверена держава з часу здобуття незалежності шляхом налагодження співробітництва з міжнародними інституціями прагне створити комплексну систему протидії внутрішнім і зовнішнім загрозам власному кібернетичному простору. Проте, як зазначають вітчизняні й західні фахівці, нині існує ціла низка проблем, що заважають нашій державі, яка прагне до ЄС, це зробити. До *найбільш значущих* серед них слід віднести [1]:

– деградацію науково-технічного потенціалу України, нерозвиненість національної інноваційної системи в інфосфері та низький рівень конкурентоспроможності в ній;

– значну уразливість інфосфери України через надмірно широке впровадження у ній західних програмних продуктів (зокрема фірми Microsoft) та використання матеріально-технічних засобів іноземного виробництва;

– непрозорість розподілу обов’язків між певними відомствами, правоохоронними органами і силовими структурами України, що спеціалізуються на проблемах кіберзахисту, та їх незадовільне кадрове забезпечення відповідними кваліфікованими фахівцями;

– відсутність загальнонаціонального координаційного центру, спроможного узгоджувати й координувати діяльність зазначених вище правоохоронних органів, силових структур і відомств щодо протидії реальним загрозам інформаційному і кіберпросторам України, та керувати проведенням комплексних навчань із забезпечення кібернетичної безпеки держави в інфосфері на кшталт

“Cyber Storm”, які проводяться у США, та/або “Cyber Europe”, що проводяться у ЄС;

– відсутність єдиного понятійно-термінологічного поля кібербезпеки України як головної складової інформаційної безпеки, а також системних нормативно-правових документів, які б регламентували діяльність зазначених відомств, правоохоронних і силових структур у сфері кіберзахисту, тощо.

Такий стан справ фактично є каталізатором для реалізації втручань і загроз в інфосферу України, результатом чого може стати порушення управління державою, її інституціями та окремими об’єктами критично важливої інформаційної і кіберінфраструктури, виникнення техногенних катастроф тощо. Це, у свою чергу, потребує від керівництва нашої держави як розроблення національної стратегії кібернетичної безпеки, котра має чітко визначити мету, завдання та пріоритети такої діяльності, а також структури, відповідальні за реалізацію заходів щодо протидії сторонньому кібервпливу, так і формування в межах окремої цільової програми державної системи кібербезпеки, варіант структурно-функціональної моделі формування якої наведено на рис. 2:

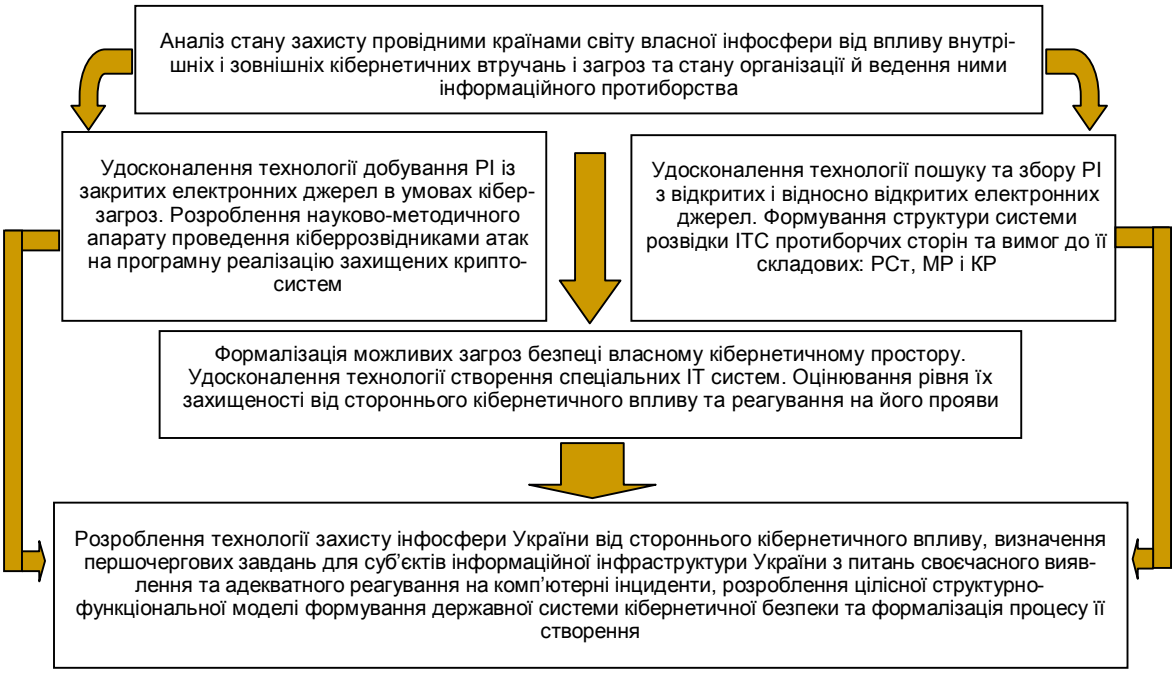



Рис. 2. Структурно-функціональна модель формування системи кібернетичної безпеки

Досвід іноземних країн та особливості українських реалій свідчать, що розв’язання основних завдань кібербезпеки неможливе без створення [1, 2]:

1) міжвідомчого структурного органу, який на постійній основі забезпечував би координацію діяльності певних відомств, правоохоронних і силових структур України з питань забезпечення кібернетичної безпеки;

2) центральних органів у структурі певних відомств, правоохоронних і силових структур України з функціями виявлення та оцінювання рівня (визначення ступеня) критичності стороннього кібервпливу, розробки концептуальних засад та надання рекомендацій щодо протидії його проявам, а також активної протидії кібератакам протиборчих сторін та впливу на їх ІТС;

3) органів власної інформаційної і кібербезпеки державних установ (відомств) та комерційних структур, які повинні тісно взаємодіяти із зазначеними центральними органами з питань вироблення єдиної політики щодо захисту як власного, так і спільного національного інформаційного і кіберпросторів.

Не виняток і галузь цивільної авіації, на суб'єктах якої (повітряні судна, авіакомпанії, аеропорти тощо) циркулює значна кількість *державних інформаційних ресурсів* [5, 6]. Умови функціонування цивільної авіації швидко і суттєво змінюються із впровадженням сучасних технологій обробки, передачі та збереження інформації, що забезпечують підвищення рівня захисту і спрощення формальностей. Найбільшого захисту потребують ресурси *критичних авіаційних інформаційних систем (КАІС),* до яких, серед іншого, належать системи: контролю доступу та охоронної сигналізації; контролю вильоту; організації повітряного руху; дистанційного технічного обслуговування; бронювання та реєстрації пасажирів; диспетчерські системи тощо [7].

Основними нормативними документами, що регламентують процеси захисту цивільної авіації від кіберзагроз, є [7-9], проте у жодному з них *не дається вичерпний перелік КАІС,* що значно ускладнює аналіз їх уразливостей і унеможливлює організацію ефективної комплексної системи інформаційної безпеки. Іншою серйозною проблемою у цій галузі є *відсутність чітко визначеного понятійного апарату,* що ґрунтується на загальноприйнятих міжнародних [10], регіональних чи галузевих стандартах (наприклад, поняття "кіберзагроза" зустрічається у кожному із зазначених документів [7-9], але його визначення чи посилання на інші нормативні документи відсутні).

Згідно з європейською політикою [9] заходи щодо забезпечення кібербезпеки мають бути включеними в Національні програми безпеки цивільної авіації, контролю якості, навчання й підготовки з питань безпеки цивільної авіації, а перелік необхідних заходів обме-

жується оцінкою загроз, розділенням мереж, підготовкою персоналу та управлінням інцидентами. Варто відзначити, що найповніший перелік заходів, яких необхідно вжити для мінімізації впливу кіберзагроз на ресурси КАІС, міститься у 8-й редакції керівництва [7]. Найбільш вагомими з-поміж них є:

– *адміністративні* (стандарти, процедури та політика безпеки, аналіз загроз та оцінка ризиків, відбір та підготовка персоналу тощо);

– *віртуальні (логічні) засоби контролю* (lDS-системи, антивірусний захист, шифрування та захист мережевих сервісів);

– *фізичні засоби контролю* (аутентифікація, контроль та управління доступом, резервне копіювання тощо).

Для вирішення зазначених проблем насамперед необхідно на базі відповідних наукових досліджень розробити *єдиний понятійний апарат,* створити *вичерпний перелік КАІС* і сформулювати *практичні рекомендації щодо впровадження кожного із вказаних заходів.* Що ж стосується більш глобального (державного) рівня, то потрібно на суб'єктах цивільної авіації створити ефективні *спеціалізовані підрозділи кібербезпеки* і приділити увагу *багаторівневій системі підготовки фахівців* у галузі забезпечення захисту цивільної авіації від кіберзагроз.

## ЛІТЕРАТУРА

1. Бурячок В.Л. Кібернетична безпека – головний фактор сталого розвитку сучасного інформаційного суспільства // Сучасна спеціальна техніка. – 2011. – № 3 (26). – С. 104-114.

2. Бурячок В.Л. Кібернетична безпека: характерні ознаки, існуючі поняття і визначення. стан питання в ГУР МО України, на державному рівні та у світі / В.Л.Бурячок, Л.В.Бурячок, В.В.Угрімов // Вісник воєнної розвідки. – 2013.

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

4. Бурячок В.Л. Стратегія оцінювання рівня захищеності держави від ризику стороннього кібернетичного впливу / В.Л.Бурячок, О.Г.Корченко, В.О.Хорошко, В.А.Кудінов // Захист інформації. – 2013. – Т. 15. – № 1. – С. 5-12.

5. Марущак А.І. Щодо поняття "інформаційні ресурси держави" криптографії / А.І.Марущак // Інформаційна безпека людини, суспільства, держави. – 2009. – № 1(1). – С. 11-15.

6. Словник термінів з кібербезпеки / за заг. редакцією Копана О.В., Скулиша Є.Д. – К. : ВБ "Аванпост-Прим". – 2012. – С. 31.

7. Doc 8973 ICAO “Керівництво з авіаційної безпеки” (Restricted). – Вид. 8. – 2011. – 748 с.

8. Додаток 17 до Конвенції про міжнародну цивільну авіацію “Безпека. Захист міжнародної цивільної авіації від актів незаконного втручання”. – Вид. 9. – 2011. – 60 с.

9. Doc 30 “Політика ЄКЦА у сфері авіаційної безпеки” (Restricted). – Вид. 13. – 2010. – 138 с.

10. ISO/IEC 27032, Information technology – Security techniques – Guidelines for cybersecuritv. – 2012. – 50 с.

*Вєдєнєєв Д.В.,*
*доктор історичних наук, професор,*
*Національна академія Служби безпеки України*

## ВИКЛИКИ БЕЗПЕЦІ ГУМАНІТАРНОЇ СФЕРИ УКРАЇНИ І НАЦІОНАЛЬНА ПАМ’ЯТЬ

Одним із магістральних напрямів розвитку сучасного світу стало формування так званого “VI технологічного укладу”, основні контури якого вивчаються, моделюються[1] або вже впроваджуються у провідних країнах світу. Карта “VI технологічного укладу” включає (поряд з біотехнологіями, нанотехнологіями, роботехнікою та штучним інтелектом) і такі напрями, як “високі гуманітарні технології” та “технології збирання і знищення соціальних суб’єктів” [1, с.324-326]. Відбувається прискорений розвиток новітніх технологій впливу на свідомість, які від простого управління людьми та спільнотами переходять на рівень творення віртуальної реальності (що сприймається як реальність існуюча), конструювання спільнот із заданими характеристиками або знищення (деструктивний вплив) легітимного державного ладу, традиційної культури, ментальності народів тощо.

Сучасні інформаційно-психологічні технології впливу на свідомість базуються на нечуваних можливостях електронних та дру-

[1] Зокрема, йдеться про розробки Інституту складності у Санта-Фе (США), розвиток теорії інноваційного розвитку Б.Артура, теорії техноценоза Л.Бадалян та В.Криворотова, структурно-демографічну модель П.Турчина тощо. Лише у США працюють понад 30 футурологічних організацій, пов’язаних з управлінськими колами та розвідувальним співтовариством.

кованих засобів масової інформації, досягненнях аналітичної психології, психології "колективного несвідомого", лінгвістики, психолінгвістики, семіотики, семантики, положень біхевіоризму, постмодернізму та інших специфічних інтелектуальних продуктів [див. 2]. Провідні держави Заходу набули і величезного досвіду застосування (як для управління власними народами, так і для дестабілізації своїх геополітичних противників у "холодній війні" 1946–1991 рр.) технологій "заміни дійсності псевдодійсністю" (за визначенням А.Безансона) [3, с. 46-47; див. також 4-7].

Важливість зміцнення й захисту національної пам'яті як громадянсько-політичного чинника з погляду забезпечення інформаційної безпеки існування України у глобалізованому світі відображена у чинному законодавстві. Загрози національній пам'яті як важливому елементу етнокультурної та політичної ідентичності громадян України цілком підпадають під визначені ст. 7 Закону України "Про основи національної безпеки України" загроз національним інтересам і національній безпеці України, а саме – "намагання маніпулювати суспільною свідомістю, зокрема шляхом недостовірної, неповної або упередженої інформації".

Затверджена Указом Президента України від 8 червня 2012 р. № 389 Стратегія національної безпеки України "Україна у світі, що змінюється" серед ключових завдань політики національної безпеки у внутрішній сфері визначила створення сприятливих умов для зміцнення єдності українського суспільства на основі європейських демократичних цінностей; збереження і розвиток духовних і культурних цінностей українського суспільства, зміцнення його ідентичності на засадах етнокультурної різноманітності; реалізацію комплексу заходів державної політики, спрямованих на консолідацію українського суспільства.

З погляду *внутрішніх негативних чинників впливу на національну пам'ять* ерозію національної пам'яті спричиняли передуім:

– перетворення історичного матеріалу на знаряддя політичної боротьби, елемент провокування іредентистських та сепаратистських настроїв, політичного екстремізму;

– прояви, із використанням "історичних аргументів", національної ворожнечі, шовінізму, національної або релігійної нетерпимості з боку окремих осіб, політичних сил, громадських організацій, ЗМІ;

– штучна консервація в історичній свідомості елементів тоталітаризму, крайнього етнонаціоналізму та інших несумісних із обраною Україною моделлю розвитку демократичної та правової держави;

– наявність у суспільній свідомості полярних, політично заангажованих та емоційно перевантажених оцінок важливих подій вітчизняної історії, що ускладнює діалог між певними суспільними, національними групами;

– поширення вітчизняними ЗМІ серед широкого загалу з комерційних або вузькокорпоративних інтересів перекрученого, фальсифікованого інформаційного продукту на історичну тематику.

На сферу національної пам'яті України скеровуються *зовнішні цілеспрямовані інформаційно-психологічні впливи* з метою послаблення реального суверенітету держави й морально-психологічної стійкості народу. Для посилення довгострокового політичного впливу в Україні, систематичної роботи із свідомістю етнічних громад своїх титульних народів в Україні, впливу на гуманітарну сферу їх буття, національну (історичну) свідомість використовуються:

– спеціалізовані державні органи сусідніх держав (як-от Департамент у справах румунів звідусіль, підпорядкований безпосередньо прем'єр-міністру Румунії, Міністерство виховання та досліджень Румунії; Відомство у справах закордонних угорців при уряді Угорщини; Турецьке агентство зі співробітництва та розвитку при МЗС Туреччини тощо);

– можливості дипломатичних та консульських представництв (на кшталт "центрів Полонії" при представництвах Республіки Польща), їх спеціалізованих підрозділів, спеціальних служб, прихована діяльність з надання подвійного громадянства, включаючи тактику прямого або завуальованого подвійного громадянства (оціночне – 30-50% румунів України мають паспорти Румунії; "картою поляка" можуть скористатися до мільйона громадян України; енергійно йде цей процес серед угорців Закарпаття тощо);

– можливості державних та недержавних інформаційних органів (так, інформаційний вплив на компактні етнічні громади Закарпаття ведуть понад 80 телерадіостанції Угорщини, Словаччини та Польщі);

– різноманітні програми, культурно-просвітні, релігійні та інші організації, фонди, які отримують часткове державне утримання (зокрема, фонди: польські – Фонд Баторія, Фонд допомоги польським школам на Сході ім. Т.Гоневича; російські – "Москва-Крим", "Москва – Севастополь"; "Соціальна ініціатива"; румунські "Культура без кордонів", Центр "Єудоксіу Хурмузакі"; турецькі – Фонд досліджень тюркського світу, "Нурчилар", фонд "Азиз Махмуд Худаі Вакули", Турецький релігійний фонд, Фонд відродження крим-

ськотатарської культури ім. С.Ізідінова; угорські – ім. Д.Йіеша, ім. Я.Апацаі Чере, "Pro Hungaris" та ін.);

– активісти національно-культурних і етнічних громадсько-політичних об'єднань громадян України (зокрема, Асоціація болгарських національно-культурних товариств та організацій в Україні, "Товариство Кирила і Мефодія"; Союз поляків України, Федерація польських товариств в Україні; "Союз буковинських румунів", Християнсько-демократичний альянс румунів в Україні, Союз румунських товариств "За європейську інтеграцію"; Карпатський культурний союз – Угорська політична партія, Угорський демократичний союз, Демократичний союз угорців України, Товариство угорської культури Закарпаття; словацька культурно-освітня організація "Матіца словенська"; Національний рух кримських татар, Кримськотатарська національна партія "Адалет", Ісламська партія Криму, Всекримська громадська організація "Ліга кримських репатріантів "Іраде"; Асоціація гагаузів Одеської області); русинські сепаратисти, які у жовтні 2008 р. на своєму Конгресі ухвалили "Акт проголошення русинської державності та утворення виконавчої влади в статусі автономної Республіки Підкарпатська Русь" (СБУ порушено за цими фактами кримінальну справу за ст. 110 КК України "Посягання на територіальну цілісність і недоторканність України");

– функціонери релігійних громад, місіонери, студенти, які навчаються у вищих навчальних закладах зарубіжних держав (так, лише у 1995–2004 рр. до Румунії виїхало на навчання тільки з Одеської області близько 600 випускників національних молдавських шкіл). При цьому добір громадян України до співпраці з НПО ведеться на конкурсній основі, із застосуванням тестування, прихованого психологічного вивчення, нейролінгвістичного програмування, після чого їх навчають за кордоном форм і методів збирання інформації, ідейно-психологічної обробки співгромадян і т.п.;

– неурядові організації зарубіжних держав (НУО), які отримують державну підтримку та поширюють свій вплив і представництво на теренах України. При цьому добір громадян України до співпраці з НУО ведеться на конкурсній основі, із застосуванням тестування, прихованого психологічного вивчення, нейролінгвістичного програмування, після чого їх навчають за кордоном формам і методам ідейно-психологічного впливу на співгромадян [див. 8-15].

Враховуючи проаналізовані вище виклики та небезпеки національній пам'яті як важливій складовій гуманітарної сфери буття України, закономірним буде постановка питання про роль науко-

вців-істориків та в цілому гуманітаріїв в обстоюванні інформаційно-гуманітарної безпеки України [див. також 16].

Ідеться передовсім про роз'яснення змісту провідних інформаційно-психологічних, етнополітичних методів та прийомів, котрі застосовуються для руйнації національної пам'яті, а саме:

– штучна ерозія позитивної, суспільно значущої для життєдіяльності народу та держави пам'яті про минуле;

– вилучення або "перекодування" змістів та світоглядних основ, котрі спираються на колективну пам'ять про минуле;

– упровадження в масову свідомість чужорідних, політично загострених тлумачень історії, які ведуть до дезінтеграції державницької організації та суспільного буття народу;

– пряма фальсифікація (фабрикація) історико-документального матеріалу або приховування "небажаної" історико-документальної бази, інформації, застосування спекулятивних (маніпулятивних) прийомів інтерпретації фактичного матеріалу;

– наполеглива дискредитація ("демонізація") історичної спадщини та традицій, ключових фігур історичного поступу нації;

– намагання довести до антагонізму світобачення в цілому та погляди на історію між різними поколіннями українського народу, що загрожує штучним перериванням цивілізаційної традиції та ерозією нації зсередини;

– створення відповідних структур, підготовка, виховання та заохочення "інтелектуального ударного загону" "війни з вітчизняною історією" з одночасними теоретико-методологічним роззброєнням та морально-психологічним спантеличенням гуманітарного професійного прошарку;

– прагнення до деінтелектуалізації, дераціоналізації масової свідомості як головної передумови "перекодування" національної пам'яті – важливої складової державно-політичної лояльності та національно-культурної (цивілізаційної) ідентичності українського народу;

– творення міфологізованих "місць пам'яті" (пам'ятників, меморіалів тощо як засобу некритичного укорінення запозичених трактувань минулого України (його спірних, болючих проблем) тощо.

## ЛІТЕРАТУРА

1. Малинецкий Г. Доклад о перспективах РФ / Г.Малинецкий // Калашников М. Новая опричнина, или Модернизация по-русски / М. Калашников и др. – М. : Фолио, 2011. – 448 с.

2. Жарков Я.М. Психолінгвістика, етнопсихологія, соціопсихологія як теоретичні основи інформаційно-психологічного впливу / Я.М.Жарков, С.М.Поліщук // Матеріали науково-практичного семінару “Інформаційна боротьба: проблеми та шляхи їх вирішення”. – К. : НАОУ, 2004. – С. 46–72.

3. Безансон А. Лихо століття: про комунізм, нацизм та унікальність голок осту / А.Безансон. – К. : Пульсари, 2007. – 136 с.

4. Панарин И.Н. Информационная война и геополітика / И.Н.Панарин. – М. : Поколение, 2006. – 560 с.

5. Петрик В.М., Остроухов В.В., Штоквиш А.А. и др. Информационно-психологическая безопасность в эпоху глобализации / В.М.Петрик, В.В.Остроухов, А.А.Штоквиш и др. – К., 2008. – 544 с.

6. Жарков Я.М. Інформаційно-психологічні операції як основна форма інформаційної боротьби / Я.М.Жарков // Труди академії [Національної академії оборони України]. – 2003. – № 41. – С. 135–145.

7. Павловська С.В. Сутність інформаційно-комунікативних заходів та особливості використання комунікативних технологій у воєнних конфліктах та локальних війнах другої половини ХХ – початку ХХІ століть / С.В.Павловська // Труди академії [Національної академії оборони України]. – 2008. – № 81. – С. 282–291.

8. Григорьев В. Военно-политические игры / В.Григорьев // “2000”. – 2009. – 15 мая.

9. Лозунько С. Двойные стандарты в ущерб национальной безопасности / С.Лозунько // “2000”. – 2009. – 15 мая.

10. Иванников И. Скрытая угроза-3: неправительственные организации / И.Иванников // Секретные материалы. – 2009. – № 7.

11. Унгуряну И. Военные спецслужбы Румынии / И.Унгуряну // Волонтер. – 2012. – № 2.

12. Іванников І. “Довгі вуха” стратегічного партнера / І.Іванников // Волонтер. – 2012. – № 4.

13. Іванников І. Польські спеціальні служби / І.Іванников // Волонтер. – 2012. – № 6.

14. Донато Д. В преддверии “Романиа маре” / Д.Донато // Oligarh.net. – 2009. – 8 сент.

15. Буркуш М. Кого манить “корона святого Іштвана”? / М.Буркуш // Волонтер. – 2012. – № 3. – С. 4–11.

16. Вєдєнєєв Д.В. Військова історія як інструмент обстоювання територіальної цілісності Української держави / Д.В.Вєдєнєєв // Воєнна історія Поділля та Буковини // Науковий збірник. – Кам’янець-Подільський, 2009. – С.413–419.

*Довгань О.Д.,*
*кандидат юридичних наук,*
*старший науковий співробітник,*
*Національна академія Служби безпеки України*

## КРИТИЧНА ІНФРАСТРУКТУРА ЯК ОБ'ЄКТ ЗАХИСТУ ВІД КІБЕРНЕТИЧНИХ АТАК

Стрімке впровадження інформаційних технологій у всі сфери життя, глобалізація інформаційних відносин зумовлюють світову тенденцію до перенесення протиправної діяльності у віртуальний простір. Сьогодні комп'ютерна злочинність, чи кіберзлочинність, для якої не існує державних кордонів, загрожує не лише правам та майну громадян, а й посягає на національні інтереси.

Зазіхання на об'єкти політичної, економічної, соціально-політичної сфер різних країн за допомогою інформаційних технологій зумовило актуалізацію проблеми протидії кібернетичній злочинності на державному рівні. Зокрема, США та країни Європейського Союзу ввели до законодавства таку дефініцію, як "критична інфраструктура".

Відповідно до указу президента США № 63 (PDD63, 1998 рік) такою інфраструктурою визначено *фізичні й інформаційні системи, необхідні для забезпечення мінімально припустимого рівня функціонування економіки й уряду*. До критичної інфраструктури віднесено: телекомунікації, енергетику, банківську й фінансову системи, транспорт, водні системи й аварійні служби.

Аналогічною є позиція ЄС – критична інфраструктура визначається як сукупність фізичних засобів та ІТ, мереж, послуг, активів, руйнування яких може призвести до негативних наслідків щодо стану здоров'я, безпеки, економічного рівня та ефективного функціонування державних інституцій.

Аналіз вітчизняної нормативної бази свідчить, що ця система в нашій державі перебуває на початковому етапі формування. Так, чинним законодавством України визначено окремі об'єкти соціально-економічної сфери України, надзвичайні події на яких можуть призвести до суспільно небезпечних наслідків, незалежно від джерела та способу реалізації такої загрози. Загальний перелік таких об'єктів передбачено підзаконними нормативними актами:

1) перелік особливо *важливих об'єктів нафтогазової галузі* (розпорядження Кабінету Міністрів України від 27.05.2009 р. № 578-р);

2) *перелік об'єктів підвищеної небезпеки підприємств, які мають стратегічне значення для економіки та безпеки держави*, що підлягають обов'язковій охороні підрозділами МВС (постанова Кабінету Міністрів України від 10.08.1993 № 615);

3) *перелік об'єктів, що становлять підвищену екологічну небезпеку* (постанова Кабінету Міністрів України від 27.07.1995 № 554).

Порядком ідентифікації та обліку об'єктів підвищеної небезпеки, затвердженим постановою Кабінету Міністрів України від 11.07.2002 № 956, визначено критерії ідентифікації таких об'єктів. Їх реєстрація здійснюється відповідно в Державному реєстрі потенційно небезпечних об'єктів (постанова Кабінету Міністрів України від 29 серпня 2002 р. № 1288) .

Крім того, суспільну небезпечність порушення штатного режиму функціонування вищенаведених об'єктів визначено Кримінальним кодексом України, а саме: статті 113 ("Диверсія"), 194-1 ("Умисне пошкодження об'єктів електроенергетики"), 261 ("Напад на об'єкти, на яких є предмети, що становлять підвищену небезпеку для оточення"), 270-1 ("Умисне знищення або пошкодження об'єктів житлово-комунального господарства"), 277 ("Пошкодження шляхів сполучення і транспортних засобів"), 279 ("Блокування транспортних комунікацій"), 292 ("Пошкодження об'єктів магістральних нафто-, газо- та нафтопродуктопроводів"), 326 ("Порушення правил поводження з мікробіологічними або іншими біологічними агентами чи токсинами"). Отже, кримінальне законодавство характеризує кіберзагрози для об'єктів соціально-економічної сфери таким чином: застосування інформаційних технологій як спосіб та засіб для вчинення вищенаведених кримінально караних діянь.

Проте наведені складові системи захисту критичної інфраструктури від кібератак оформлені фрагментарно й не мають єдиної системоутворювальної основи. Так, сьогодні у вітчизняному законодавстві відсутнє визначення поняття "критична інфраструктура", а також регламентація її складу.

На нашу думку, слід розглядати поняття "критична інфраструктура" на різних рівнях. У *широкому розумінні* – це сукупність об'єктів економіки, державного управління, соціальної сфери, руйнування та/або виведення з ладу яких призводить до суспільно небезпечних наслідків для держави, суспільства та особи незалежно від засобу та способу негативного впливу (вибух, підпал, кібернетична атака тощо). У *вузькому розумінні* (через призму забезпечення кібернетичної безпеки) критична інфраструктура – це сукупність інформаційних, телекомунікаційних та інформаційно-телекомунікаційних мереж, несанкціоноване втручання в роботу яких призводить до сус-

пільно небезпечних наслідків у сферах управління державою, економікою, здоров'я та добробуту населення.

Вважаємо, що формування переліку об'єктів критичної інфраструктури має здійснюватися за однозначно визначеними, загальними для усіх установ та підприємств критеріями, де критерії – це сукупність правил, що ґрунтується на таких основних показниках:

1) категорія інформації, яка обробляється в інформаційно-телекомунікаційних системах (мережі) об'єкта (відкрита, з обмеженим доступом);

2) призначення інформаційно-телекомунікаційної системи (мережі);

3) можливість настання суспільно небезпечних наслідків у разі несанкціонованих дій у цій мережі.

Зауважимо, що останній показник є визначальним у підходах зарубіжних фахівців.

Відповідно до визначеної системи показників до об'єктів критичної інфраструктури мають належати насамперед інформаційно-телекомунікаційні мережі органів державної влади, підприємств, установ, організацій, несанкціоноване втручання в роботу яких призводить до настання суспільно небезпечних наслідків у вигляді:

– розголошення, втрати державної таємниці та іншої інформації з обмеженим доступом;

– виникнення надзвичайних ситуацій техногенного характеру, які створюють загрозу життю і здоров'ю значних верств населення;

– блокування роботи або руйнування особливо важливих об'єктів життєзабезпечення, великих та середніх підприємств промисловості, енергетики, транспорту, зв'язку;

– виникнення масових протестних заходів, а також заворушень, що супроводжуються насильством, обмежують права і свободи громадян; завдання значної матеріальної шкоди економіці держави.

Відтак, системоутворювальним нормативно-правовим документом у сфері захисту національної критичної інфраструктури від кібератак має стати Закон України "Про кібернетичну безпеку", в якому доцільно визначити:

– понятійний апарат у сфері кібернетичної безпеки (дефініції "кібербезпека", "кібератаки", "кібертероризм", "кіберзлочинність", "кіберзагроза", "критична інфраструктура" тощо);

– критерії віднесення об'єктів до таких, що мають важливе значення для забезпечення національної безпеки й оборони України та потребують першочергового захисту від кібернетичних атак (критична інфраструктура), порядок формування такого переліку,

повноваження владних структур щодо його затвердження та подальшого запровадження;

– повноваження державних структур з питань протидії кіберзагрозам; механізми управління та прийняття рішень тощо;

– засади співробітництва державного та приватного секторів у сфері захисту критичної інфраструктури.

*Марущак А.І.,*
*доктор юридичних наук, професор,*
*Навчально-науковий інститут інформаційної безпеки*
*Національної академії Служби безпеки України*

## РОЗВИТОК ПРАВОВОГО РЕГУЛЮВАННЯ ПРОЦЕДУР ОТРИМАННЯ ІНФОРМАЦІЇ ПРАВООХОРОННИМИ ОРГАНАМИ УКРАЇНИ

Останніми роками спостерігається тенденція розвитку галузі інформаційного права, пов'язана із розмежуванням прав і обов'язків учасників інформаційних відносин. Формально вона закріплена у новій редакції Закону України "Про інформацію", у нових законодавчих актах: законах України "Про доступ до публічної інформації", "Про захист персональних даних", Кримінальному процесуальному кодексі України, у змінах до законів України "Про оперативно-розшукову діяльність", "Про контррозвідувальну діяльність" та ін.

Закріплені зазначеними нормативно-правовими актами процедури інформаційного обміну між уповноваженими на здійснення правоохоронної функції державними органами і приватними суб'єктами безпосередньо стосуються інформаційної безпеки особи, суспільства, держави. Мовою зарубіжних стандартів інформаційної безпеки такі процедури впливають на "сервіс інформаційної безпеки" суб'єкта – "вплив на конфіденційність". Адже більшість випадків стосуються доступу до конфіденційної і таємної інформації. Тим самим виникає конфлікт інтересів переважно двох суб'єктів: держави – в контексті здійснення правоохоронної функції і приватного суб'єкта, який намагається забезпечити нерозголошення власної інформації з обмеженим доступом.

Відзначимо, що правове регулювання видів правоохоронної діяльності – оперативно-розшукової, контррозвідувальної, кримінальної процесуальної – останніми роками значною мірою ґрунтується на врахуванні вироблених наукою інформаційного права України

класифікації інформації з обмеженим доступом. Така тенденція свідчить про подальше впровадження конституційного принципу: правоохоронним органам дозволено тільки те, що передбачено законом, у практику інформаційного обміну з приватними суб'єктами.

Суттєвою новелою є впровадження у кримінальний процес такої процедури, як отримання правоохоронними (а також іншою стороною кримінального провадження) тимчасового доступу до речей і документів. Статті 160-166 Кримінального процесуального кодексу України передбачають, що сторони кримінального провадження мають право звернутися до слідчого судді під час досудового розслідування чи суду під час судового провадження із клопотанням про тимчасовий доступ до речей і документів. Тимчасовий доступ до речей і документів полягає у наданні стороні кримінального провадження особою, у володінні якої знаходяться такі речі і документи, можливості ознайомитися з ними, зробити їх копії та, у разі прийняття відповідного рішення слідчим суддею, судом, вилучити їх (здійснити їх виїмку). Як бачимо, законодавець розрізняє три інформаційно-правові можливості, що включені до права доступу до документів: ознайомитися з ними, зробити їх копії, вилучити їх (здійснити їх виїмку) у разі прийняття відповідного рішення слідчим суддею, судом [1].

Варто зауважити, що при формулюванні переліку речей і документів, які містять охоронювану законом таємницю, не зовсім коректно враховано класифікацію інформації з обмеженим доступом, вироблену наукою інформаційного права і закріплену у відповідних законах. Зокрема, передбачена конфіденційна інформація, в тому числі така, що містить комерційну таємницю. Хоча останню інформаційне законодавство визначає видом таємної, а не конфіденційної інформації. Крім того, потребує подальшого наукового дослідження режим інформації, яка знаходиться в операторів та провайдерів телекомунікацій, про зв'язок, абонента тощо і його співвідношення з персональними даними особи.

Слідчий суддя, суд постановляє ухвалу про надання тимчасового доступу до речей і документів, якщо сторона кримінального провадження у своєму клопотанні доведе наявність достатніх підстав вважати, що ці речі або документи:

1) перебувають або можуть перебувати у володінні відповідної фізичної або юридичної особи;

2) самі по собі або в сукупності з іншими речами і документами кримінального провадження, у зв'язку з яким подається клопотання, мають суттєве значення для встановлення важливих обставин у кримінальному провадженні;

3) не становлять собою або не включають речей і документів, які містять охоронювану законом таємницю.

Слідчий суддя, суд постановляє ухвалу про надання тимчасового доступу до речей і документів, які містять охоронювану законом таємницю, якщо сторона кримінального провадження також доведе:

4) можливість використання як доказів відомостей, що містяться в цих речах і документах, та

5) неможливість іншими способами довести обставини, які передбачається довести за допомогою цих речей і документів [1].

На практиці виникають приклади неправильного застосування такої процедури отримання інформації правоохоронними органами, як тимчасовий доступ до речей і документів, котрі містять охоронювану законом таємницю.

Так, Апеляційний суд Закарпатської області 10.01.2013 р. виніс ухвалу, якою скасував ухвалу слідчого судді Тячівського районного суду від 11.12.2012 р. про надання тимчасового доступу до магнітного носія інформації, де містяться відомості про рух коштів по відділенню № 0647 АТ "Райффайзен Банк Аваль" за 27.08.2010 рік, можливість ознайомитися з даною інформацією та зробити роздруківку руху коштів за 27.08.2010 рік, що знаходиться у Закарпатській обласній дирекції АТ "Райффайзен Банк Аваль".

Суть справи така. Ухвалою слідчого судді Тячівського районного суду від 11.12.2012 р. задоволено клопотання заступника начальника СВ Тячівського РВ УМВС України в Закарпатській області ОСОБА_7 про тимчасовий доступ до магнітного носія інформації, де містяться відомості про рух коштів по відділенню № 0647 АТ "Райффайзен Банк Аваль" за 27.08.2010 р., можливість ознайомитися з даною інформацією та зробити роздруківку руху коштів за 27.08.2010 р., що знаходяться у Закарпатській обласній дирекції АТ "Райффайзен Банк Аваль.

Виконавчий директор Закарпатської ОД АТ "Райффайзен Банк Аваль" ОСОБА 6 в апеляції просив вказану ухвалу слідчого судді скасувати, оскільки в цій частині не міститься вимога щодо ознайомлення (одержання копії) конкретного документа, а зазначено відомості про рух коштів по відділенню за 27.08.10 р., що може призвести до порушення прав інших осіб.

Заслухавши суддю-доповідача, доводи представника апелянта, міркування прокурора, апеляційний суд вважав, що апеляційна скарга підлягала до задоволення, з наступних підстав. Згідно з вимогами ст. 62 Закону України "Про банк і банківську діяльність" інформація щодо фізичних і юридичних осіб, що містить банківську таємницю, розкривається банками не інакше, як за рішенням суду.

Відповідно до ч. 5 ст. 163 КПК України слідчий суддя, суд постановляє ухвалу про надання тимчасового доступу до речей і документів, якщо сторона кримінального провадження у своєму клопотанні доведе наявність достатніх підстав вважати, що ці речі або документи: 1) перебувають або можуть перебувати у володінні відповідної фізичної чи юридичної особи; 2) самі по собі або в сукупності з іншими речами і документами кримінального провадження, у зв'язку з яким подається клопотання, мають суттєве значення для встановлення важливих обставин у кримінальному провадженні; 3) не становлять собою або не включають речей і документів, які містять охоронювану законом таємницю.

Як убачається з ухвали, слідчий суддя, приймаючи рішення про надання дозволу на тимчасовий доступ до документів та можливість зробити роздруківку руху коштів, не врахував, що в клопотанні міститься вимога про одержання доступу не до *конкретного документа, який має значення для встановлення обставин у кримінальному провадженні*, а доступу до інформації, яка не має такого значення.

Апеляційний суд ухвалу слідчого судді Тячівського районного суду від 11.12.2012 р. про надання заступнику начальника СВ Тячівського РВ УМВС України в Закарпатській області ОСОБА_7 тимчасового доступу до магнітного носія інформації, на якому містяться відомості про рух коштів по відділенню № 0647 АТ "Райффайзен Банк Аваль" за 27.08.2010 р., можливість ознайомитися з даною інформацією та зробити роздруківку руху коштів за 27.08.2010 р., що знаходяться у Закарпатській обласній дирекції АТ "Райффайзен Банк Аваль", яка є юридичною особою та розташована в м. Ужгороді по вул. Театральній, 19, Закарпатської області, скасував [2].

Як бачимо, суддя розмежував поняття доступу до конкретного документа, який має значення для встановлення обставин у кримінальному провадженні, й доступу до інформації, яка не має такого значення.

Протилежне за юридичними наслідками рішення 01.02.2013 р. прийняв слідчий суддя Карлівського районного суду Полтавської області у справі № 531/166/13-к за провадженням 1-кс/531/14/13, розглянувши клопотання про доступ до речей і документів.

Старший слідчий СВ Карлівського РВ УМВС України в Полтавській області звернувся до суду з клопотанням про доступ до речей і документів, які містять охоронювану законом таємницю, а саме – надання копій документів щодо відомостей з ВАТ АБ "Укргазбанк", мотивувавши клопотання тим, що в провадженні Карлівського РВ

УМВС України в Полтавській області перебувають матеріали досудового розслідування, внесеного до Єдиного реєстру досудових розслідувань за № 12012180000001 від 20.11.2012 р., за ознаками кримінального правопорушення, передбаченого ч.1 ст. 388 КК України за фактом невиконання зобов'язань ОСОБА_2 умов договору кредиту між ним та ВАТ АБ "Укргазбанк".

З метою встановлення осіб, причетних до вчинення цього кримінального правопорушення, потрібно було тимчасово отримати доступ до документів, які містять охоронювану законом таємницю, шляхом ознайомлення та надання копій документів щодо відомостей про укладання між ВАТ АБ "Укргазбанк" та фізичною особою ОСОБА_2 ІНФОРМАЦІЯ_1 кредитних договорів і договорів застави.

На підставі викладеного, керуючись ст. 162-166 КПК України слідчий суддя ухвалив клопотання ст. слідчого СВ Карлівського РВ УМВС України в Полтавській області задовольнити. Надати ст. слідчому СВ Карлівського РВ УМВС України в Полтавській області доступ до документів, які містять охоронювану законом таємницю, шляхом ознайомлення та надання копій документів щодо зазначених у клопотанні відомостей.

Як висновок відзначимо неоднозначне розуміння таємниць у кримінальному процесі, що зумовлює вплив на сервіс "конфіденційність" інформаційної безпеки суб'єктів, які надають відповідну інформацію правоохоронним органам.

Подальшого наукового обґрунтування потребує розмежування процедур отримання інформації правоохоронними органами у формі ознайомлення, зняття копій і виїмки.

## ЛІТЕРАТУРА

1. Кримінальний процесуальний кодекс України від 13 квітня 2012 р. // Голос України. – 2012. – № 90–91.

2. Ухвала Апеляційного суду Закарпатської області від 10.01.2013 р. [Електронний ресурс] – Режим доступу до Єдиного держ. реєстру судових рішень : www.reyestr.court.gov.ua.

3. Ухвала слідчого судді Карлівського районного суду Полтавської області від 01.02.2013 р. [Електронний ресурс] – Режим доступу до Єдиного держ. реєстру судових рішень : www.reyestr.court.gov.ua.

*Остроухов В.В.,*
*доктор філософських наук, професор,*
*Національна академія Служби безпеки України*

## ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНІ АСПЕКТИ ТЕРОРИЗМУ

Виступ присвячено з'ясуванню тісного зв'язку терористичної діяльності з інформаційними процесами у суспільстві, залежності успішності дій терористів від діяльності ЗМІ, а також можливості використання терористами спеціальних інформаційних технологій – засобів і прийомів інформаційної війни.

Основною метою будь-якого теракту є, як відомо, зовсім не сам факт здійснення того чи іншого злочинного діяння (вбивства, руйнування, захоплення заручників) та його матеріальні збитки, а насамперед психологічний вплив на якомога ширшу аудиторію (залякування, привертання уваги громадськості, провокування до певних дій чи бездіяльності). Таким чином, тероризм – засіб психологічного впливу. Його головний об'єкт – не ті, хто став жертвою, а ті, хто залишився живим. Його мета – не вбивство, а залякування і деморалізація живих. Жертва – інструмент, вбивство – метод.

Цим тероризм відрізняється від диверсійних дій, мета яких – зруйнувати об'єкт (міст, електростанцію) чи ліквідувати противника.

Цілі, подібні до терористичних, споконвіку переслідували й фахівці інформаційної боротьби, намагаючись застосуванням певним чином організованої інформації (комунікативні технології) залякати та деморалізувати вороже військо, посіяти в ньому розбрат, завоювати довіру мирного населення, спровокувати вияви незадоволення владою у ворожому стані. Отже, вже у давнину можемо спостерігати спільні риси у цих двох способів боротьби і насамперед спільність мети – досягнення відповідного психологічного впливу.

Іншою спільною рисою тероризму та інформаційної війни є те, що вони базуються на так званій ідеї "малої війни". Суть її – досягнення максимального результату за мінімуму витрат. І терористичні акти, і спеціальні інформаційно-пропагандистські операції досить часто розглядаються як можливий шлях зрівняння можливостей протиборчих сторін, одна з яких значно перевищує іншу потенційно.

Ще одним моментом, який споріднює ці явища, є їх тісна пов'язаність з процесами комунікації. Поки комунікаційна система суспільства залишалася слабко розвинутою, засоби масової інформації відігравали значну роль, тероризм, як, до речі, й інформаційні війни, не мав широкого поширення. Ситуація змінюється в епоху

капіталізму, коли процеси обміну інформацією і діяльність ЗМІ набувають принципово іншого значення. І для війни, і для боротьби шляхом терору відкриваються в наш час широкі можливості, пов'язані з інформаційною революцією останніх десятиріч, яка зумовила кардинальні зміни в суспільстві: зароджуються нові культурні та економічні тенденції, з'являється інформаційне виробництво – продукування інформації як самостійного виду товару, формуються нові види соціальної комунікації. Така сфера життя, як національна безпека, в тому числі інформаційна безпека, не могла залишитися поза впливом інформаційного фактора.

З одного боку, інформація набула системоутворювального значення в усіх сферах життєдіяльності, з іншого – інформаційна інфраструктура набуває статусу критичної (життєво важливої для існування держави) й потребує для свого захисту збалансованої державної політики, зокрема в інформаційній сфері.

В умовах інформаційного суспільства всі без винятку об'єкти національної безпеки (людина, суспільство, держава) стають чутливими до інформації, яка їх оточує. Таким чином, цілеспрямовано змінюючи інформацію, зафіксовану на певних носіях, керуючи каналами комунікації, впливаючи на технічні засоби оброблення інформації, можна змінювати рішення, а відтак і дії об'єктів національної безпеки.

Динамізм сфери інформаційних міжнародних відносин, що спостерігається останнім часом, зумовлений низкою важливих факторів:

- насамперед крахом біполярної моделі світу та формуванням натомість багатополярної моделі;
- виходом на міжнародну арену не лише окремих держав та їхніх об'єднань, а й таких нетрадиційних гравців, як, наприклад, міжнародні терористичні рухи, які є все більш зростаючою загрозою безпосереднього впливу на внутрішню політику держав і міжнародні відносини в цілому. Сьогодні міжнародний тероризм перетворився на політичний суб'єкт, який безумовно враховується при формуванні міждержавних відносин та основ світової безпеки. Він характеризується великим впливом на громадську думку, а відтак і на суспільну свідомість, що перетворює терористів на впливових політичних акторів.

Тероризм, як і будь-який вид людської діяльності, еволюціонує. Відтак, якщо раніше терористи ставили на меті передусім зміну окремих дій уряду шляхом убивств політичних діячів, то тепер вони формулюють завдання впливу на суспільство в цілому з метою зміни політики уряду. Суспільство стає головним об'єктом діяльності терористів.

Сьогодні склалася ситуація, коли терористичні організації довели, що задля успішного ведення війни і досягнення перемоги, яка втілюється в отриманні впливу на владу противника, не обов'язково мати потужні збройні сили або найновішу зброю. Відтак збільшення витрат держав виключно на власний військово-оборонний комплекс у більшості випадків стає неефективним оскільки не може гарантувати безпеки власних громадян на власній території. Відомий приклад – трагічні події 11 вересня 2001 року у США. Таким чином, якщо війни четвертого покоління (Друга світова війна) або п'ятого покоління (війни в Афганістані чи Іраці) велися за таких умов, коли ворога, хоча би приблизно, можна було оцінити за показниками військової могутності й локалізувати, принаймні частково, то терористи вивели війну на наступний рівень розвитку – асиметричних насильницьких дій та величезного інформаційного резонансу.

Нині залежно від політичних цілей терористів театром їхніх дій стає весь світ, механізмом – насильство щодо цивільного населення, головним об'єктом – суспільство та громадська думка, а основним засобом досягнення вимог, погроз та підтримки інтересу – засоби масової інформації.

Тому вдосконалення інформаційних методів боротьби з тероризмом стає більш актуальним, ніж ескалація виключно військового протистояння з ним.

В Україні, попри те, що країна майже не підпадає під терористичні атаки і практично не стикається з тероризмом безпосередньо, дослідженню інформаційних методів протидії тероризму необхідно надавати системного характеру. Це пов'язано з тим, що Україна є членом міжнародного співтовариства, активно співпрацює, зокрема у військово-інформаційній сфері, як з ООН і НАТО, так і з країнами СНД.

Крім того, не слід випускати з уваги фактор потенційного міжетнічного напруження та можливої активізації діяльності терористичних угруповань. Ідеться, зокрема, про Автономну республіку Крим, де нині складається все більш небезпечна політико-етнічна ситуація, що гальванізується економічними (земельні питання), етнічними (актуалізація інтересів татарського населення) та зовнішньополітичними (перебування збройних сил Російської Федерації) чинниками.

Пропоную у 2014 році обрати таку тему конференції: "Інформаційна безпека: сталий людський розвиток. Ціннісний вимір".

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

# АКТУАЛЬНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ФОРМУВАННЯ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

У контексті формування глобального інформаційного простору та інформаційного суспільства в Україні тема конференції вбачається вкрай актуальною. З огляду на викладене пропонуємо звернути увагу на деякі філософсько-правові проблеми забезпечення інформаційної безпеки в сучасних умовах.

*Перше* – філософські аспекти розбудови інформаційного суспільства та формування нових суспільних відносин.

Нині людство підійшло до певної межі, яка відділяє одну епоху від іншої. Наука переконливо доводить, що майбутнє суспільство кардинально відрізнятиметься від сучасного.

У контексті зазначеного становлять інтерес погляди Е.Тоффлера, який виокремлює три хвилі суспільних змін на Землі. Перша хвиля пов’язана з формуванням і розвитком аграрного суспільства, друга – індустріального суспільства, а третя (сучасна) – інформаційного суспільства (Тоффлер Э. Третья волна : пер. с англ. /Э. Тоффлер. – М. : ООО “Издательство АСТ”, 2004. – С. 31–40).

Застосування логіки досліджень Е.Теффлера, а також аналіз вітчизняної історії дає змогу виокремити такі основні історичні періоди розвитку суспільства на українських теренах:

– аграрне суспільство (почало формуватися близько 7,5 тисяч років тому з часів розвиненої аграрної цивілізації – так званої “трипільської культури” та фактично існувало до другої половини XX століття);

– індустріальне суспільство (почало зароджуватися у XVIII столітті та сформувалося у другій половині XX століття);

– інформаційне суспільство (почало формуватися наприкінці XX століття).

Аналогічні хронометричні рамки характерні й для більшості інших країн світу. Кожному із вказаних періодів були притаманні свої особливості суспільних відносин у різних сферах життєдіяльності суспільства та їх відповідне регулювання (на рівні звичаїв,

традицій чи права). Водночас, кожна наступна форма суспільства намагалася враховувати й використовувати особливості й досягнення попередньої.

Нині в Україні та світі фактично відбувається досить складний та стрімкий перехід від індустріального до інформаційного суспільства.

Основною відмінністю цього переходу є стрімка зміна сформованих раніше суспільних відносин практично в усіх сферах життєдіяльності людини, суспільства і держави, що потребує кардинального перегляду ролі сучасної науки в цілому і правової науки зокрема.

*Друге* – проблема формування нового безпекового середовища в контексті поширення нових інформаційно-комунікаційних технологій.

Ще у 1990-х роках у рекомендаціях Ради Європи зверталася увага на необхідність прискореного формування інформаційного суспільства у країнах Євросоюзу, оскільки від цього суттєво залежатимуть перспективи їх подальшого розвитку.

Також зауважимо, що становлення інформаційного суспільства в Україні й інших державах світу, а також формування глобального інформаційного простору безпосередньо пов'язані зі створенням і розвитком сучасних інформаційно-комунікаційних технологій. Нині під їх безпосереднім впливом:

1) кардинально змінюється міжнародна спільнота, українське суспільство та суспільні інформаційні відносини;

2) формується нова структура економіки та змінюються економічні відносини;

3) трансформується ринок праці і характер трудових відносин, які часто набувають транснаціонального характеру;

4) формується нове безпекове середовище, яке потребує комплексного наукового опрацювання та перегляду безпекової інформаційної політики.

*Третє* – проблема виокремлення і захисту життєво важливих інтересів людини, суспільства і держави в умовах інформаційної глобалізації.

За нашими оцінками, враховуючи тенденції формування національного і глобального інформаційного простору, а також наявні та можливі виклики і загрози інформаційній безпеці, до найбільш важливих інтересів людини, суспільства і держави, що підлягають захисту у цій сфері, слід віднести:

1) безпеку людини і захист громадян від інформаційного насильства, інформаційної агресії та маніпуляційного впливу на свідомість, спричинення шкоди психічному та фізичному здоров'ю людини;

2) захист соціокультурних, історичних і національних традицій народу України від розмивання та можливої руйнації в умовах інформаційного глобалізму та агресивного нав'язування зовнішніх, часто руйнівних цінностей;

3) захист інформаційної інфраструктури та інформаційних ресурсів, насамперед баз даних, які містять персональні дані громадян (ця проблема нині є вкрай актуальною), а також відомостей, що становлять державну таємницю, чи інших відомостей з обмеженим доступом;

4) забезпечення безпеки та сприяння розвитку електронного врядування й системи електронних адміністративних послуг;

5) протидія розвідувально-підривній та іншій протиправній діяльності спецслужб іноземних держав, організацій, груп та осіб на шкоду інтересам України в інформаційній сфері;

6) боротьба з тероризмом та організованою злочинністю, насамперед транснаціональною, в інформаційній сфері.

З наведеного випливає головне завдання держави і права – сформувати ефективні законодавчі механізми й передумови для своєчасного виявлення, запобігання, припинення чи локалізації реальних та потенційних викликів і загроз інформаційній безпеці.

Крім цього, актуалізується проблема належного врегулювання юридичної відповідальності за вчинення злочинів та інших правопорушень в інформаційній сфері, передусім тих, що створюють загрозу життю і здоров'ю людини, посягають на законні інтереси суспільства і держави.

Зазначені та інші проблеми інформаційної безпеки потребують комплексного наукового опрацювання і можуть бути предметом подальших наукових досліджень.

*Сідак В.С.,*
*доктор історичних наук, професор,*
*заслужений діяч науки і техніки,*
*Університет "КРОК"*

## ДИВЕРСИФІКАЦІЯ СУСПІЛЬНОЇ СВІДОМОСТІ ЯК ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ДЕРЖАВИ ТА ЇЇ НЕЙТРАЛІЗАЦІЯ

Немає сумніву, що в умовах глобалізації проблема забезпечення національної безпеки постала гостро, як ніколи раніше. А її невід'ємною складовою є безпека інформаційна, що включає безпеку інформації та безпеку інформаційного поля.

Саме безпека останнього в умовах глобалізації виходить на перший план. Відповідно до Закону України “Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки” інформаційна безпека – це стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому попереджається завдання шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації.

Мусимо констатувати неналежний стан інформаційної безпеки в Україні через низку причин як внутрішнього, так і зовнішнього характеру. Серед серйозних загроз XXI ст. у цій сфері на чільне місце виходить диверсифікація суспільної свідомості. Українські науковці В.Петрик, В.Остроухов, О.Штоквиш, М.Галамба визначають її як розпорошення уваги правлячої еліти держави на вирішення різних штучно акцентованих проблем і відвертання тим самим уваги від вирішення нагальних першочергових для нормального функціонування суспільства і держави завдань суспільно-політичного та економічного розвитку. Актуальність цієї проблеми підтверджують події в різних регіонах світу.

До методів диверсифікації суспільної свідомості згадані вище дослідники відносять:

– дестабілізацію обстановки в державі чи окремих її регіонах;

– активізацію кампанії проти політичного курсу правлячої еліти держави та окремих її лідерів у різних міжнародних установах;

– ініціювання антидемпінгових кампаній та іншого роду скандальних судових процесів, застосування міжнародних санкцій з інших причин.

Погоджуючись із вказаними підходами не можу, водночас, не зауважити, що тут має місце певне звуження методів диверсифікації. Адже виходить, що вона є не більше, ніж складовою інформаційного протиборства. Тому вважаю, що до основних методів у такій ситуації слід додати відвертання уваги і зусиль вищого військово-політичного керівництва держави на другорядні, а то й на “нікчемні” об’єкти.

До об’єктів дивесифікаційної діяльності у сфері суспільної свідомості можемо віднести загальні та спеціальні.

До загальних об’єктів належать зовнішня і внутрішня політика країни, система захисту її національної безпеки. До спеціальних – конкретні заходи щодо забезпечення функціонування зазначеної

системи, сили і засоби, задіяні в реалізації політики держави, організація діяльності органів безпеки, правоохоронних інституцій тощо.

Використання диверсифікації суспільної свідомості становить загрозу не лише для конституційного ладу та інформаційної безпеки країни, й для її територіальної цілісності. Адже одним із важливих елементів маніпулювання суспільною свідомістю є висунення сепаратистських та іредентистських гасел, що є особливо актуальним для України.

Сучасні вчені подібні міжнародні конфлікти поділяють на власне іредентистські, сепаратистські й автономістські. Намагання держави, де виник іредентистський рух, придушити його силовим шляхом та підтримка його ззовні у свою чергу призводять до особливо гострих міждержавних криз. З усіх тлумачень іредентизму найбільш прийнятним, на мою думку, є його визначення як різновиду національних рухів, що виступають за відокремлення певної території з метою її подальшого приєднання до сусідньої держави.

Численні етнічні конфлікти стали характерною ознакою саме кінця XX ст. Їхня природа різноманітна. Інколи вони мають характер боротьби за національне самовизначення (наприклад, баски в Іспанії). Однак частіше етнічні конфлікти виникають тоді, коли нацменшина певної країни вже має по сусідству своє національно-адміністративне утворення. Більше того, як свідчить історичний досвід, компактне проживання певної національної меншини поряд із державним утворенням, де вона є титульною нацією, нерідко призводить до виникнення міжнародних конфліктів. На жаль, у міжнародному праві це питання врегульоване не досить чітко. Із цілком зрозумілих причин окремі громадяни можуть забажати жити у своїй державі, як це часто було в XX столітті.

Неодмінною ознакою іредентистських рухів є наявність політичних осередків націоналістичного спрямування. Говорячи про націоналізм, ми розглядаємо його як прихильність до власної нації, що декларується політичним шляхом. Не вкладаючи притаманного радянській історіографії негативного змісту в цей термін, мусимо зазначити, що націоналістичні прояви можуть супроводжуватись агресивними планами та діями однієї нації проти іншої, аж до етнічних чисток.

Визначальним фактором гостроти конфлікту сьогодення можемо вважати вплив третьої сторони. Напевне, в жоден інший історичний період імовірність мирного розв'язання подібних суперечностей не залежала настільки від відповідальності політичних діячів, ніж сьогодні. Навіть елементарна етноконфесійна поляризація може призвести до непередбачуваних наслідків. Роль каталізатора вибуху

можуть відіграти як псевдо націоналізм, так і численні "історичні образи", які кожен народ має до своїх сусідів. Певні суперечності, поєднані з трагічною історією, сприймаються як непереборні перешкоди. Взаємна ненависть зберігається і проявляється в політиці етнічних чисток, причому лідерство в політичному житті захоплюють деструктивні сили, котрі намагаються усунути будь-які форми співіснування етнічних груп на одній території та створити на ній однорідну етнічну масу.

"Убийте їх сьогодні, інакше вони уб'ють вас завтра" – цей лозунг уперше широко використано під час вірмено-азербайджанського конфлікту в Нагірному Карабасі, звучав він і в Косово. Останні приклади особливо наочно демонструють приреченість етноконфесійного конфлікту в теперішній час без активного втручання саме третьої сторони.

Отже, іредентизм вважається однією з основних диверсифікаційних загроз сучасності. Слід зауважити, що в таких ситуаціях існує і серйозна загроза міжнародній безпеці. Конфлікти швидко переростають у міжнародні, оскільки при розгортанні іредентистських рухів неминучим є втручання в конфлікт інших держав. Після чого він набуває характеру збройного конфлікту, який у свою чергу може бути як локальним, так і багатостороннім.

При цьому конфлікт надзвичайно швидко приходить до стадії ескалації, що, як правило, призводить да застосування сили. Як casus belli конфліктуючі сторони використовують:

а) політичні рішення конфронтаційного характеру;

б) випадковий інцидент з людськими жертвами або матеріальними втратами;

в) провокацію;

г) інсинуацію, тобто штучне створення інциденту.

Причому до провокативних методів нині частіше вдається слабша сторона, маючи на меті насамперед привернення на свій бік світової спільноти.

Гострота воєнно-політичних криз, викликаних іредентистськими рухами, зумовлюється тим, що вони становлять одну з найбільших загроз для територіальної цілісності й політичного режиму держави. Криза має запеклий і безкомпромісний характер. Приводом тут виступає цілий комплекс політичних, релігійних, соціально-економічних та інших причин.

Іредентистські рухи зазвичай виникають при одночасному загострення соціально-економічних суперечностей та етнічних розбіжностей. При цьому конфлікт може відразу набувати іредентистського забарвлення, а може пройти певну еволюцію: автономізм – сепа-

ратизм – іредентизм (наприклад, рух турків-кіпріотів, боротьба косовських албанців).

Протидія диверсифікації суспільної свідомості у процесі її реалізації вкрай важка. Однак цілком посильним є завдання її упередження шляхом нейтралізації зусиль.

Основними формами нейтралізації можна вважати: інформаційний патронат, інформаційну кооперацію та інформаційне протиборство.

*Інформаційний патронат* – це форма забезпечення інформаційної безпеки фізичних та юридичних осіб з боку держави та її органів. При цьому інформаційне забезпечення містить збирання (добування) відомостей про дестабілізуючі фактори та інформаційні загрози, їхнє оброблення, обмін інформацією між органами управління й суб'єктами та засобами системи захисту інформаційної безпеки. Інформаційний захист здійснюється шляхом ухвалення певних законопроектів, забезпечення судового захисту, проведення оперативно-розшукових та слідчих заходів силами й засобами правоохоронних органів тощо.

*Інформаційна кооперація* – це форма забезпечення інформаційної безпеки рівноправних суб'єктів інформаційного процесу (фізичних, юридичних, міжнародних), що містить сукупність взаємоузгоджених дій цих суб'єктів. Такі дії спрямовані на одержання відомостей про дестабілізуючі фактори, дестабілізуючі й інформаційні загрози та захист від них доступними законними способами й засобами.

*Інформаційне протиборство* – це форма забезпечення інформаційної безпеки, що характеризується, з одного боку, впливом на життєво важливі системи пошуку, обробки, поширення та зберігання інформації противника (особи, організації, держави), а з іншого – застосуванням заходів захисту своїх подібних систем від несанкціонованого та деструктивного впливу.

Інформаційне протиборство здійснюється між різноманітними соціальними суб'єктами (особами, суспільствами, державами), проте низка таких конфліктних взаємодій має певні, відносно стійкі ознаки, які в сукупності утворюють окремі форми протиборства (інформаційну війну, інформаційний тероризм, інформаційну злочинність).

Виходячи із вище наведеного, з точки зору інформаційного протиборства, вбачається нагальною потреба окремої розробки проблеми своєчасного виявлення фактів поширення диверсифікаційного впливу та його нейтралізації.

*Шмоткін О.В.,*
*кандидат юридичних наук, професор,*
*заслужений юрист України,*
*Національна академія Служби безпеки України*

# ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ ІНФОРМАЦІЙНОЇ ФУНКЦІЇ ПРАВА В УМОВАХ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

Необхідність подальшого удосконалення юридичного механізму захисту прав людини, підвищення ролі права у сучасному суспільстві зумовлюють науковий інтерес до дослідження функцій права. Функціональний аналіз права вже не раз перебував у центрі уваги дослідників. Але роль та значення функцій права не можуть бути сталими, адже його соціальне призначення визначається потребами суспільного розвитку. А роль інформаційної функції права, яка належить до загальносоціальної групи функцій права, в умовах сучасного інформаційного суспільства зростає. Зважаючи на це, зростає і увага науковців до проблем, пов'язаних з цією сферою.

Питання інформаційної функції права побіжно розглядалися у процесі дослідження тих чи інших аспектів функціонування права (М.Байтін, О.Гаврилов, В.Кудрявцев, В.Лебєдєв, Д.Липинський, О.Лощихін, І.Москаленко, А.Міхайлянц, Н.Оніщенко, М.Полєвой, Т.Радько, М.Расолов, А.Риженков, В.Смирнов, Н.Чечина та ін.). Окремі дослідники інформаційну функцію права вивчали у галузевому контексті. Так, М.Матійко досліджував інформаційну функцію цивільного права, О.Миронець – ефективність інформаційної функції права в Україні як законодавчої гарантії. Однак, по-перше, їх праці дещо застаріли, по-друге, раніше не проводилися наукові дослідження, в яких розкривалася б еволюція сутності інформаційної функції права, зумовлена змінами суспільного розвитку.

Функції права – це основні напрями впливу права на суспільство і правову систему. За видами розрізняють загальносоціальні та спеціально-юридичні функції права. До загальносоціальних відносять економічну, політичну, ідеологічну та інформаційну функції, до спеціально-юридичних – регуляторну (статичну та динамічну) й охоронну (профілактичну, каральну, відновлювальну). Отже, інформаційна функція права – це інформаційний вплив права на суспільство і правову систему.

Інформаційна здатність права – це один із суттєвих факторів, що дозволяє віднести його до елементів духовної культури суспільства. Не викликає сумніву, що право виникає і як інформатор, і як

регулятор суспільних відносин. У держави і суспільства достатньо каналів, засобами яких здійснюється інформування суб'єктів права. Проте право як регулятор суспільних відносин одночасно грає роль інформатора їх суб'єктів. Таким чином, воно виконує інформаційну функцію поряд зі своїми суто юридичними завданнями, набуваючи також інформаційної якості. У цьому виявляється його соціальна природа, здатність впливати на волю, свідомість і психіку людини, реалізуватися через людське сприйняття.

Учені не досягли одностайності у визначенні сутності, місця та ролі інформаційної функції права у системі правових функцій. Так, Т.Радько вважає, що вона є допоміжною, тобто належить до неосновних соціальних функцій права [1].

І.Казьмін наголошує на інформативній (пізнавальній) складовій інформаційної функції права. Він зазначає, що система права як модель суспільних відносин містить відомості про особливості структури та функціонування конкретного суспільства [2]. Дійсно, право вбирає у себе, а потім розкриває інформацію про різнобічні явища суспільного життя, оскільки у ньому міститься величезна кількість наукових дефініцій, юридичних формул, історичних та життєвих відмінностей, політичних і правових оцінок, юридичних рекомендацій, заборон, дозволів тощо.

В.Синюков вказує на орієнтаційну роль інформаційної функції права. На його думку, право є потужним джерелом моральної орієнтації суб'єктів суспільних відносин, а воно також формує соціально корисну, позитивну спрямованість правомірної поведінки суб'єктів [3]. Правова інформація – це інформація, за допомогою якої виражається (і, відповідно, формується) певний світогляд.

Ф.Фаткулін виокремлює модально-інформаційну функцію права, сутність якої полягає у доведенні нормотворчими органами відповідної правової інформації до суб'єктів суспільних відносин [4]. Держава інформує кожного суб'єкта правових відносин про суб'єктивні права та юридичні обов'язки, закладені у правових нормах у вигляді моделі бажаної або забороненої поведінки. Отже, право – це один із найважливіших засобів соціальної інформації, який використовує держава. Причому ця інформація розрахована не тільки на пасивну поведінку суб'єктів права. Вона передбачає певні дії у відповідь, приводить до досягнення позитивного результату, задоволення інтересів учасників правовідносин (громадян, посадових осіб, організацій).

Останнім часом науковці також виділяють комунікативну компоненту інформаційної функції права, адже останнє як інформаційна система виступає засобом комунікації між суб'єктом та об'єктом

управління, специфічним “посередником” між законодавцем та громадськістю, між творцями правових настанов та фізичними чи юридичними особами [5].

Таким чином, інформаційна функція права виявляється як 1) джерело знань про структуру, зміст та закономірності функціонування правової системи і суспільства в цілому (пізнавальна складова); 2) засіб для інформування, ознайомлення з правилами поведінки (орієнтаційна складова); 3) регулятор суспільних відносин, що визначає порядок певних дій (регулятивна складова); 4) засіб комунікації між державою та громадськістю (комунікативна складова). Виокремлюються два аспекти змісту інформаційної функції права: загальна інформаційна дія права та інформаційна дія, що реалізується через систему юридичних засобів, тобто через механізм правового регулювання [6].

В умовах інформаційного суспільства все більшого значення набуває регулятивна компонента інформаційної функції права, адже сьогодні навіть специфічна правова інформація стала більш доступною. Зокрема, для цивільного права характерним є засвоєння правових норм із неофіційних джерел (друзі, знайомі, сусіди тощо). Джерелом інформації про норми адміністративного та кримінального права часто виступають засоби масової інформації. Таким чином, роль інформатора, який здійснює орієнтацію поведінки суб’єктів суспільних відносин, виконують сьогодні сучасні засоби масової комунікації (соціальні мережі, ЗМІ), тоді як до офіційних видань фізичні та юридичні особи звертаються переважно у випадках, які потребують чіткої регламентації дій – регулювання.

Виокремлення комунікативної компоненти інформаційної функції права, на нашу думку, також стало можливим лише в умовах інформаційного суспільства.

Так, В. Ковальський, розкриваючи складну взаємодію принципів і функцій права, зазначає, що останні є своєрідною відповіддю на потреби суспільного розвитку, наслідком законодавчої політики, що концентрує ці потреби і трансформує їх у позитивне право, публічні обов’язки. Змінюються, збільшуються суспільні потреби – змінюються та розширюються функції та принципи права. І навпаки, зменшуються потреби – це відбивається і на функціях права. У теперішній час у результаті суспільного розвитку відбувся перехід від статичного розуміння функцій права до динамічного, тобто від однобічного (командного) до дихотомічного (соціально-ціннісного) характеру права. Тому, вважає В.Ковальський, функції права доцільно визначати двояко: один компонент функції відбиває її стабільність, інший – динаміку, змінність відповідно до суспільно-

правового розвитку. Прикладом такої двоїстості є функції організаційна та інтегративна (організаційно-інтегративна), соціальна та економічна (соціально-економічна), культурна та виховна (культурно-виховна), аксіологічна та регулятивна (регулятивно-аксіологічна) і, певна річ, інформаційна та комунікативна (інформаційно-комунікативна) [7].

Викладене дає підстави для певних висновків. Функції права, їх сутність та значення зумовлюються особливостями суспільного розвитку. В умовах сучасного інформаційного суспільства зростає роль інформаційної функції права, для якої характерними є:

1) виокремлення динамічної комунікативної складової;

2) збільшення важливості регулятивної компоненти порівняно з пізнавальною та орієнтаційною.

Ми торкнулися лише деяких аспектів реалізації інформаційної функції права в умовах інформаційного суспільства. Не викликає сумнівів потреба подальшого наукового вивчення цього питання.

## ЛІТЕРАТУРА

1. Радько Т.Н. Функции права / Т.Н.Радько // Общая теория государства и права : академический курс в 2 т. / под ред. проф. М.Н.Марченко. – М. : Зерцало, 2000. – Т. 2 : Теория права. – С. 53.

2. Казьмин И.Ф. Общие проблемы права в условиях научно-технического прогресса / И.Ф.Казьмин. – М. : Юрид. лит-ра, 1986. – 191 с.

3. Синюков В.Н. Российская правовая система: введение в общую теорию / В.Н.Синюков. – Саратов : Изд-во Сарат. ун-та, 1994. – 495 с.

4. Фаткуллин Ф. Проблемы теории государства и права / Ф.Фактуллин. – Казань, 1987. – С. 204-210.

5. Скуріхін С.М. Функціональний аспект правової культури військовослужбовців / С.М.Скурхін // Ученые записки Таврического национального университета им. В.И.Вернадского ; Серия “Юридические науки”. – Том 22(61). – 2009. – № 1. – С. 350-356.

6. Матійко М.В. Інформаційна функція цивільного права : автореф. дис... канд. юрид. наук / М.В.Матійко; Одеська національна юридична академія. – Одеса, 2009. – 20 с.

7. Ковальський В.С. Функції права: ціннісний та сутнісний виміри / В.С.Ковальський // Альманах права. – 2012. – № 3. – С. 58–62.

# ДЕРЖАВНО-ПРАВОВІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

*Авдошин І.В.,*
*кандидат юридичних наук,*
*старший науковий співробітник,*
*Національна академія Служби безпеки України*

## УДОСКОНАЛЕННЯ СИСТЕМИ АДМІНІСТРАТИВНОГО УПРАВЛІННЯ У СФЕРІ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ УКРАЇНИ З УРАХУВАННЯМ ДОСВІДУ КРАЇН ЄС І НАТО

Сучасні процеси державотворення в Україні, реформування усіх сфер соціально-політичного життя зумовлюють необхідність вивчення досвіду інших країн, у тому числі з питань охорони державної таємниці та ролі державних органів у цій сфері діяльності в загальній адміністративно-управлінській системі. Зокрема, пропонується розглянути та врахувати досвід окремих постсоціалістичних країн ЄС і НАТО, які протягом 2010-2012 років здійснили значні перетворення в реформуванні системи охорони державної таємниці та адміністративного управління нею (Естонія, Литва, Болгарія, Румунія, Чехія та інші).

З практичної точки зору зазначене дасть можливість розробити концептуальні підходи для вдосконалення національних правових механізмів адміністративного управління системою охорони державної таємниці в Україні.

Зазначимо, що основна мета взаємодії (співробітництва) НАТО як організації з будь-якою країною-членом або партнером – гарантування безпеки інформації котрою сторони обмінюються або передають незалежно від цілей такої співпраці. Нова стратегічна концепція НАТО висуває доволі жорстко вимоги до забезпечення безпеки секретної інформації та діяльності спецслужб країн-членів щодо її охорони і збереження, встановлюючи низку принципів поводження з секретною інформацією для кожного співробітника. Особливе значення надається програмі контррозвідувальної зони відповідальності, мета якої – захист секретної інформації, технологій і тим самим конкурентоспроможності в епоху глобалізації. Розв'язання цього завдання передбачається за рахунок посилення комунікації та обізнаності, розвитку партнерських відносин з ключовими державами, на-

вчаючи та формуючи їх здатність розуміти, що є загрозами (небезпеками) з точки зору контррозвідки і як забезпечити захист від них.

У системі забезпечення реалізації національної політики безпеки згаданих постсоціалістичних країн-членів ЄС і НАТО одне із чільних місць займає система внутрішньої безпекової політики, яка визначає загальну адміністративну структуру цієї системи, функції органів державної влади в діяльності із забезпечення національної безпеки, основні з яких спрямовані на забезпечення внутрішньої стабільності та захист суспільства і громадян. Підкреслимо, що для належного забезпечення національної безпеки, особлива увага, зокрема в законодавстві вказаних країн, приділяється функціонуванню та ієрархічній побудові системи адміністративного управління сферою охорони секретної інформації.

Аналіз розглянутих адміністративно-управлінських моделей у сфері охорони державної таємниці в країнах ЄС і НАТО дає змогу зробити певні узагальнення. Українське законодавство визначає Службу безпеки України спеціально уповноваженим органом державної влади у сфері охорони державної таємниці. У розглянутих постсоціалістичних країнах-членах ЄС і НАТО для належної організації та координації охорони державної таємниці створюються органи державної влади з широкими виконавчими повноваженнями. Вони відповідають за організаційно-правове забезпечення охорони секретної інформації, підзвітні та підпорядковані урядам, при цьому спецслужби виконують виключно безпекову та контрольну функції. Саме ці органи готують пропозиції уряду щодо організації захисту державної таємниці; аналізують та розглядають заяви і скарги стосовно вдосконалення діяльності із застосування чи можливості застосування вимог законодавчих актів, розглядають і засвідчують результати безпекового контролю, проведеного стосовно окремих посадових осіб, у тому числі безпекових органів, звітують перед президентами і парламентами щодо стану охорони державної таємниці. При цьому встановлено чіткі законодавчі вимоги до цих органів, їх права та обов’язки.

Тобто, на відміну від української моделі в цих країнах чітко визначено суб’єкт, відповідальний за організацію та координацію діяльності у сфері захисту секретної інформації. Таким суб’єктом є уряд, який формує відповідальний державний орган – комітет (комісію) із повноваженнями, закріпленими законодавством.

Подібна схема колись існувала в Україні, але без детальної законодавчої регламентації компетенції державних органів у сфері охорони державної таємниці з’ясувати відповідального за організацію цієї діяльності було неможливо.

Адміністративно-управлінські моделі аналізованих країн у сфері охорони державної таємниці за своєю формою та змістом близькі. Однак, на нашу думку, найдосконалішою з них за формальними ознаками й водночас найбільш подібною до української є литовська модель управління системою охорони секретної інформації. Загальне керівництво цією системою здійснює президент Литовської Республіки, уряд країни забезпечує реалізацію державної політики у цій сфері шляхом організації всіх напрямів відповідної діяльності, зокрема й безпекового. При уряді Литви створено інституцію зі статусом органу виконавчої влади – Комісію з координації захисту таємниці. Її права й обов'язки чітко визначено законодавством. Особливістю є те, що члени Комісії призначаються за відповідними квотами від президента, уряду та сейму. Очолює Комісію, як правило, Генеральний директор Департаменту державної безпеки, який підзвітний президенту та парламенту. Секретаріат та підрозділи Комісії створюються на базі відповідних структур Департаменту державної безпеки, що передбачено його статусом органу виконавчої влади у сфері охорони державної таємниці, котрий опікується питаннями як організаційного, так і безпекового характеру (схема близька за своїм змістом вітчизняній, але з більш чітким законодавчим визначенням статусу спеціальної служби з доволі широкими повноваженнями у сфері охорони державної таємниці).

Вважаємо, що литовське законодавство може послужити зразком при вдосконаленні адміністративно-управлінської моделі системи охорони державної таємниці України з урахуванням власного досвіду, який засвідчив як певні переваги, так і недоліки покладання відповідальності за стан охорони державної таємниці саме на спецслужбу.

З огляду на викладене з метою вдосконалення адміністративно-управлінської моделі у сфері охорони державної таємниці пропонується:

1. Законодавчо визначити Кабінет Міністрів України відповідальним за охорону державної таємниці в державі, як це випливає з конституційних повноважень уряду, який здійснює заходи щодо забезпечення національної безпеки України.

2. При Кабінеті Міністрів України створити Державну комісію з питань охорони державної таємниці, члени якої призначаються Президентом України за поданням Прем'єр-міністра України. Законодавчо визначити її повноваження шляхом внесення відповідних змін до Закону України "Про державну таємницю". Головою цієї Комісії за посадою має бути Голова Служби безпеки України. Загальне керівництво діяльністю Державної комісії здійснює Президент Украї-

ни, а безпосереднє керівництво її роботою покладається на Голову Служби безпеки України. Кількість членів Комісії та її персональний склад визначаються Кабінетом Міністрів України, виходячи з покладених завдань і функцій.

3. Департамент охорони державної таємниці та ліцензування Служби безпеки України, здійснюючи і контролюючи дії з охорони державної таємниці, виконує функції секретаріату (в рамках спеціально створеного структурного підрозділу або на правах автономної структури СБ України) Державної комісії з питань охорони державної таємниці. Керівник цього підрозділу призначається Кабінетом Міністрів України за поданням голови Державної комісії. Секретаріат готує матеріали засідань Комісії, організує втілення їх в життя шляхом прийняття відповідних рішень та контролює їх виконання суб'єктами режимно-секретної діяльності.

Реалізація зазначених пропозицій дозволить: по-перше, визначити орган, відповідальний за організацію діяльності, пов'язаної із забезпеченням охорони державної таємниці; по-друге, чітко визначити та конкретизувати завдання Служби безпеки України в системі охорони державної таємниці на законодавчому рівні, що дасть їй змогу належним чином забезпечувати їх реалізацію, зосередивши зусилля саме на безпековій та контрольній складових цієї діяльності.

*Алтинцева Н.М.,*
*Національна академія Служби безпеки України*

*Шевченко К.О.,*
*Національна академія Служби безпеки України*

## ІНФОРМАТИЗАЦІЯ ДЕРЖАВНИХ ОРГАНІВ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

На етапі формування інформаційного суспільства, коли визначальним цивілізаційним активом виступає інтелектуальний капітал, основним кінцевим продуктом виробництва стають інформаційно-комунікаційні технології (ІКТ). Інтеграція національного інформаційного простору до світового, з одного боку, і його захищеність та суверенітет, з іншого, є джерелами інформаційної безпеки держави. Одною з головних вимог до створення такого простору є централізація управління інформацією, а зокрема – інформатизація органів державної влади, концептуальні основи якої визначені відповідними державними програмами.

Правовою основою інформатизації є закони України “Про Концепцію Національної програми інформатизації”, “Про Національну програму інформатизації”, “Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки”. 29 серпня 2012 року Кабінет міністрів України ухвалив проект Указу Президента “Про Стратегію розвитку інформаційного суспільства в Україні”, який, з-поміж іншого, передбачає впровадження електронного врядування. Загальне керівництво інформатизацією здійснює Державне агентство з питань науки, інновацій та інформатизації України (Держінформнауки України), діяльність якого спрямовується і координується Кабінетом Міністрів України через міністра освіти і науки, молоді та спорту України [9].

Концептуальні засади управління інформаційною безпекою розглядаються у працях Є.Скулиша, О.Довганя, В.Остроухова, А.Марущака, В.Петрика. Проблемами інформаційного забезпечення діяльності органів державної влади займалися О.Бакаєв, Л.Бакаєв, Ю.Лисенко, М.Лепа, В.Порохня, В.Тронь, С.Довгий, О.Копійка, Ю.Черєпін, Ю.Марчук та інші.

Під терміном “інформатизація” ми розуміємо “сукупність взаємопов’язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесів, що спрямовані на створення умов для задоволення інформаційних потреб громадян та суспільства на основі створення, розвитку і використання інформаційних систем, мереж, ресурсів та інформаційних технологій, які побудовані на основі застосування сучасної обчислювальної та комунікаційної техніки” [4].

Національною програмою інформатизації визначено, що інформатизація державного сектору реалізується через розроблення політики та організаційно-правового забезпечення інформатизації, інформатизацію стратегічних напрямів розвитку державності, державного фінансово-економічного контролю, соціальної сфери, в галузі екології, науки, освіти та культури [4].

Сьогодні Україна має певний досвід інформатизації державних органів та впровадження інформаційно-комунікаційних систем у їх діяльність. Зокрема, сформовано загальні правові засади інформатизації державних органів: прийнято ряд нормативно-правових актів, які, зокрема, регулюють створення інформаційних електронних ресурсів державних органів та установ, гарантії та механізми доступу до публічної інформації на цих ресурсах, розвиток електронного урядування та відкритого уряду, електронного документообігу. Крім того, закладено основи безперешкодного доступу громадян до

будь-якої інформації, що не становить державної таємниці. Активізується робота із запровадження новітніх ІКТ в публічному секторі (освіта, наука, охорона здоров'я, культура та ін.).

Варто також відзначити, що органами державної влади та органами місцевого самоврядування запроваджено значну кількість інструментів електронного урядування, які можна віднести до кращих світових практик. Так, створено низку відомчих інформаційно-аналітичних систем, центрів і мереж, які забезпечують роботу органів державної влади, (наприклад, Інтегрована міжвідомча автоматизована система обміну інформацією з питань контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон "Аркан"; Єдина інформаційно-аналітична система "Вибори"; автоматизована система моніторингу інфекційних захворювань для Міністерства охорони здоров'я та ін.), єдиних державних реєстрів у різних галузях (судових рішень, підприємств та організацій України, об'єктів державної власності та ін.).

Таким чином, основним результатом процесу інформатизації українських органів державної влади стало впровадження ІКТ, яке має локальний, відомчий характер. Цілісна ж система інформаційно-аналітичного забезпечення державних органів ще не створена, а правове забезпечення інформатизації потребує оновлення на базі постійного моніторингу стану справ. Серед факторів, які уповільнюють, а в деяких аспектах і унеможливлюють процеси інформатизації, виділимо недосконалість загальнодержавної політики, повільну та недостатню координацію впровадження електронного урядування, обмежене бюджетне фінансування, закордонну елементну базу та програмне забезпечення, із якими працюють постачальники ІТ-послуг, слабку пропускну здатність та надійність зв'язку, незбалансованість фундаментальних та прикладних розробок.

Отже, очевидно, що інформатизація державного сектору має позитивний вплив на стан інформаційної безпеки особи, суспільства та держави. Основними кроками на шляху до розвитку цієї сфери мають стати прийняття національної стратегії розвитку інформаційного суспільства, впровадження електронного урядування, створення електронного уряду та становлення електронної демократії, координація впровадження інструментів електронної демократії на всіх рівнях, забезпечення відкритості інформації про діяльність органів державної влади й місцевого самоврядування.

Реалізація таких заходів вимагатиме значних ресурсів та узгоджених організаційних змін, але дасть змогу говорити про передумови формування інформаційної влади, а відтак – набуття громадянами України статусу суб'єкта управління.

## ЛІТЕРАТУРА

1. Дітковська М.Ю. Упровадження новітніх інформаційних технологій в органах державної влади і місцевого самоврядування / М.Ю.Дітковська // Теорія та практика державного управління : зб. наук. праць. – Х. : Вид-во ХарРІНАДУ “Магістр”, 2008. – Вип. 3 (22). – С. 147–251.

2. Закон України “Про Концепцію Національної програми інформатизації” // [Електронний ресурс]. – Режим доступу : http: zakon4.rada.gov.ua/laws/show/75/98.

4. Закон України “Про Національну програму інформатизації” // [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/74/98.

5. Закон України “Про інформацію” від 2 жовтня 1992 р. // [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/2657-12.

6. Закон України “Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки” від 9 січня 2007 р. // [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/537-16.

7. Інформаційна безпека (соціально-правові аспекти): підручник / [В.В.Остроухов, В.М.Петрик, М.М.Присяжнюк] ; за заг. ред. Є.Д.Скулиша. – К. : КНТ, 2010. – 776 с.

8. Про державну політику інформатизації України: Указ Президента України від 31.05.1993 № 186/93. [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/186/93.

9. Про затвердження Положення про Державне агентство з питань науки, інновацій та інформатизації: України Указ Президента України від 8 квітня 2011 року №437/2011. [Електронний ресурс]. – Режим доступу : http://www.dknii.gov.ua/images/stories/polozhennya derzhinformnauky.doc.

10. Проект Стратегії розвитку інформаційного суспільства в Україні “Від інформаційного суспільства до суспільства знань”. [Електронний ресурс]. – Режим доступу : http://www.dknii.gov.ua/images/stories/03.08.2012_start.doc.

11. Яковлева Л.І. Інформатизація влади в Україні: теоретичні засади та механізм впровадження / Л.І.Яковлева // Вестник СевГТУ : сб. науч. трудов. – Севастополь : Изд-во Севастоп. нац. техн. ун-та, 2008. – Вып. 91. – С. 41–43.

*Архипов О.Є.,*
*доктор технічних наук, професор,*
*НТУУ "КПІ"*

## ДЕРЖАВНА ТАЄМНИЦЯ У СФЕРІ НАУКИ І ТЕХНІКИ: ФІНАНСОВО-ЕКОНОМІЧНИЙ АСПЕКТ

Влітку 1940 року до відділу винахідництва Народного комісаріату оборони було подано три заявки на винаходи, що стосувалися конструкції ядерної бомби та способів збагачення урану-235. Співробітники Українського фізико-технічного інституту (УФТІ, м. Харків) Ф.Ф.Ланге, В.А.Маслов, В.С.Шпінель уперше запропонували використання звичайної вибухівки як запалу для утворення критичної маси та ініціювання ланцюгової ядерної реакції (саме у такий спосіб потім підривалися усі ядерні бомби) та відцентровий спосіб розділення ізотопів (цей спосіб і нині лежить в основі промислового виробництва збагаченої уранової суміші) [1]. Однак усі заявки отримали негативні відгуки й були заслані до спецсховища, а відповідні науково-дослідні роботи не отримали фінансування. Лише у 1946 році відділ винахідництва Червоної Армії зареєстрував авторське свідоцтво № 6358с "Атомна бомба або інші боєприпаси" та ще дві заявки харків'ян. Таким чином, формально вони є винахідниками ядерної бомби. Видані авторські свідоцтва не підлягали опублікуванню, тому прізвища винахідників стали відомі широкому загалу лише у дев'яностих роках. Єдиний, хто на той час залишався серед живих – В.С.Шпінель так оцінив можливий розвиток ситуації, якби заявки харків'ян були належно оцінені: "Думаю, що за тих можливостей, які пізніше мав Ігор Курчатов, ми б отримали її (ядерну бомбу) у 1945 році".

На жаль (чи на щастя), історія не знає умовного способу, та й судження стосовно можливих перспектив "харківського проекту" дуже різні, суперечливі, іноді діаметрально протилежні. Однак було б цікаво отримати хоча б загальну характеристику наслідків, зокрема фінансово-економічних втрат, зумовлених суб'єктивізмом фахівців-експертів та посадовців, які дали негативні відгуки щодо змісту заявок.

З цього погляду чи не найбільш прикрою виглядає ситуація, коли, з одного боку, поданий проект не отримує фінансування, а з іншого (про всяк випадок) – його зміст та матеріали оцінюються як секретні. В такому разі заявники проекту фактично відсторонюються від його виконання, що спричиняє низку негативних наслідків. Зокрема, у нашому випадку ніхто із авторів не зміг продовжити ро-

боту за тематикою проекту. В.А.Маслов невдовзі загинув на фронті, Ф.Ф.Ланге та В.С.Шпінель мусили докорінно змінити сферу своїх наукових інтересів: дослідження за "старою" ядерною тематикою тепер могли тривати лише в межах проекту, однак відсутність фінансування зробила це нереальним.

Крім того, введення режиму секретності різко обмежило можливості ознайомлення широкого загалу науковців з основними ідеями та результатами, наведеними в заявці. Фактично в УФТІ припинилися прикладні роботи, напрям яких збігався з тематикою проекту, перервався процес спадковості у набутті та переданні знань у цілій науковій галузі, формування й розвиток відповідних наукових шкіл.

Щодо формальної дати початку роботи над радянським атомним проектом. Такою вважається 11 лютого 1943 року, коли було прийнято постанову Державного комітету оборони СРСР про організацію в Москві спеціальної лабораторії атомного ядра, керівником якої призначено І.В.Курчатова. Тобто роботи за атомним проектом було розпочато на три роки пізніше подання "харківської заявки", в іншому місці, новим колективом розробників та в абсолютно відмінній економічній та зовнішньополітичній обстановці. З серпня 1945 року (тобто вже після бомбардування Хіросіми і Нагасакі) роботи над проектом набули форс-мажорного характеру, що для економіки країни, яка тільки-но з величезними втратами вийшла з війни у Європі, було надтяжким випробуванням. Радянську атомну бомбу отримано у 1948 році (29 серпня 1948 року – успішний підрив бомби на полігоні в Семипалатинській області), тобто через чотири роки після терміну, названого В.С.Шпінелєм.

Таким чином припинення фінансування роботи, яку було віднесено до секретних, призвело до низки виключно негативних наслідків. З іншого боку, витрати на фінансування системи охорони засекреченого проекту, практичне застосування результатів реалізації якого є непевним, можуть завдати значної економічної шкоди, адже вартість заходів з охорони секретів, за різними оцінками [2, 3], сягає 15-20% вартості усього проекту. Тобто, якщо загальний термін виконання проекту становить 3–5 років, сукупні витрати на охорону секретів будуть вельми серйозними. Можливим компромісом у цій ситуації вбачається практика засекречування результатів, отриманих в процесі виконання інженерно-технологічних, дослідно-конструкторських розробок, тоді як результати фундаментальних і теоретичних досліджень (за деякими винятками) становитимуть відкриту інформацію [4].

У будь-якому разі держексперт з питань таємниць має приймати рішення про віднесення певної інформації до державної таємниці не тільки за рівнем можливих втрат від оприлюднення цієї інформації, а також і за можливими негативними економічними та суспільно-політичними наслідками, зумовленими обмеженням доступу до означеної інформації.

## ЛІТЕРАТУРА

1. Гаташ В. Фізика з грифом "Цілком таємно" / В.Гаташ // Дзеркало тижня, №5 (430), 08.02.2003 р.

2. Архипов О.Є. Критерії визначення можливої шкоди національній безпеці України у разі розголошення інформації, що охороняється державою : моногр. / О.Є.Архипов, О.Є.Муратов. – К. : Наук.-вид. відділ НА СБ України, 2011. – 195с.

3. Архипов О.Є. Системний підхід до оцінювання ефективності захисту державної таємниці / О.Є.Архипов, В.П.Ворожко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні / Наук.-техн. зб. – К., 2005. – Вип. 10. – С. 18–22.

4. Филин С.А. Информационная безопасность / С.А.Филин. – М. : Изд-во "Альфа-Пресс", 2006. – 412 с.

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

## ПРОБЛЕМНІ ПИТАННЯ НАКЛАДЕННЯ АДМІНІСТРАТИВНИХ ТА ГРОШОВИХ СТЯГНЕНЬ ЗА НЕНАДАННЯ ІНФОРМАЦІЇ ПОСАДОВИМ ОСОБАМ ПРАВООХОРОННИХ ОРГАНІВ

Сфера охорони правопорядку є надзвичайно динамічною, комплексною, вона потребує постійного вдосконалення, взаємодії правоохоронних структур, можливих тільки при належному інформаційному забезпеченні [1, с. 282]. Реалії сьогодення засвідчують, що інформація на вимогу посадових осіб правоохоронних органів не завжди надається належним чином. Однією з основних причин такої ситуації є вади законодавства, що встановлює відповідальність за ненадання інформації посадовим особам правоохоронних органів.

Проблемам правового регулювання обігу інформації та відповідальності за правопорушення у вказаній сфері присвячували свої дослідження Арістова І.В., Бандурка О.М., Брижко В.М., Гурковський В.І., Кормич Б.А., Кохановська О.В., Марущак А.І., Макаренко В.В., Сопілко І.М. та інші. Їх праці стосувалися переважно загальних питань, або проблем обігу інформації певного виду, наприклад, з обмеженим доступом. Враховуючи невирішені раніше аспекти загальної проблеми правового регулювання обігу інформації, зазначимо, що новизна представлених тез доповіді полягає в тому, що в них розкриваються питання правової регламентації надання інформації саме посадовим особам правоохоронних органів.

Щодо ненадання інформації зазначимо, що найчастіше вказані правопорушення тягнуть за собою адміністративну відповідальність. Одним із актуальних напрямів реформування українського адміністративного права є модернізація інституту адміністративної відповідальності, зокрема за правопорушення в інформаційній сфері [2, с. 4]. Під час розгляду зазначених правопорушень виникають певні ускладнення. Так, чинний Кодекс України про адміністративні правопорушення (далі – КУпАП) не має окремої глави, присвяченої саме правопорушенням в інформаційній сфері, а правопорушення, які можна було б до неї включити, розміщені у різних главах Особливої частини КУпАП [3]. (Розглядаючи досвід зарубіжних країн щодо регламентації адміністративної відповідальності за правопорушення у сфері обігу інформації, слід зазначити, що, наприклад, Кодекс про адміністративні правопорушення Російської Федерації містить Главу 13 “Адміністративні правопорушення у галузі зв’язку та інформації”. Але навіть у цій главі зібрані не всі правопорушення у сфері обігу інформації [4]).

Проаналізувавши зміст чинного КУпАП, до правопорушень, пов’язаних із посяганням на право доступу до інформації, можна насамперед віднести проступки, відповідальність за які передбачена ч. 1 ст. 53-2; ч. 1 ст. 82-3, п. 3 ч. 1 ст. 83-1, ч. 1 ст. 91-3, ч. 1 ст. 91-4; ч. 1 ст. 92-1; ч. 3 ст. 96; ч. 1 ст. 163-5; ч. 1 ст. 166-4, ч. 1 ст. 166-6, ч. 1 ст. 166-9, ч. 1 ст. 172-8, ч. 1 ст. 186-3, п. 2-4 ч. 1 ст. 212-2, ч. 1 ст. 212-3, п. 2 ч. 1 ст. 212-4 [3]. Вважаємо, що законодавцю слід об’єднати всі вказані правопорушення в одній главі КУпАП, як це зроблено стосовно інших правопорушень, скажімо тих, що посягають на власність (Глава 6 КУпАП) [3].

Слід зауважити, що норми, які встановлюють відповідальність за ненадання інформації правоохоронним органам, містяться не лише в КУпАП, а також і в інших нормативно-правових актах. Відповідно до ч. 2 ст. 133 Кримінального процесуального кодексу Украї-

ни (далі – КПК України) слідчий, прокурор під час досудового розслідування мають право викликати особу, якщо є достатні підстави вважати, що вона може дати показання, які мають значення для кримінального провадження. У главі 12 КПК України запропоновано певний порядок накладення грошового стягнення за невиконання учасниками кримінального процесу процесуальних обов'язків [5]. Вважаємо, що накладення вказаного грошового стягнення за своєю суттю є не заходом забезпечення провадження, застосуванням адміністративної відповідальності до учасників кримінального процесу. Зазначимо, що КУпАП містить норми про адміністративну відповідальність за невиконання певних процесуальних обов'язків, наприклад, ст. 185-3 КУпАП передбачає адміністративну відповідальність за злісне ухилення від явки в суд свідка, потерпілого, позивача, відповідача, експерта, перекладача; а ст. 185-4 КУпАП передбачає відповідальність за злісне ухилення свідка, потерпілого, експерта, перекладача від явки до органів досудового слідства або дізнання [3]. Якщо автори КПК України не відносять накладення вказаного грошового стягнення ані до заходів адміністративної, ані до заходів кримінальної відповідальності, то фактично це новий вид провадження, який регламентований лише чотирма статтями КПК України (ст. 144-147) [5]. Через таку незначну кількість статей, що регламентують провадження по накладенню грошового стягнення за невиконання процесуальних обов'язків, виникає багато процесуальних питань, які КПК України не врегульовано. Тому пропонуємо вилучити із КПК України норми, що регламентують накладення грошового стягнення за невиконання процесуальних обов'язків, та передбачити у КУпАП відповідальність за вчинення зазначених правопорушень.

Підсумовуючи викладене, підкреслимо, що правове регулювання відповідальності за ненадання інформації посадовим особам правоохоронних органів потребує подальшого вивчення та вдосконалення.

## ЛІТЕРАТУРА

1. Бандурка О.М. Теорія і практика управління органами внутрішніх справ України : моногр. / О.М.Бандурка. – Х. : Еспада, 2004. – 779 с.

2. Благодарний А.М. Адміністративна відповідальність за порушення законодавства про державну таємницю : моногр. / А.М.Благодарний. – К. : Вид-во НА СБ України, 2008. – 180 с.

3. Кодекс України про адміністративні правопорушення від 7 грудня 1984 року № 8073-X [Електронний ресурс]. – Режим доступу : http://zakon.nau.ua.

4. Кодекс Российской Федерации об административных правонарушениях от 30 грудня 2001 року N 195-ФЗ [Електронний ресурс]. – Режим доступу : http://www.consultant.ru.

5. Кримінальний процесуальний кодекс України від 13 квітня 2012 року № 4651-VI [Електронний ресурс]. – Режим доступу : http://zakon.nau.ua.

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

*Шамсутдінов О.В.,*
*кандидат юридичних наук,*
*Національна академія Служби безпеки України*

*Салагор І.М.,*
*Управління СБУ в Чернівецькій області*

## ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ В СИСТЕМІ БІОЛОГІЧНОЇ БЕЗПЕКИ УКРАЇНИ

На початку третього тисячоліття перед людством постала життєво важлива глобальна проблема біологічної безпеки. Актуальність її зумовлена не стільки негативним впливом природних явищ, скільки антропогенною діяльністю, що стала джерелом згубного впливу на біосферу.

Розвиток науки, зокрема біотехнології, хоча й дав змогу людству перемогти небезпечні інфекційні хвороби, створив прецеденти контамінації навколишнього середовища високовірулентними збудниками бактеріальної, вірусної та рикетсійної природи. Недосконалість систем біологічного контролю при масованому впровадженні біотехнології у виробництво лікувальних і діагностичних імунобіологічних препаратів, продуктів харчування, біологічно активних добавок тощо становить реальну біологічну небезпеку для людей.

Незважаючи на ратифікацію конвенцій про заборону біологічної і токсинної зброї (1972 р.), у багатьох країнах тривають роботи, безпосередньо або опосередковано пов’язані зі створенням суперекотоксикантів біологічної природи. Існуючі банки штамів збудників інфекційних хвороб, відносна простота і доступність технології ви-

роблення токсикантів і культивування патогенних штамів мікроорганізмів створюють реальну небезпеку використання їх в антигуманних цілях.

Світ мікроорганізмів постійно еволюціонує, вдосконалюючи при цьому свої адаптаційні механізми стосовно нових несприятливих для середовища їх існування чинників. Відбуваються кількісні та якісні зміни епідемічного процесу, у тому числі генетична трансформація збудників інфекційних захворювань. У таких умовах загрозливою тенденцією сьогодення стало виникнення нових інфекційних захворювань. "Емерджентними" (від англ. emergence – виникнення) називають інфекційні захворювання, які існували в популяції людей і раніше, але раптом почали знову поширюватися, спричиняючи різке зростання кількості постраждалих. До нових відносять інфекційні захворювання, які на певній географічній території раніше взагалі не спостерігалися [1].

Глобальний характер біологічної небезпеки визначає перспективу розробки принципово нових засобів і методів профілактики і захисту населення, вдосконалення заходів з ліквідації наслідків негативного впливу контамінантів.

Ефективність і комплексність вирішення всіх аспектів проблеми біологічної безпеки значною мірою визначається доступністю відомостей, інформованістю фахівців з відповідних питань, активною наступальною інформаційною політикою держави у зазначеній сфері.

Імунізація є одним з практичних заходів з реалізації як вітчизняної, так і міжнародної програм з біологічної безпеки та біологічного захисту. Сьогодні вона вважається одним із найбільш ефективних та економічно доцільних засобів медичного втручання в епідемічний процес – профілактики численних захворювань та запобігання епідеміям.

Україна поряд з іншими європейськими державами долучилася до заходів "Європейського тижня імунізації", започаткованого у 2005 році в дев'яти країнах. У 2007 році у "тижні імунізації" взяли участь близько 20 країн, у 2008 – 32 із 53 держав-членів Європейського регіону ВООЗ. Мета акції – розширення охоплення вакцинацією населення, поглиблення розуміння, що кожна людина потребує захисту від хвороб, поліпшення пропаганди імунізації.

Преса, телебачення, радіо відіграють значну роль у формуванні суспільної думки. Це стосується і питань вакцинації, довіра до якої населення серйозно знизилася через безпрецедентну кампанію про-

тидії в ЗМІ. Помилкові уявлення, що вакцинація є більшою загрозою, ніж сама хвороба, призводять до збільшення кількості захворювань висококонтагіозними інфекціями.

Відзначимо, що в довакцинальний період на території України реєстрували високий рівень захворюваності і смертності від інфекційних хвороб. Так, на початку XX сторіччя протягом 15 років тільки від кору померло близько 500 тис. дітей. За роки проведення у країні заходів з імунопрофілактики захворюваність на інфекційні хвороби зменшилася в десятки разів, проте зниження рівня охоплення щепленнями у середині 1990-х років призвело до епідемії дифтерії, зростанню захворюваності на кір та краснуху. Під час епідемії дифтерії в Україні у 1994-1996 рр. на території більшості областей реєстрували підвищений рівень захворюваності на цю хворобу. Траплялися навіть смертельні випадки: у 1995-1996 рр. померло 317 людей, з них 79 дітей [2].

За словами Р.Богатирьової, "високого рівня охоплення щепленнями можна досягти, з одного боку, за достатнього рівня забезпечення імунобіологічними препаратами та відповідального ставлення населення до свого здоров'я, а з іншого – за умови грамотної інформаційної кампанії" [3].

У ході формування і подальшої реалізації Державної цільової програми біобезпеки та біологічного захисту на 2015-2020 роки [4] слід, на нашу думку, приділити значну увагу заходам інформаційного забезпечення системи біологічної безпеки України.

Крім зазначених вище, до таких заходів слід віднести також оперативне інформування та підготовку фахівців у сфері біологічної безпеки. З цією метою вбачається важливим об'єднати нормативно-правові, наукові та прикладні матеріали з цієї проблеми, розосереджені по численних інформаційних медичних, екологічних, ветеринарних, епідеміологічних, біохімічних, мікробіологічних, біотехнологічних рубриках, у рамках однієї дисципліни, а відповідні навчальні матеріали розподілити за такими інтегральними розділами:

1. Нормативно-правове регулювання у сфері біологічної безпеки.
2. Джерела біологічної небезпеки.
3. Біологічний тероризм і біологічні диверсії.
4. Засоби та методи виявлення біологічної небезпеки та індикації біологічних уражаючих агентів.
5. Методи та засоби технічного захисту, профілактики та лікування.
6. Ліквідація наслідків біологічного зараження.

## ЛІТЕРАТУРА

1. Слободкін В.І. Деякі особливості розвитку епідемічного процесу за сучасних умов виробництва харчових продуктів [Електронний ресурс] / В.І.Слободкін, Н.Г.Шелкова, В.М.Левицька. – Режим доступу : http://www.medved.kiev.ua/arh_nutr/art_2006/n06_3_2.htm.

2. Європейський тиждень імунізації в Україні // Газета "Еженедельник АПТЕКА" (інтернет-версія). – № 42 (513). – 31 жовтня 2005 року [Електронний ресурс]. – Режим доступу : http://www.apteka.ua/article/34173.

3. Раїса Богатирьова: Щорічно вакцинація рятує життя трьох мільйонів дітей в усьому світі / Богатирьова Раїса // Медичний світ. – 21.03.2013 [Електронний ресурс]. – Режим доступу : http://medsvit.org/news/1/1698/ra-sa-bogatirova-schor-chno-vaktsinats-ya-ryatu-zhittya-troh-m-ljon-v-d-tej-v-usomu-sv-t/.

4. Розпорядження КМУ від 25 червня 2012 р. №466-р "Про схалення Концепції Державної цільової програми біобезпеки та біологічного захисту на 2015-2020 роки" [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/466-2012-%D1%80.

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

## ПИТАННЯ ВІДСТЕЖЕННЯ ОСІБ З ВИКОРИСТАННЯМ СОЦІАЛЬНИХ МЕРЕЖ

Останнім часом у глобальних інформаційно-телекомунікаційних мережах усе більшого поширення набуває новий вид протиправної деструктивної діяльності – відстеження осіб, збирання та аналіз персональних даних користувачів, які потім передаються для несанкціонованого використання стороннім особам, здебільшого для комерційних, а у ряді випадків і злочинних цілей, відбувається розголошення та протиправне використання конфіденційної інформації щодо сфери приватного життя, порушуються особисті конституційні права людей.

Автор уже неодноразово наголошував, що сучасний стан накопичення та збереження персональних даних особи у соціальних мережах створює плідне підґрунтя для втягування наших співгромадян

іноземними спецслужбами, терористичними та іншими злочинними організаціями у протиправну діяльність [1, 2].

При цьому слід підкреслити, що раніше здебільшого мали місце факти лише викрадення персональних даних користувачів, проте останнім часом почастішали випадки відстеження конкретних користувачів соціальних мереж, їх соціальних та особистих зв'язків і пристрастей. Найбільшого поширення це явище набуло в соціальній мережі Facebook. На практиці це здійснюється з використанням різних сучасних технологій, наприклад, файлу ідентифікатора cookie [1, с. 316–317].

Показово, що соціальна мережа Facebook у 2007 році запустила соціальну маркетингово-рекламну систему Facebook Beacon ("Маяк"). Система мала повідомляти "друзям" користувача соціальної мережі, які ресурси він відвідав, проте фактично обмін даними здійснювався без дозволу користувачів. В результаті виникла хвиля протестів, і засновнику Facebook довелося вибачатися за порушення права користувачів на конфіденційність.

Мусимо констатувати, що попит на персоніфіковану конфіденційну інформацію про користувачів постійно зростає, а розробники соціальних мереж створюють усе нові інтерфейси і платформи для збору саме такої інформації. Зокрема, соціальна мережа Facebook розробила і впровадила користувальницький інтерфейс Timeline, який дозволяє користувачам відстежувати всі події в своєму житті від моменту реєстрації в соціальній мережі. Цю інформацію, вочевидь, будуть використовувати як соціальні мережі, так і їх "замовники" у своїх цілях, зокрема і протиправних.

Більше того, придбавши соціальний геологаційний сервіс Glancee, Facebook можна проводити пасивне визначення місця перебування конкретного користувача мережі. Цей сервіс ніби "дружнього стеження" сповіщає користувача про те, що поруч знаходяться його "друзі", їх зв'язки та особи зі схожими інтересами. На відміну від Forsquare, Glancee показово не вимагає реєстрації. Він працює у "тіні", фактично проводячи моніторинг GPS-даних із мобільних телефонів. При цьому творці додатку рекламують сервіс як "спосіб виявити навколо себе приховані зв'язки" [3]. Варто звернути увагу на те, що під слушним приводом сьогодні соцмережа Facebook розробляє відповідний додаток і для смартфонів.

Відстеження переміщення користувачів соціальних мереж також проводиться через з'ясування IP-адрес, з яких користувач заходив, наприклад, в особисту пошту. Зокрема, співробітники Інституту Макса Планка в Німеччині протягом 2009–2011 років стежили за кореспонденцією 43 млн (!) користувачів поштового аккаунту Yahoo [4].

Як вважають експерти, можливими є угоди між конкретними державами і володільцями соцмереж за схемою “розширення за контроль”. Справді, на практиці розвиток не анонімних мереж для конкретної держави може бути вигідним, оскільки вони є чудовим джерелом отримання інформації для спецслужб. Зокрема, встановлення контролю над соціальними мережами відповідає загальній доктрині РФ щодо кіберпростору [5]. Доказом практичної реалізації таких спрямувань є те, що в 2012 році мала місце зустріч засновника соціальної мережі Марка Цукерберга з російським прем’єр-міністром Д.Медведєвим, де обговорювалася присутність мережі Facebook у Росії не тільки як соцмережі, а і як компанії, котра працює з найбільш передовими технологіями.

На сьогодні Facebook створили черговий додаток – програму пошуку Graph Search. Пошук ведеться за інформацією, яка знаходиться в профілі чи в публічному доступі. До речі, нові налаштування не дозволяють закривати інформацію, яка перебуває в профілі. Всіх інших налаштувань приватності Facebook дотримується. Але, напевно, в пошуковику закладено можливості зчитувати закриту інформацію фахівцям соцмережі, а також спецслужб.

Пошукові запити можна уточнювати для отримання більш чітких відповідей. Якщо дані пошуку відсутні або їх недостатньо, підключається програма-пошуковик Bing, яка інтегрована з Facebook. Тобто результати web-пошуку також доступні, хоча не є основними.

Цей новий інструмент пошуку інформації стає легальним, проте, він продовжує виконувати функцію відстеження.

На жаль, вітчизняна правоохоронна система неспроможна сьогодні забезпечити належний захист наших громадян і національні інтереси від протиправних діянь, що реально вчиняються проти них з використанням викрадених із соціальних мереж персональних даних. Це, у свою чергу, зумовлює об’єктивну необхідність негайного вироблення на державному рівні принципово нових підходів до забезпечення захисту інтересів особи, суспільства та держави у цій сфері.

## ЛІТЕРАТУРА

1. Гавловський В.Д. До питання несанкціонованого збору та систематизації персональних даних користувачів через соціальні мережі / В.Д.Гавловський // Боротьба з організованою злочинністю і корупцією : наук.-практ. журнал. – 2011. – № 2-3 (25-26). – С. 312–320.

2. Гавловський В.Д. Використання соціальних мереж іноземними спецслужбами як потенційна загроза національній безпеці України / В.Д.Гавловський // Актуальні проблеми управління інформа-

ційною безпекою держави : зб. матер. наук.-практ. конф. (30 березня 2012 р., м. Київ). – К : Наук.-вид. відділ НА СБ України, 2012. – С. 56–59.

3. Интернет-паноптикум Facebook / [Електронний ресурс]. – Режим доступу : http://www.sostav.ua/news/2012/10/02/127/52214.

4. За нами следят через Интернет / [Електронний ресурс]. – Режим доступу : http://ukrlenta.net/za-nami-sledyat-cherez-internet.

5. Савин Л. Холодная кибервойна [Електронний ресурс] – Режим доступу : http://www.stoletie.ru/geopolitika/holodnaja_kibervojna_632.htm).

*Гіда О.Ф.,*
*кандидат юридичних наук, доцент,*
*Міжвідомчий науково-дослідний центр*
*з проблем боротьби з організованою злочинністю*
*при РНБО України*

## СУЧАСНИЙ СТАН ОРГАНІЗАЦІЙНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ СИСТЕМИ КІБЕРБЕЗПЕКИ УКРАЇНИ

За роки незалежності Україна здійснила певні кроки на шляху розвитку національної інформаційної сфери. Сьогодні державна інформаційна політика націлена на розбудову якісно нового вітчизняного інформаційного суспільства, що, у свою чергу, є запорукою поступального політичного і соціально-економічного руху [1, с. 2].

Зазначені процеси відбуваються в умовах інтенсивного міжнародного інформаційного обміну через глобальні комп'ютерні мережі, посиленого впливу електронних і друкованих ЗМІ на соціально-політичне та культурне життя країни, моральний стан суспільства, формування громадської думки та участь громадян у суспільних процесах [2, с. 60].

Саме тому вкрай важливо створити підґрунтя для формування якісно нового інформаційного простору в Україні, а також необхідні умови для його інтеграції у світовий інформаційний простір з відповідним забезпеченням інформаційної безпеки особистості, суспільства і держави.

Кінцевою метою державної інформаційної політики має стати прагнення до побудови в країні демократичного і безпечного інформаційного суспільства, інтегрованого у світове інформаційне співтовариство. Для успішного вирішення цього завдання, на наш погляд, необхідно сконцентрувати зусилля на вирішенні таких проблем.

*Перше*. Забезпечити сприятливі умови для створення, розвитку і ефективного використання інформаційних ресурсів у всіх сферах діяльності.

Одним із пріоритетних завдань є формування, модернізація і використання національних інформаційних ресурсів, інформаційно-телекомунікаційної інфраструктури, інформаційних, телекомунікаційних і комп'ютерних технологій [2, с. 74]. Особливо слід зосередитись на зміцненні вітчизняного науково-виробничого потенціалу інформатизації, телекомунікацій і зв'язку.

*Друге.* З урахуванням міжнародних стандартів забезпечити розвиток вітчизняної інформаційно-телекомунікаційної інфраструктури з метою виробництва інформаційного продукту та ефективної системи надання різних інформаційних послуг користувачам передусім населенню.

Особливу увагу слід приділити реформуванню інформаційного забезпечення в системі органів державної влади.

*Третє.* Сприяти розвиткові вітчизняного ринку інформаційних і телекомунікаційних систем та технологій, орієнтованих на роботу у внутрішніх комп'ютерних мережах. Доцільно звернути увагу на суттєве посилення підтримки вітчизняних розробників і національних наукових шкіл, які працюють в інформаційній сфері, та визначення системи державних пільг у цій галузі.

*Четверте*. Продовжити роботу з нормативного регулювання функціонування в Україні міжнародних інформаційних систем, а також електронних і друкованих засобів масової інформації. Це має забезпечувати насамперед вільний обіг інформації та конституційне право громадян на її пошук, отримання, виробництво і розповсюдження. Важливим убачається й активізація співпраці держави з мас-медіа.

Назріла потреба розробки правових, економічних і організаційних механізмів для забезпечення в діяльності ЗМІ балансу інтересів особистості та держави, сприяння ефективному виконанню ними функції об'єктивного й неупередженого інформування суспільства про події внутрішнього та міжнародного життя, недопущення монополізації інформаційних ресурсів.

*П'яте.* Виникла об'єктивна необхідність посилення державного контролю за діяльністю міжнародних неурядових організацій, що існують за рахунок засобів і ресурсів, у тому числі фінансових, наданих іноземними державами та їх міжнародними представництвами. Як свідчить практика, представництва низки МНО в Україні відкрито лобіюють інтереси іноземних країн, підтримують опозиційні сили та проводять активну роботу, спрямовану на зміну чинної влади [3, с. 116].

Тому інформаційна політика держави має скеровуватись на нівелювання інформаційних атак, що здійснюються іноземними МНО і завдають значної шкоди внутрішнім інтересам України та її міжнародному іміджу.

*Шосте.* Правове регулювання інформаційних відносин у суспільстві має спрямовуватися на забезпечення рівності всіх учасників інформаційної взаємодії та контролю за дотриманням законодавства у цій сфері.

Необхідно також передбачити способи і механізми захисту суспільства від неправдивої, викривленої чи недостовірної інформації, яка надходить через ЗМІ, запровадити ефективну систему щодо недопущення негативних наслідків, пов'язаних із втручанням у внутрішні справи України з боку інших держав.

*Сьоме.* Нормативно-правова база у сфері регулювання розвитку інформаційного суспільства (чинна та яка готується) і заходи щодо формування державної інформаційної політики мають повною мірою узгоджуватися із завданнями у сфері інформаційної безпеки.

З цією метою необхідно запровадити ефективну систему своєчасного виявлення та протидії використанню нових інформаційних технологій для створення загроз національній безпеці України [4, с. 186].

*Восьме.* Стратегія розбудови інформаційного суспільства України має передбачати активну співпрацю в цій галузі з іншими державами. У цьому напрямі доцільно здійснити комплекс заходів, спрямованих на забезпечення інтересів країни в міжнародному інформаційному обміні, безпеку національних інформаційних ресурсів та інформаційно-телекомунікаційної інфраструктури й участь офіційних структур у розробці міжнародного законодавства з цих питань.

Таким чином, поглиблення демократичних процесів в Україні напряму пов'язане з урегулюванням суспільних відносин в інформаційній сфері, створенням ефективної системи взаємодії всіх елементів інформаційного суспільства та нейтралізації інформаційно-психологічних впливів, скерованих на маніпулювання свідомістю суспільства, зміну його соціальної поведінки, що породжує напруженість і зниження рівня керованості в державі. Врахування цих проблем при визначенні основних засад і реалізації державної інформаційної політики сприятиме посиленню безпеки країни в політичній, економічній та соціальній сферах, стане дієвим засобом протидії загрозам національній безпеці України.

## ЛІТЕРАТУРА

1. Про основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки : Закон України від 1 січ. 2007 р. № 537-V

/ [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/537-16/print1359538156662403.

2. Почепцов Г.Г. Інформаційна політика [Текст] : навч. посіб. / Г.Г.Почепцов, С.А.Чукут. – К. : Вид-во УАДУ, 2002. – Ч. 1. – 88 с.

3. Поляруш А.А. Украина: эволюция “революций” / А.А.Поляруш, А.М.Юрченко. – К. : Саммит-книга, 2013. – 219 с.

4. Нормативно-правові та методологічні засади упорядкування інформаційних відносин : наук.-метод. посіб. / авт. кол. : В.Брижко, В.Цимбалюк, М.Швець ; [за ред. В.Тація, В.Тихого, М.Швеця]. – К. : ТОВ “Пан Тот”, 2009. – 324 с.

*Горова С.М.,*
*кандидат наук із соціальних комунікацій,*
*Міжвідомчий науково-дослідний центр*
*з проблем боротьби з організованою злочинністю*
*при РНБО України*

## СУЧАСНИЙ НАЦІОНАЛЬНИЙ ІНФОРМАЦІЙНИЙ СУВЕРЕНІТЕТ І ОСОБЛИВОСТІ ЙОГО ЗАБЕЗПЕЧЕННЯ В УМОВАХ ГЛОБАЛІЗАЦІЇ

Інформаційний суверенітет тісно пов’язаний з інформаційною базою, що є основою існування і розвитку нації. Тобто, *суверенні масиви інформації містять ту частину загального інформаційного ресурсу, без якої неможливе існування і розвиток нації.* Порівняно з інформацією загальної значимості суверенна частина ресурсів соціальних інформаційних баз змінюється саме під впливом викликів, що зумовлюють еволюцію суверена. Суверенні масиви інформації (в масштабах держави, нації – це надбання багатьох попередніх поколінь, наявний уже доробок покоління нинішнього) відіграють суттєву еталонну, стабілізуючу роль, забезпечують спадкоємність напрацьованих традицій, духовно-ціннісних орієнтирів у сфері інфотворення.

Наявність багаторівневої системи необхідних для розвитку держави, нації всіх елементів сучасної складної соціальної структури суверенних інформаційних ресурсів, що у своїй сукупності становлять інформаційний суверенітет українського суспільства, є показником його гармонійного розвитку і життєздатності. У нинішньому швидкоплинному за подіями і ситуаціями світі ефективність інформаційного суверенітету вимірюється якістю контролю інфор-

маційних ресурсів національними засобами. Цей контроль останнім часом особливо ускладнений розвитком новітніх інформаційних технологій, зокрема, соціальних мереж.

З розвитком глобального інформаційного простору, процесів глобальної інформатизації, соціальних інформаційних комунікацій, з одного боку, і демократизації суспільства, що охоплює все більше регіонів земної кулі, диференціює суспільство, – з іншого, проблема забезпечення інформаційного суверенітету народів і держав набуває все більшого значення. Лише її успішна реалізація може забезпечити відвернення загрози всесвітньої уніфікації, тобто тупикового шляху розвитку нашої цивілізації.

Практика інформаційної діяльності протягом останніх десятиріч свідчить, що такі загрози насамперед пов'язані з:

– можливістю порушення змістовної цілісності, недостатнього забезпечення необхідної вичерпності суверенних масивів інформації у структурі соціальних інформаційних баз для існування і розвитку держави, нації, всіх необхідних соціальних складових сучасного суспільства;

– можливістю порушення організаційної структури дотримання і розвитку інформаційного суверенітету;

– відсталістю у процесі розвитку інформаційних технологій, призначених для обслуговування суверенних масивів інформації, а також технологій забезпечення і розвитку інформаційного суверенітету;

– зменшенням значення інформаційного ресурсу ЗМІ як джерела оновлення суверенних інформаційних ресурсів через зниження якості відображення державних, національних інтересів, можливим послабленням їх значення в об'єктивному, оперативному інформуванні суспільства про найбільш значимі для нього події, у зв'язку з погіршенням якості інформаційної діяльності, ослабленням суспільної ролі в утвердженні духовно-ціннісних орієнтирів сучасної України;

– відставанням правової бази забезпечення інформаційного суверенітету від об'єктивних умов його реалізації;

– порушенням основ збереження балансу вітчизняних (державних, національних) інтересів у міжнародному інформаційному співробітництві.

Суттєві загрози дотриманню оптимального для розвитку суспільства інформаційного суверенітету пов'язані з недостатньою ефективністю організаційної діяльності щодо оновлення суспільно значущих ресурсів інформації та їх використанням.

Негативним фактором є також неефективне використання інструментів захисту інформаційного суверенітету при поповненні відповідних суверенних масивів інформації новими надходженнями

через канали всіх видів ЗМІ: друкованих, електронних, а також тих у їхньому складі, що у процесі свого розвитку набувають самобутності та виокремлюються як Інтернет-ЗМІ, соціальні комунікації.

Слід однак зауважити, що сьогодні, порівняно із розвитком ЗМІ, інструменти захисту інформаційного суверенітету розвиваються слабо. Можна констатувати, що сучасні українські ЗМІ у своїй сукупності не забезпечують необхідної збалансованості у відображенні суспільного життя. У їх спектрі нерівномірно представлені всі активні суб'єкти суспільного життя. Розвиток приватних ЗМІ призводить до втрати позицій в інформаційному просторі державних ЗМІ. У теперішній час інтереси держави дуже кволо представлені у соціальних мережах.

При цьому варто звернути увагу на те, що загроза техніко-технологічного відставання інформаційної сфери існування українського суспільства зумовлює загрози інформаційному суверенітету під впливом цілої низки негативних чинників. Серед них найбільш відчутною є засновані зазвичай на нових технологічних рішеннях комп'ютерна злочинність, комп'ютерний тероризм, несанкціоноване проникнення в суверенні масиви інформації, що становлять державну та іншу передбачену законом таємницю, інтелектуальну власність соціальних структур та окремих членів суспільства. Як свідчить міжнародна практика, реальними сьогодні є також загрози, пов'язані зі спробами введення в суверенні інформаційні масиви недостовірної, руйнівної для них інформації.

На противагу негативним інформаційним стратегіям необхідні рішучі дії управлінських структур, підтримані позицією активної частини громадськості щодо перехоплення ініціативи у висвітленні ситуації та вжиття заходів із подолання можливих криз. Зменшення дієвості та нівелювання спрямованих проти України інформаційних акцій передбачають також зміну тематизації задіяних у випадку кризових явищ сценаріїв, створення та функціонування централізованої системи антидифамації та представлення власної позиції [1].

Варто підкреслити, що організаційні форми впливу на інформаційні процеси у справі забезпечення суверенітету можуть бути ефективними лише в разі комплексного їх застосування. Інформаційна сфера України і насамперед її інформаційні ресурси сьогодні не мають ефективної правової бази для свого збереження і розвитку. Отже, цінним може бути врахування досвіду розвинених країн, що нині рухаються шляхом цілеспрямованого правового впорядкування відносин у національному інформаційному просторі, ухвалюють необхідні законодавчі акти, перебудовують діяльність органів державної влади, які відповідають за формування та реалізацію інформаційної політики [2].

Загалом, як наголошує С.Петраков, за результатами ґрунтовного аналізу різних підходів до державного регулювання інформаційної сфери серед інваріантних властивостей, що виступають ядром будь-якої концепції регулювання інформаційної сфери, можна виділити використання комплексного підходу, заснованого на підтримці балансу інтересів держави, суспільства, підприємницьких кіл і окремої особи. При цьому підкреслюється провідна координуюча роль держави як органу, здатного виразити й забезпечити захист інтересів усього суспільства [3].

Вітчизняні центри збереження інформації, складові забезпечення національного інформаційного суверенітету поки що використовують малоефективні форми кооперації, не виступають об'єднаним, потужним інформаційним, заснованим на суверенних масивах інформації ресурсом, орієнтованим на задоволення запитів українського користувача, гідного представлення інформаційного потенціалу України в глобальному інформаційному просторі.

Отже, вирішення проблеми якісного зберігання, ефективного використання і перспективного розвитку суверенних для кожної держави, нації масивів інформації можливе лише в разі вироблення єдиної стратегії, загальної системи реалізації національної політики, ефективних інструментів забезпечення інформаційного суверенітету, що в сучасних умовах є важливим чинником суспільного розвитку.

## ЛІТЕРАТУРА

1. Варивода Я.О. Інформаційне супроводження зовнішньополітичних рішень / Я.О.Варивода // Інформаційно-аналітична діяльність у міжнародних відносинах : матеріали наук.-практ. конф. – Хмельницький : ТУП, 2003. – Ч. 2. – С. 3–7.

2. Е-майбутнє та інформаційне право / В.Брижко, В.Цимбалюк, М.Швець, М.Коваль, Ю.Базанов ; [за ред. М.Швеця]. – [2-ге вид., доп.]. – К. : НДЦПІ АПрН України, 2006. – С. 117–122.

3. Петраков С.І. Моделі державного регулювання інформаційної сфери: закордонний досвід [Електронний ресурс] / С.І.Петраков // Актуальні проблеми державного управління : зб. наук. пр. Харк. регіон. ін-ту держ. упр. Нац. акад. держ. упр. при Президентові України. – 2011. – № 1 (39). – Режим доступу : http://www.kbuapa.kharkov.ua/e-book/apdu/2011-1/.

*Гринь А.К.,*
*кандидат технічних наук, доцент,*
*Національна академія Служби безпеки України*

# ФОРМУВАННЯ ЗМІСТУ ВИЩОЇ ОСВІТИ ФАХІВЦІВ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Кардинальні зміни у політичному, економічному та соціальному житті, орієнтація країни на інноваційний розвиток визначили необхідність модернізації системи освіти. Значення цієї проблеми, її соціальна вага відображені в положеннях та принципах, закріплених у Законі України "Про вищу освіту", а також отримали розвиток у концептуальних документах – "Національній доктрині розвитку освіти" (затверджена Указом Президента України від 17 квітня 2002 року № 347/2002) та "Основних напрямах реформування вищої освіти в Україні" (затверджена Указом Президента України від 12 вересня 1995 року № 832/95).

Для реформування та розвитку вищої освіти в Україні потрібні якісно нові підходи до інноваційного оновлення змісту вищої освіти майбутніх фахівців із забезпечення інформаційної безпеки держави. Ця діяльність спрямована на забезпечення переходу до демократичної правової держави, соціально-орієнтованої ринкової економіки, а також подолання можливого відставання від позитивних світових тенденцій економічного та суспільного розвитку.

Вітчизняна система підготовки фахівців спроможна гідно конкурувати з відповідними системами розвинених країн світу. Подальший розвиток можливий винятково за умови підтримки з боку науково-педагогічної спільноти, посилення ролі держави у цій сфері, глибокої та всебічної модернізації професійної підготовки фахівців, пошуку та розробки інноваційних рішень.

Головною метою розвитку змісту вищої освіти було і залишається інноваційне оновлення та забезпечення відповідної якості освіти на основі збереження її фундаментальності, престижності, конкурентоздатності, відповідності актуальним та перспективним потребам особи, суспільства, держави. Для досягнення поставленої мети необхідно досягти нової сучасної якості освіти у сфері інформаційної безпеки держави, сформувати нормативно-правові та організаційно-економічні механізми залучення бюджетних та позабюджетних ресурсів, підвищення ролі всіх учасників навчально-виховного процесу.

У сучасних умовах зміст вищої освіти активно модернізується. Здійснюється перехід від дисциплінарно-професійної моделі освітнього процесу до проблемно-орієнтованої підготовки фахівців, де системоутворювальним фактором стає зміст та структура їхньої майбутньої професійної діяльності. Саме такий підхід до навчання відповідає сучасним уявленням про фундаментальну освіту, про організацію навчально-виховного процесу підготовки фахівців, здатних ефективно вирішувати професійні завдання, адаптуватися до нових умов та перетворень, займатися самоосвітою.

Актуальність проблеми полягає в тому, щоб максимально спираючись на існуючі доробки вдосконалити зміст вищої освіти у галузі інформаційної безпеки держави з метою забезпечення відповідності пріоритетним завданням шляхом підготовки фахівців з високими професійними та особистими якостями.

На нашу думку, вирішення цієї проблеми полягає в розробці інноваційного змісту вищої освіти у галузі інформаційної безпеки держави, що має вирішальне значення для досягнення випереджувального характеру вітчизняної освіти, її відповідності актуальним та перспективним потребам особи, суспільства, держави.

Використання нормативно-правової бази вищої освіти в Україні з урахуванням Стратегії національної безпеки України "Україна у світі, що змінюється", Стратегії державної кадрової політики на 2012-2020 роки, завдань керівництва Служби безпеки України з актуальних питань удосконалення відомчої системи підготовки кадрів у сфері забезпечення державної безпеки та її подальшого інноваційного розвитку дозволить здійснити концептуальне наукове та прикладне обґрунтування сутності, змісту, структури та напрямів ефективного розвитку підготовки фахівців у галузі інформаційної безпеки держави.

*Гуз А.М.,*
*доктор історичних наук, доцент,*
*Національна академія служби безпеки України*

## СТАНОВЛЕННЯ ТА РОЗВИТОК СВІТОВИХ СТАНДАРТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Жодне суспільство не може існувати без законодавства та нормативних документів, які регламентують правила, процеси, методи виготовлення та контролю якості товарів, робіт і послуг, а також га-

рантують безпеку життя, здоров'я, майна людей та навколишнього середовища. Стандартизація якраз і є тією сферою, якій притаманні ці функції.

Стандартизація – діяльність, що полягає у встановленні положень для загального і багаторазового застосування щодо наявних чи можливих завдань з метою досягнення оптимального ступеня впорядкування у певній сфері, результатом якої є підвищення ступеня відповідності продукції, процесів та послуг їх функціональному призначенню, усуненню бар'єрів у торгівлі і сприянню міжнародному співробітництву.

Об'єктом стандартизації є продукція, процеси та послуги, зокрема матеріали, приміщення, обладнання, системи, їх сумісність, правила, процедури, форми методи чи взагалі діяльність.

Метою стандартизації в сучасному світі є забезпечення безпеки життя та здоров'я людини, тварин, рослин, а також майна та охорони довкілля, створення умов для раціонального використання всіх видів національних ресурсів та відповідності об'єктів стандартизації своєму призначенню, сприяння усуненню технічних бар'єрів у торгівлі.

У 1947 році була створена Міжнародна організація зі стандартизації (International Standards Organization – ISO, штаб-квартира – в Женеві). Першочерговою її метою стало створення лише системи стандартів, які б сприяли міжнародній торгівлі. Більшість країн світу мають національні представництва та національні комітети в ISO.

ISO взаємодіє з іншими міжнародними організаціями зі стандартизації. В галузі інформаційної безпеки такою організацією є IEC – Міжнародна електротехнічна комісія, створена в 1906 р., метою якої є встановлення міжнародних стандартів у всіх галузях, пов'язаних з електрикою, електронікою та радіотехнікою.

Міжнародною організацією зі стандартизації прийнято низку стандартів, які діють у Європейському співтоваристві. Основні з них: ISO 9000, ISO 9001, ISO 9004 (менеджмент якості); ISO 10001, ISO 10002, ISO 10003, ISO 10004 (задоволеність споживачів); EN 9100 (СМК в аерокосмічній галузі); ISO/TS 16949 (СМК в автомобілебудуванні); ISO 14001 (екологічний менеджмент); OHSAS 18001 (професійна безпека); ISO 31000 (менеджмент ризиків); ISO 20000 (СМК ІТ-послуг); ISO 22000 (продовольча безпека); ISO 26000 (соціальна відповідальність); ISO 50000 (системи менеджменту в енергетиці); ISO 27001 (інформаційна безпека).

Перші стандарти інформаційної безпеки розроблено на початку 1980-х років. Вони стосувалися передусім інформаційної безпеки ПЕОМ.

Ключовим міжнародним стандартом з безпеки інформації є розроблений Міжнародною організацією стандартів ISO/IEC 17799:2000 Information Security Management Standard (Code of Practice for Information Security Management) – звід правил і норм управління безпекою в галузі інформаційних технологій [5]. ISO 17799 містить практичні правила з управління інформаційною безпекою, які можуть використовуватися як критерії для оцінки механізмів безпеки організаційного рівня, включаючи адміністративні, процедурні та фізичні заходи захисту.

Варто зазначити, що цей стандарт бере свій початок з 90-х років XX ст. Саме тоді Британський інститут стандартів (BSI) за участі комерційних організацій, (Shell, National Westminster Bank, Midland Bank, Unilever, British Telecommunications, Marks & Spencer, Logica та ін.) зайнявся розробкою стандарту управління інформаційною безпекою. В 1995 р. був прийнятий національний британський стандарт BS 7799 **(**Практичні правила управління інформаційною безпекою) з управління інформаційною безпекою та її організації незалежно від сфери діяльності.

Перша частина стандарту мала рекомендаційний характер, а друга – призначалася для сертифікації та містила частину обов'язкових вимог, які не увійшли до першої.

У 1999 році опубліковано другу частину стандарту: BS 7799 частина 2 "Системи управління інформаційною безпекою – Специфікація та керівництво щодо застосування" (Системи управління інформаційною безпекою – специфікації з керівництвом з використання). На цій базі був "розроблений стандарт ISO / IEC 27001:2005 "Інформаційні технології. Методи забезпечення безпеки. Системи менеджменту інформаційної безпеки. Вимоги", відповідно до якого може проводитися сертифікація.

У 2005 році вийшла нова редакція стандарту ISO 17799:2005 – сертифікаційний стандарт ISO 27001. У 2007 році ISO 17799 переопрацьовано і перевидано під номером ISO / IEC 27002.

Основний зміст стандарту зберігся, але багато що було повністю перероблено, щоб краще відповідати новим інформаційним загрозам і викликам безпеці.

Сьогодні міжнародні стандарти інформаційної безпеки все більше стають основою для розробки стандартів безпеки й ефективних методів управління інформаційною безпекою в конкретній організації, на підприємстві, в установі.

## ЛІТЕРАТУРА

1. Беляков К. Інформатизація організаційно-правової сфери суспільної діяльності / К.Беляков // Право України. – 2004. – № 6. – С. 88-92.

2. Кушакова-Костицька Н. Від свободи слова до інформаційного суспільства / Н.Кушакова-Костицька // Право України. – 2004. – № 7. – С. 129-133.

3. Задорожня Л. До питання огляду законодавства в інформаційній сфері / Л.Задорожня // Правова інформатика. – 2004. –№ 3. – С. 18-23.

4. Сідак В. Міжнародний стандарт ISO 17799 як складова в галузі менеджменту інформаційної безпеки / В.Сідак, В.Артемов // Юридичний журнал "ЮСТИНІАН" № 11/2007 [Електронний ресурс]. − Режим доступу : http://www.justinian.com.ua/article.php?id=2802.

5. Богданов О. "Адаптація міжнародного стандарту управління інформаційною безпекою ISO / IEC 27001:2005у структурах державного управління України". [Електронний ресурс] / О.Богданов, О.Бакалинський. – Режим доступу : http://nc.nusta.com.ua/Kyrsi%202009/tezi/images_tezi/S_6_Bogdanov_Bakalynsky_1.htm.

6. Анализ международного стандарта ISO 15408 : информационная технология, методы и средства // Бизнес и безопасность. – 2007. – № 561.



*Гусейніков Ю.В.,*
*Національна академія Служби безпеки України*


## КІБЕРТЕРОРИЗМ – НОВІТНЯ ЗАГРОЗА НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ

Зростання і глобалізація економіки, насиченість її новими телекомунікаційними технологіями, комп'ютеризація таких життєво важливих сфер діяльності суспільства, як зв'язок, енергетика, транспорт, системи зберігання і транспортування нафти та газу, фінансова й банківська системи, оборона й національна безпека, забезпечення роботи міністерств і відомств, перехід на методи електронного управління технологічними процесами у виробництві спричиня-

ють усе більшого поширення терористичних акцій за допомогою високих технологій. Кібертероризм є серйозною загрозою для країни, де функціонують банківська, транспортна та енергетична системи, а особливо там, де уряд, державний і приватний сектор економіки спираються на інформаційні мережі та швидкий доступ до високих технологій.

Під терміном "кібертеракт" розуміються, як правило, дії щодо дезорганізації інформаційних систем, залякування населення і створення небезпеки загибелі людей, заподіяння значної майнової шкоди чи настання інших тяжких наслідків, з метою впливу на прийняття рішення органами влади або міжнародними організаціями, а також погроза вчинення зазначених дій з тією ж метою.

Кібертеракт – це серйозна загроза людству, порівнянна з ядерною, бактеріологічною і хімічною зброєю. Ступінь цієї загрози в силу своєї новизни не до кінця усвідомлена й належно вивчена. Кібертеракт не має державних кордонів, кібертерорист здатен однаково загрожувати інформаційним системам, розташованим у будь-якій точці земної кулі. Виявити і нейтралізувати віртуального терориста вельми проблематично через надто малу кількість залишених їм слідів та їх специфіку.

На відміну від звичайного терориста, який для досягнення своїх цілей використовує вибухівку або стрілецьку зброю, кібертерорист вдається до сучасних інформаційних технологій, комп'ютерних систем та мереж, спеціального програмного забезпечення, призначеного для несанкціонованого проникнення в комп'ютерні системи й організації віддаленої атаки на інформаційні ресурси жертви.

Важко не погодитися з позицією В.М.Бутузова щодо основних причин і чинників розвитку злочинності у сфері високих інформаційних технологій, до яких він відніс:

- низьку спроможність держав здійснювати ефективний контроль над національним сегментом інформаційного простору через: ще не сформовану правову базу, як національну, так і міжнародну, розвиток якої відстає від інформаційно-технологічних зрушень; необхідність у значних фінансових, технологічних та кадрових ресурсах;

- злочинність у сфері високих інформаційних технологій має не тільки організований характер, а ще й транснаціональний;

- відсутність достатньої судової практики у кримінальних справах вказаної категорії;

- корупцію;

- політичну, економічну та соціальну нестабільність у суспільстві тощо.

Для України питання забезпечення кібернетичної безпеки суттєво актуалізується з розвитком й поширенням систем “електронного урядування”, “електронного банкінгу”, “електронної комерції”, “електронної медицини”, “електронної освіти” тощо, які роблять інформаційно-телекомунікаційні системи урядового, оборонного, виробничого, кредитно-фінансового, комунального та інших секторів уразливими для деструктивного впливу з кіберпростору.

За останні роки у нас зросла кількість кіберзлочинів. У цьому питанні Україна втрачає ще й свою міжнародну репутацію, оскільки її кіберпростір часто використовується злочинцями для атак на мережі інших країн. Прикладом може слугувати арешт співробітниками СБ України восени 2011 року п’ятьох кіберзлочинців, які входили до міжнародної злочинної групи, що атакувала закордонні фінансові установи.

Заслуговують на пильну увагу і події 2012 року, які розгорнулися в Україні навколо закриття сайту www.ex.ua, коли в результаті невдоволення зазначеними діями, хакери атакували сайти органів державної влади, що призвело до дестабілізації їх роботи. І хоча це був своєрідний протест, немає гарантії, що в майбутньому подібне не буде здійснено з терористичною метою.

Отже, з огляду на масштабність і динамічність проникнення інформаційно-телекомунікаційних технологій у всі сфери життєдіяльності особи, суспільства та держави в процесі інтеграції нашої країни до глобальної інформаційної цивілізації, проблема забезпечення її кібернетичної безпеки як невід’ємної складової кожної зі сфер національної безпеки, управління процесами в яких пов’язане із застосуванням указаних технологій, потребує негайного й ефективного розв’язання, що неможливо здійснити без відповідних законодавчих новацій. Першочерговими вбачаються такі кроки:

1. Відповідно до Рішення Ради національної безпеки і оборони України від 25 травня 2012 року “Про заходи щодо посилення боротьби з тероризмом в Україні” розробити проект Закону України “Про кібернетичну безпеку України”;

2. Внести відповідні зміни до законів України “Про основи національної безпеки України”, “Про оборону України”, “Про боротьбу з тероризмом”, “Про засади внутрішньої і зовнішньої політики”, “Про об’єкти підвищеної небезпеки”, Кримінального кодексу України.

## ЛІТЕРАТУРА

1. Про Рішення Ради національної безпеки і оборони України від 25 травня 2012 року “Про заходи щодо посилення боротьби з тероризмом в Україні” : Указ Президента України від 8 червня

2012 року № 388/2012 / [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/388/2012.

2. Науково-практичний коментар Розділу XVI КК України “Злочини у сфері використання електронно-обчислюваних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку”/ за ред. В.С.Картавцева. – К. : Вид-во НА СБ України, 2005. – 102 с.

3. Організаційно-правові та тактичні основи протидії злочинності у сфері високих інформаційних технологій : навч. посіб. / за ред. Б.В.Романюка; Є.Д.Скулиша. – К., 2011. – С. 95–96.

*Дмитренко Е.С.,*
*доктор юридичних наук, професор,*
*Національна академія Служби безпеки України*

## АКТУАЛЬНІ ПИТАННЯ ЗАХИСТУ ПОДАТКОВОЇ ІНФОРМАЦІЇ

Однією з ознак правової держави та свідченням формування громадянського суспільства є функціонування досконалого механізму захисту інформації, зокрема податкової, яка сприяє реалізації покладених на Міністерство доходів і зборів України (Міндоходів України) завдань і функцій та забезпеченню інформаційної безпеки у сфері оподаткування.

Незважаючи на важливість механізму захисту інформації, це питання, як свідчать джерела [1, 2], окремо науковцями не розглядалося. Його дослідження також актуалізується у зв’язку з прийняттям відповідних норм у Податковому кодексі України (ПК України) [3], які не є досконалими, отже, потребують ретельного вивчення.

Поняття “податкова інформація” вживається у ПК України у такому ж значенні, як у ст. 16 Закону України “Про інформацію” від 02.10. 1992 р., тобто як сукупність відомостей і даних, що створені або отримані суб’єктами інформаційних відносин у процесі поточної діяльності й необхідні для реалізації покладених на контролюючі органи завдань і функцій [4, ст. 16]. Щодо поняття “право на податкову інформацію”, то шляхом аналізу відповідних джерел визначимо його як можливість вільного одержання, використання, поширення, зберігання і захисту інформації, необхідної для реалізації прав, свобод і законних інтересів [2, с. 12; 4, статті 5–6] суб’єктів інформаційних відносин у сфері оподаткування. Зазначене поняття тісно пов’язане з іншим – “режимом доступу до податкової інформації”, – за яким таку інформацію поділяють на відкриту та інфор-

мацію з обмеженим доступом – конфіденційну, таємну, службову [4, статті 20–21].

Оскільки питання захисту податкової інформації пов'язані з механізмом реалізації права на податкову інформацію, то у ст. 21 ПК України закріплено обов'язки контролюючих органів не допускати розголошення інформації з обмеженим доступом, що одержується, використовується, зберігається під час реалізації функцій, покладених на контролюючі органи, а також надавати органам державної влади та органам місцевого самоврядування на їх письмовий запит відкриту податкову інформацію в порядку, встановленому законом. Інакше за невиконання (неналежне виконання) цих обов'язків посадові особи Міндоходів України можуть нести відповідальність згідно із законом.

Іншою нормою – ст. 63 ПК України – передбачено, що інформація, яка збирається, використовується та формується у зв'язку з обліком платників податків, вноситься до інформаційних баз даних (комп'ютерних і телекомунікаційних мереж, мереж та каналів передачі даних тощо) й використовується з урахуванням обмежень, передбачених для податкової інформації з обмеженим доступом.

Реалізація права на податкову інформацію передбачає певний зв'язок між реальною доступністю податкової інформації та режимом доступу до неї й поділ інформації за ступенем доступності на доступну і недоступну для певного суб'єкта. Доступність інформації зумовлена не лише її юридичним статусом, а й фактичними умовами використання для різних суб'єктів [1, с. 52] та умовами надання (платно чи безоплатно). Окрім того, реалізація права на податкову інформацію усіма суб'єктами інформаційних відносин, безперечно, є ефективним засобом дотримання законності у сфері оподаткування.

З урахуванням зазначеного, у законодавстві мають бути чітко визначені усі випадки, коли орган Міндоходів України має право вимагати та отримувати від платника або інших суб'єктів податкову інформацію, а платник податків та інші суб'єкти інформаційних відносин у сфері оподаткування зобов'язані її надати.

Новелою та позитивною стороною ПК України є, безперечно, наявність у п. 73.3 ст. 73 норми про реалізацію права органів Міндоходів України на звернення до платників податків із письмовим запитом про надання податкової інформації, необхідної для виконання покладених на ці органи функцій і завдань.

Однак у результаті ретельного аналізу інших норм ПК України, зокрема пп. 20.1.2, 20.1.6, 20.1.8 ст. 20, статей 77-80, 83, 85, які стосуються механізму проведення податкових перевірок, було виявле-

но колізію між ними та нормою ст. 73 ПК України. Сутність колізії полягає в тому, що відповідно до змісту зазначених норм територіальний орган Міндоходів України має право для здійснення передбачених податковим законодавством функцій отримувати безоплатно від платників, у порядку, визначеному ПК України, значно більший обсяг податкової інформації й не за письмовим запитом. Йдеться про інформацію, довідки, копії документів, засвідчені підписом платника податків (його посадовою особою) та скріплені печаткою (за наявності), про фінансово-господарську діяльність, отримувані доходи, видатки платників податків та іншу інформацію, пов'язану з обчисленням та сплатою податків, дотриманням вимог іншого законодавства, а також фінансову й статистичну звітність, у порядку та на підставах, визначених ПК України [8, п.п. 20.1.2, 20.1.6, 20.1.8 ст. 20]; матеріали, які можуть бути підставою для висновків під час проведення документальної планової, документальної позапланової, документальної невиїзної, фактичної перевірок [3, статті 77-80]; додаткову інформацію [3, ст. 80**]**.

Уважаємо, що з метою реалізації права платників податків, інших суб'єктів інформаційних відносин на податкову інформацію зміст цих та інших норм щодо податкової інформації слід узгодити таким чином, щоб інформацію орган Міндоходів України отримував від інших суб'єктів інформаційних відносин за процедурою, визначеною у ст. 73 ПК України.

Іншою проблемою є наявність колізії між п. 73.3 ст. 73 і п.п. 78.1.1, 78.1.4, 78.1.9 ст. 78 ПК України щодо термінів надання інформації на запит органу Міндоходів України, який становить місяць із дня, що настає за днем надходження запиту (п. 73.3), а у випадках, передбачених у п.п. 78.1.1, 78.1.4, 78.1.9, – 10 днів. Оскільки останній термін, на нашу думку, є коротким і може бути недотриманим, що спричинить обов'язкове проведення документальної позапланової виїзної перевірки, вважаємо доцільним застосувати в усіх випадках єдиний термін надання інформації на запит органу Міндоходів України – місяць з дня, що настає за днем надходження запиту.

Таким чином, чітке визначення у законодавстві повноважень суб'єктів інформаційних відносин у сфері оподаткування сприятиме функціонуванню ефективного механізму захисту податкової інформації, а отже, забезпеченню інформаційної безпеки у цій сфері.

## ЛІТЕРАТУРА

1. Соснін О.В. Проблеми державного управління системою національних інформаційних ресурсів з наукового потенціалу України

/ О.В.Соснін. – К. : Ін-т держави і права ім. В.М.Корецького НАН України, 2003. – 572 с.

2. Марущак А.І., Концептуальний підхід до забезпечення доступу до інформації в Україні / А.І.Марущак, Є.Д.Скулиш // Інформаційна безпека людини, суспільства, держави. – 2012. – № 1(8). – С. 11–17.

3. Податковий кодекс України від 02.12.2010 р. № 2755-VI // Відомості Верховної Ради України. – 2011. – № 13–17. – Ст. 112.

4. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650.

*Драчук С.М.,*
*кандидат юридичних наук,*
*Національна академія Служби безпеки України*

## ПРОБЛЕМИ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОГО РИНКУ УКРАЇНИ В КОНТЕКСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Забезпечення будь-якого виду безпеки у сучасному світі неможливо уявити без належного правового регулювання відповідних суспільних відносин, у тому числі без унормованого адекватно до наявних потреб категорійно-понятійного апарату.

Сьогодні найкращою гарантією безпеки, наприклад на регіональному рівні (ОБСЄ), залишається бажання та здатність кожної держави-учасниці підтримувати верховенство закону, що цілком виправдано посідає центральне місце в концепції європейської безпеки.

В Україні відповідно до Конституції визнається і діє принцип верховенства права. Його також віднесено до одного з основних принципів забезпечення національної безпеки України, дотичного до інформаційної безпеки.

Обидва принципи, хоча і мають певну різницю в ієрархічній структурі, зводяться, серед іншого, й до необхідності чіткого визначення та єдиного розуміння понять і термінів, що вживаються в інформаційній сфері.

В Україні триває процес формування та розвитку інформаційного ринку, який має кореспондуватися і відповідати певним критеріям інформаційної безпеки, в тому числі правового характеру.

Поняття "*інформаційний ринок*" на законодавчому рівні визначається як система економічних, організаційних і правових відносин

щодо продажу й купівлі *інформаційних ресурсів, технологій, продукції* та *послуг*.

Водночас на законодавчому рівні вживається поняття "*ринок інформаційно-комунікаційних технологій*", який перебуває в стані активного становлення та за умов ефективного забезпечення його безпеки може стати фундаментом розвитку інформаційного суспільства в Україні. Недаремно відповідно до одної із стратегічних цілей розвитку інформаційного суспільства в Україні віднесено покращення стану інформаційної безпеки в умовах використання новітніх інформаційно-комунікаційних технологій.

В подальшому, виходячи з проблематики нашої конференції, ми пропонуємо акцентувати увагу саме на правових відносинах.

Перш за все звертаємо Вашу увагу на відсутність у наведеному визначенні поняття "*інформаційний ринок*" можливості *обміну* інформаційними ресурсами, технологіями, продукцією. Теорія ринку та практика побудови ринкової економіки обов'язково поруч із продажем і купівлею оперує цим поняттям (обмін).

Наступним ключовим поняттям інформаційного ринку є "*інформаційний ресурс*".

На законодавчому рівні поняття "*інформаційний ресурс*" визначається як сукупність документів у інформаційних системах (бібліотеках, архівах, банках даних тощо). В більшості підзаконних нормативно-правових актів ця правова конструкція збереглася. Виняток становить лише позиція Міністерства фінансів України, яка полягає у трактуванні поняття "*інформаційний ресурс*" як інформації, що циркулює в електронній формі у телекомунікаційній мережі Мінфіну. Також цікавою є практика визначення цього поняття у міжурядових угодах України про співробітництво в галузі технічного захисту інформації, зокрема з РФ, у якій до поняття "*інформаційні ресурси*" поруч із групами документів включені також окремі документи.

Поняття "*інформаційна продукція*" в національному законодавстві визначається у двох законодавчих актах як матеріалізований результат інформаційної діяльності, призначений для задоволення потреб суб'єктів інформаційних відносин (Закон України "Про інформацію") та документована інформація, яка підготовлена й призначена для задоволення потреб користувачів (Закон України "Про Національну програму інформатизації"). Цікаво, що Закон України "Про захист прав споживачів" оперує поняттям "безпека продукції".

Водночас на підзаконному рівні під "*інформаційним продуктом*" розуміються цифрові дані, призначені для задоволення інформаційних потреб користувача, у тому числі програмний продукт.

Щодо поняття "*інформаційна технологія*" відмічається чітке його визначення та застосування як на законодавчому, так і на під-

законному рівнях. Воно, зокрема, визначається як цілеспрямована організована сукупність інформаційних процесів із використанням засобів обчислювальної техніки, що забезпечують високу швидкість оброблення даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування.

Під поняттям "інформаційна послуга" у вітчизняній правовій системі, на законодавчому рівні, розуміється діяльність із надання інформаційної продукції споживачам із метою задоволення їхніх потреб.

На підзаконному рівні унормовано поняття "*інформаційні послуги загального призначення*" як, інформаційні послуги, надання яких не потребує ідентифікації суб'єктів правових відносин.

Хоча інформаційна продукція та інформаційні послуги є об'єктами цивільно-правових відносин, що регулюються цивільним законодавством України в контексті формування в Україні інформаційного ринку, варто нагадати, що держава здійснює контроль і нагляд за господарською діяльністю суб'єктів господарювання у такій сфері, як споживання (за якістю і безпечністю інформаційної продукції та послуг). Крім того, споживачі, які перебувають на території України, під час придбання, замовлення або використання інформаційних послуг із метою задоволення своїх потреб мають право на безпеку інформаційних послуг.

Безпека інформаційних послуг поруч із безпекою інформаційної продукції має посідати одне з ключових місць у структурі забезпечення інформаційної безпеки України, яку недаремно віднесено Основним законом України до одної з найважливіших функцій держави, справи всього українського народу.

Законом України "Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки" передбачено, що вирішення проблем інформаційної безпеки має здійснюватися шляхом удосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, а також правоохоронної діяльності в інформаційній сфері.

Враховуючи викладене вище, пропонуємо:

- розробити та закріпити в Законі України "Про захист прав споживачів" поняття "безпека послуги";

- на законодавчому рівні, з метою забезпечення національної безпеки, оборони чи інших загальносуспільних інтересів слід установити винятки з правила щодо заборони СБ України та її посадовим особам ухвалювати акти та вчиняти дії, які запроваджують обмеження на інформаційному ринку, не передбачене законодавством;

- розглянути питання щодо впровадження законодавчого обмеження діяльності іноземних інвесторів та підприємств з іноземними інвестиціями на інформаційному ринку, виходячи з інтересів національної безпеки України. Для цього на законодавчому рівні визначити інформаційний ринок як таку галузь господарювання, в якій установлюється загальний розмір участі іноземного інвестора, виходячи з вимог забезпечення національної безпеки.

## ЛІТЕРАТУРА


1. Хартія Європейської безпеки // Міжнародний документ, ОБСЄ/19.11.1999 року.
2. Закон України "Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки" № 537–V // Відомості Верховної Ради України. – 2007. – № 12. –Ст. 102.
3. Закон України "Про науково-технічну інформацію" № 3322-XII // Відомості Верховної Ради України. – 1993. – № 33 від 17.08.1993 р.
4. Закон України "Про Національну програму інформатизації" № 74/98-ВР // Відомості Верховної Ради України. – 1998. – № 27–28 від 17.07.1998 р.
5. Закон України "Про інформацію" № 2657–XII // Відомості Верховної Ради України. – 1992. – № 48 від 01.12.1992 р.
6. Господарський кодекс України № 436-IV // Відомості Верховної Ради України. – 2003. – № 18 від 02.05.2003 р.
7. Словник термінів з кібербезпеки / за заг. ред. О.В.Копана, Є.Д.Скулиша. – К. : ВБ "Аванпост-Прим", 2012. – 214 с.



*Захаров О.В.,*
*Національна академія Служби безпеки України*


## ПРАВОВЕ РЕГУЛЮВАННЯ ОБМЕЖЕННЯ ДОСТУПУ ДО ПУБЛІЧНОЇ ІНФОРМАЦІЇ У СФЕРІ ЗЕМЛЕУСТРОЮ І МІСТОБУДУВАННЯ

Стаття 10 Європейської конвенції про захист прав і основоположних свобод (далі – Конвенція) [1] проголошує: кожен має право на свободу вираження поглядів. Це право включає *свободу дотримуватися своїх поглядів, одержувати і передавати інформацію та ідеї без втручання органів державної влади і незалежно від кордонів.*

Конвенція виходить із того, що свобода вираження поглядів як загальний об'єкт правової охорони ст. 10 Конвенції може реалізовуватись у три способи, які згадуються незалежно один від одного. Свобода дій особи стосовно поглядів пов'язана в Конвенції з терміном "дотримуватись", а "інформації та ідеї" – термінами "одержувати" і "передавати". Термінологічний аналіз ст. 10 Конвенції дає підстави уважати, що вчинення дій власне інформаційного характеру – дій із передачі й одержання даних – уважається охоронюваною свободою тільки стосовно інформації та ідей. Якщо ж ітиметься про погляди, то Конвенція гарантує свободу їх дотримування.

Ця свобода не може бути ототожненою із правом поширити чи отримати дані. Ми схиляємось до думки, що дотримання поглядів як свобода особи полягає у використанні отриманих даних або споживанні ефектів від поширення даних (ефектів політичного, фінансово-економічного, особистого характеру). При цьому такі дії особи є в інформаційному плані "мовчазними", не пов'язаними з обміном даними, отже, можуть бути віддаленими від актів отримання й поширення інформації та ідей у просторі, в часі, а також мати різне коло осіб.

З іншого боку, свобода вираження своїх поглядів, з огляду на зміст ст. 10, не може зводитись тільки до свободи поширення інформації. Адже, окрім поширення інформації та ідей, свобода вираження поглядів може реалізовуватись ще в такі способи, як одержання інформації й додержання власних поглядів. Отже, свобода вираження поглядів не може зводитись до актів обміну інформацією.

Цю особливість свободи дотримуватись поглядів слід ураховувати під час визначення меж дії ст. 10 Конвенції. Адже в низці випадків може здаватись, що певна поведінка особи чи її права на певну річ не охороняються гарантіями ст. 10 Конвенції, зокрема через віддаленість такої поведінки чи речі від актів отримання й поширення інформації та ідей у просторі й часі.

Наприклад, дотримання поглядів особою може здійснюватись не тільки в таких економічно нейтральних формах, як вибір (зміна) особою свого імені або зовнішнього вигляду, але і в таких економічно й суспільно значущих формах, як створення об'єктів містобудування чи благоустрою; запровадження певної структури і прийомів управління організацією; вчинення правочинів щодо майна на підставі отриманих офіційних даних про нього з державних реєстрів; створення об'єктів інтелектуальної власності та інше. Не дивлячись на те, що перераховані дії не можуть уважатись поширенням чи отриманням інформації та ідей, вони мають ознаки об'єкта охорони ст. 10 Конвенції саме як результати дотримання поглядів певної особи.

Наведені міркування дають можливість визначити відмінність між поглядами й інформацією та ідеями як об'єктами свобод особи: погляди особи включають не тільки інформацію та ідеї, але й те, в чому інформація та ідеї можуть втілюватись, (насамперед, продукти праці та виробництва, поведінка (дії) особи). Тому ст. 10 Конвенції охороняється не тільки свобода щодо думок та висловлювань, але і щодо предметів матеріального світу, що мають матеріальну цінність. У зв'язку з таким тлумаченням виникає практична необхідність співвідношення свободи вираження поглядів із правом мирно володіти власністю.

Не можна не помітити, що свобода вираження поглядів передбачена також ст. 34 Конституції України [2]. Однак, на відміну від ст. 10 Конвенції, наша Конституція не містить указівку на способи її реалізації, такі як дотримання поглядів, отримання і передавання інформації та ідеї. З огляду на це викладені вище висновки мають застосовуватись і до випадків реалізації ст. 34 Конституції. На жаль, вітчизняна конституційна практика зводить передбачене ч. 1 ст. 34 Конституції право до виключно актів інформаційної взаємодії.

Поширюючи ці положення на способи вираження поглядів, відмінні від одержання і поширення інформації, зокрема на дотримання своїх поглядів під час створення матеріальних об'єктів, слід стверджувати про закріплення у ст. 10 Конвенції права особи вимагати від держави та органів місцевого самоврядування не втручатись у виробничу чи професійну діяльність такої особи з огляду на ідеологічні, релігійні, естетичні й культурні мотиви.

Так, відповідно до Закону України "Про архітектурну діяльність" [3] проект – документація для будівництва об'єктів архітектури, що складається з креслень, графічних і текстових матеріалів, інженерних і кошторисних розрахунків, які визначають містобудівні, об'ємно-планувальні, архітектурні, конструктивні, технічні та технологічні рішення, вартісні показники конкретного об'єкта архітектури, та відповідає вимогам державних стандартів, будівельних норм і правил. Архітектурне рішення – авторський задум щодо просторової, планувальної, функціональної організації, зовнішнього вигляду й інтер'єру об'єкта архітектури, а також інженерного та іншого забезпечення його реалізації, викладений в архітектурній частині проекту на всіх стадіях проектування і зафіксований у будь-якій формі.

Виходячи з викладеного, проектування об'єктів містобудування цілком охоплюється поняттям вираження своїх поглядів, які охороняються ст. 10 Конвенції. Відповідно до цього обмежити таке право можливо тільки у випадках, передбачених ч. 2 ст. 10 Конвенції, тобто в інтересах національної безпеки, територіальної цілісності або

громадської безпеки, для охорони порядку чи запобігання злочинам, для охорони здоров'я або моралі, захисту репутації або прав інших осіб, запобігання розголошенню конфіденційної інформації чи для підтримання авторитету й безсторонності суду, і необхідно в демократичному суспільстві.

Тому, наприклад, обмеження архітекторів і забудовників державними санітарними нормами відповідає цим цілям, а обмеження, встановлені передбаченими ст. 18 Закону України "Про регулювання містобудівної діяльності" планами зонування територій населеного пункту[1], – ні. Так, чинне колись обмеження на забудову присадибних ділянок будинками, які мають більш ніж один поверх, мало б розглядатись як порушення ст. 10 Конвенції та , відповідно, ст. 34 ч. 1 Конституції (якщо ми уявно застосуємо ці норми до тих часів). Не відповідає ст. 10 Конвенції право органів містобудування й архітектури, передбачене ст. 29 ч. 6 Закону України "Про регулювання містобудівної діяльності" [4], включати до складу вихідних даних на будівництво вимоги до архітектурних та інженерних рішень.

Іншою проблемою є забезпечення права на вільне виявлення архітектором і забудовником своїх поглядів у частині отримання даних містобудівної документації для підготовки передпроектних пропозицій або намірів забудови земельної ділянки. Мова йде про отримання даних (зокрема в графічній формі) про плани червоних ліній, згаданий вище план зонування, дані геологічних вишукувань, дані про наявні або заплановані лінії комунікацій та інше. Отримання цих даних і врахування їх при проектуванні є необхідним, оскільки орган містобудування та архітектури має право відмовити у наданні вихідних даних на будівництво, якщо наміри забудови не відповідають містобудівній документації, на підставі ч. 4 ст. 29 Закону України "Про регулювання містобудівної діяльності". Аналогічним чином стоїть питання про отримання цих даних підчас здійснення замовниками будівництва або власниками земельних ділянок землевпорядного проектування, рішення якого (в частині меж земельних ділянок, віднесення їх до певного виду цільового призначення) так само має відповідати містобудівній документації (ст. 24 Закону). Надання цих даних є оплатним, а строк виконання відповід-

[1] Відповідно до Закону України "Про регулювання містобудівної діяльності" план зонування території розробляється на основі генерального плану населеного пункту (у його складі або як окремий документ) з метою визначення умов та обмежень використання території для містобудівних потреб у межах визначених зон.

них документів перевищує встановлений в Законі України “Про доступ до публічної інформації” [5] двадцяти денний термін.

## ЛІТЕРАТУРА

1. Конвенція про захист прав і основоположних свобод // Офіційний вісник України. – 2006. – № 32. – Ст. 2371.

2. Конституція України // Відомості Верховної Ради України. – 1996. – № 30. – Ст. 141.

3. Закон України “Про архітектурну діяльність” // Відомості Верховної Ради України. – 1999. – № 31. – Ст. 246.

4. Закон України “Про регулювання містобудівної діяльності” // Офіційний вісник України. – 2011. – № 18. – Ст. 735.

5. Закон України “Про доступ до публічної інформації” // Голос України. – 2011. – № 24.

*Єрьоміна Л.В.,*
*Національна академія Служби безпеки України*

## НАПРЯМИ УДОСКОНАЛЕННЯ ЗАКОНОДАВСТВА УКРАЇНИ У СФЕРІ КІБЕРБЕЗПЕКИ: ТЕРМІНОЛОГІЧНИЙ АСПЕКТ

У Стратегії національної безпеки України “Україна у світі, що змінюється” від 8 червня 2012 р. підкреслюється той факт, що “…на тлі зростання викликів і посилення загроз національній безпеці зберігається невідповідність сектору безпеки і оборони України завданням захисту національних інтересів, що характеризується … нездатністю України протистояти новітнім викликам національній безпеці (явищам і тенденціям, що можуть за певних умов перетворитися на загрози національним інтересам), пов’язаним із застосуванням інформаційних технологій в умовах глобалізації, насамперед кіберзагрозам”.

У контексті удосконалення нормативно-правової бази протидії тероризму Президентом України поставлено завдання в найкоротші терміни розробити і внести в установленому порядку на розгляд Верховної Ради України проект Закону України ,“Про кібернетичну безпеку України”.

Вказане є ще одним свідченням невідповідності сучасного законодавства, спрямованого на забезпечення кібернетичної безпеки, реаліям сьогодення. В умовах інтенсифікації технічного прогресу в

кіберпросторі та динамічних змін оперативної обстановки у сфері високих технологій можна говорити про суттєве "відставання" відповідної нормативно-правової бази від потреб часу.

Аналіз законодавства України, а також наукових напрацювань фахівців різних відомств, на які покладено завдання забезпечення кібербезпеки, свідчить про фрагментарність понятійного поля вказаної сфери, що унеможливлює формування дієвих нормативно-правових документів із протидії кіберзагрозам. При цьому подекуди законодавець оперує термінами в кіберсфері, юридичних визначень яких фактично не має. Це стосується і таких основоположних термінів, як "кіберпростір" та "кіберзагроза".

Проведене дослідження дає підстави визначити поняття "кіберзагроза" як обумовлену вразливість інформаційно-телекомунікаційної системи країни, можливість виникнення негативних наслідків для інтересів суспільства, держави та особи в результаті здійсненого в кіберпросторі впливу на вказану систему.

Під кіберпростором у цьому визначенні розуміємо інформаційне середовище (простір), яке створене та функціонує за допомогою технічних (насамперед, комп'ютерних) систем, при взаємодії людей між собою та взаємодії цих систем) при управлінні ними людьми.

З огляду на сформульоване визначення поняття "кіберзагроза" під "*видами кіберзагроз* слід розуміти класифіковану сукупність конкретних способів виникнення негативних наслідків для інтересів суспільства, держави та особи в результаті здійсненого в кіберпросторі впливу на інформаційно-телекомунікаційну систему.

Зокрема, серед найбільш актуальних проявів кіберзагроз можна виділити:

– порушення порядку оброблення і захисту інформації в державних інформаційних ресурсах;

– активне використання спеціальних шкідливих комп'ютерних програм (насамперед, комп'ютерних вірусів).

– несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем та комп'ютерних мереж, у яких обробляються державні електронні інформаційні ресурси;

– несанкціонований збут або розповсюдження інформації з обмеженим доступом, яка зберігається в державних інформаційних ресурсах;

– несанкціоновані дії з інформацією, яка обробляється в державних інформаційних ресурсах, вчинені особами, які мають право доступу до неї.

Таким чином, виходячи від сформульованого поняття "кіберзагроза", можливо у найзагальнішому вигляді, не претендуючи на ви-

черпність, визначити сам термін ,“кібербезпека” як стан захищеності інтересів особи, суспільств та держави від кіберзагроз.

Запропоновані терміни пропонуємо інтегрувати не тільки у проект Закону України “Про кібернетичну безпеку України”, але й у “Стратегію кібернетичної безпеки України”, що дозволило б фактично завершити формування основних концептуальних документів у сфері організаційно-правових засад забезпечення кібербезпеки.

*Касперський І.П.,*
*кандидат юридичних наук,*
*старший науковий співробітник,*
*Національна академія Служби безпеки України*

## КРИТЕРІЇ КЛАСИФІКАЦІЇ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ У ЗАКОНОДАВСТВІ УКРАЇНИ

Захист інформаційних ресурсів від протиправних посягань та незаконного використання на сьогодні є чи не найважливішим завданням на шляху розвитку новітнього інформаційного суспільства, у якому інформація позиціонується як ціннісний ресурс функціонування усіх суспільних сфер.

Першочерговим завданням законодавця у цьому напрямі є встановлення та належне закріплення класифікації інформації з обмеженим доступом, яка б дозволила відносити конкретну інформацію до певного виду, щодо якого і встановлюється власна система захисту. Належна класифікація забезпечує можливість досягнення відповідності засобів захисту інформації розміру тієї шкоди, яку буде завдано інтересам особи, суспільства, держави внаслідок розголошення кожного з видів інформації з обмеженим доступом. Дисбаланс у цій сфері призводить не тільки до надмірних затрат щодо перебільшеного захисту інформаційних ресурсів, а й до невиправданих обмежень прав суб’єктів інформаційної діяльності на отримання доступу до інформації, та до економічних та іміджевих утрат унаслідок надзвичайної “закритості” діяльності окремого суб’єкта.

На жаль, на сьогодні є всі підстави уважати, що законодавством не повністю виконано завдання щодо класифікації інформації з обмеженим доступом. Для ілюстрації суті проблеми звернемось до змісту чинного регулювання у цій сфері.

Законодавцем у Законі України “Про інформацію” інформацію з обмеженим доступом поділено на конфіденційну, таємну і служ-

бову [1]. Критерій розподілу інформації на таємну і конфіденційну полягає у рівні диспозитивності в обмеженні доступу до неї: доступ до таємної обмежується обов'язково відповідно до закону, а режим обігу конфіденційної визначають її власники (крім суб'єктів владних повноважень) на власний розсуд [2]. Проте, виходячи зі змісту законодавчих визначень комерційної таємниці, можливо дійти висновку, що вона повністю входять до обсягу даного законодавцем визначення конфіденційної інформації, бо Господарським кодексом установлено, що "склад і обсяг відомостей, що становлять комерційну таємницю, спосіб їх захисту визначаються суб'єктом господарювання відповідно до закону" [3]. Такі властивості комерційної таємниці цілком виправдано спонукають науковців висувати пропозиції щодо її віднесення до конфіденційної інформації [4]. Та й сам законодавець у Кримінально-процесуальному кодексі до охоронюваної законом таємниці відніс "конфіденційну інформацію, в тому числі таку, що містить комерційну таємницю" [5]. Подібні суперечності мають непоодинокий характер: законодавець називає таємницю страхування конфіденційною інформацією щодо діяльності та фінансового стану страхувальника…" [6].

Відсутність чітких критеріїв видового поділу інформації з обмеженим доступом викликає непорозуміння у складі тих суб'єктів, які зобов'язані забезпечувати охорону даних, змісті тих режимів захисту, які вони зобов'язані застосовувати, та вносить дисбаланс у рівні такого захисту.

Вирішення названої проблеми вимагає перегляду сьогоднішньої класифікації інформації з обмеженим доступом у контексті уніфікації режимів захисту однакових за статусом видів "закритих" даних.

Виходячи зі змісту чинного законодавства, можливо виділити ознаки, за якими наразі класифікується інформація з обмеженим доступом:

– вид суб'єктів, на які покладено обов'язок щодо охорони певного виду інформації з обмеженим доступом у зв'язку з наявністю у них прав володіння, використання, розпорядження цими даними (держава, банк, лікар, адвокат тощо);

– процеси діяльності людини, суспільства чи держави, під час яких відбувається обіг такої інформації (усиновлення, страхування, поштовий чи телефонний зв'язок);

– об'єкт, якому буде завдано шкоду у випадку розголошення інформації з обмеженим доступом (національна безпека, інтереси клієнта банку).

Застосування такого різнопланового переліку критеріїв призвело до невизначеності статусу інформації з обмеженим доступом у

процесі її обігу в різних видах правовідносин. Подолати проблему множинності різних за змістом режимів захисту інформації, створити єдине правове поле із єдиними вимогами щодо методів і засобів забезпечення захисту даних, що підлягають охороні, можливо шляхом об'єднання в межах окремих класів різних видів інформації з обмеженим доступом.

На основі викладеного пропонуємо внести зміни до класифікації інформації з обмеженим доступом в Україні, поклавши в її основу форму власності на інформацію. Вибір цього стрижневого критерію зумовлений тією обставиною, що будь-який суб'єкт отримує можливість захищати інформацію за однієї умови – він повинен бути як мінімум її володільцем, а це компонент права власності, без наявності якого висувати до відповідного суб'єкта вимоги щодо захисту абсолютно безпідставно.

Ми також наполягаємо на тому, що правова регламентація інформації з обмеженим доступом повинна забезпечити дворівневу систему класифікації. Це дозволить забезпечити уніфікацію систем захисту окремих видів інформації, яка на сьогодні захищається у різних правових режимах. Тобто варто вести мову про розподіл інформації з обмеженим доступом на класи та види в межах класу.

У цьому контексті уважаємо цілком доцільним підтримати пропозицію авторів законопроекту "Про державні секрети" [7] щодо об'єднання в одному класі "державні секрети" державної таємниці та службової інформації (колишньої конфіденційної інформації, що є власністю держави) як взаємопов'язаних видів з єдиним суб'єктом захисту, перевівши службову інформацію у статус службової таємниці. На нашу думку, використання для класифікації державної інформації з обмеженим доступом назви "службова таємниця" убачається більш вдалим, ніж "службова інформація", оскільки останній термін не містить жодних ознак того, що це інформація з обмеженим доступом, а загальні ознаки службової інформації дозволяють розглядати її як певний вид саме таємних даних, застосування захисту щодо яких є обов'язковим.

Також цілком слушною в цьому аспекті є пропозиція Г.Виноградової щодо віднесення до професійної таємниці таких видів інформації з обмеженим доступом: лікарська таємниця, професійна таємниця суддів, адвокатська таємниця, таємниця вчинення нотаріальних дій (нотаріальна таємниця), аудиторська таємниця, таємниця усиновлення [8]. Необхідність такого об'єднання полягає у підтвердженні суттєвої спільної ознаки перерахованих видів таємної інформації: ці дані, потрапляючи у володіння різних суб'єктів (банк, адвокат, лікар, нотаріус), стосуються інших фізичних та юридичних

осіб (клієнтів, пацієнтів), яким передусім буде завдано шкоду внаслідок її розголошення.

Проте класифікаційне об'єднання видів таємної інформації повинно термінологічно відрізнятися від самого видового ряду і в цьому випадку замість терміна таємниця, на нашу думку, варто використати більш збірне поняття "секрети". Саме тому ми висуваємо пропозицію щодо об'єднання усіх видів таємної інформації (крім державної таємниці) в одному класі – *професійні секрети*, під яким пропонуємо розуміти клас інформації з обмеженим доступом, що об'єднує види таємної інформації, яка надходить у володіння та користування суб'єктів інформаційної діяльності у зв'язку з виконанням ними своїх функцій і підлягає захисту від неправомірного витоку з боку цих суб'єктів через можливість завдання шкоди внаслідок розголошення цієї інформації правам і законним інтересам її власників. Важливість цього об'єднання зумовлена необхідністю встановлення належного рівного ставлення усіх уповноважених суб'єктів до "чужої інформації" включно із встановленням однакової відповідальності за її протиправне розголошення.

Запропонована система класифікації забезпечує чіткий поділ інформації з обмеженим доступом на три класи відповідно до суб'єктного складу власників інформації, інтереси яких захищатимуться шляхом обмеження доступу до інформації: для державних секретів – це державні інтереси, для конфіденційної інформації – приватні, а для професійних секретів – спільні інтереси власників, користувачів і розпорядників цієї інформації.

Для досягнення цілей запропонованої класифікації потрібно забезпечити внесення низки змін до чинного законодавства, якими необхідно вивести інформацію, яка на сьогодні вважається комерційною таємницею, із класу таємної інформації, визнавши її конфіденційною, окремим законом закріпити поняття та однаковий режим захисту усіх видів професійної таємниці, а також передбачити можливість використання статусу конфіденційної інформації лише в режимі збереження її власником, забезпечивши у випадку правомірного переходу цих даних до інших суб'єктів обов'язкове набуття цією інформацією статусу таємної.

## ЛІТЕРАТУРА

1. Закон України "Про інформацію" від 13.01.2011 р. // Офіційний вісник України. – 2011. – № 10. – Ст. 445.

2. Закон України "Про доступ до публічної інформації" // Голос України. – 2011. – № 24.

3. Господарський кодекс України // Офіційний вісник України. – 2003. – № 11. – Ст. 462.

4. Сляднєва Г.О. Право суб'єкта господарювання на комерційну таємницю та його захист : автореф. дис. на зд. наук. ступ. канд. юр. наук : 12.00.04. / Г.О.Сляднєва. – Донецьк, 2005. – С .7

5. Кримінально-процесуальний кодекс України // Відомості Верховної Ради України. – 2013. – № 11–12. – Ст. 88.

6. Закон України "Про страхування" // Відомості Верховної Ради України. – 1996. – № 18. – Ст. 78.

7. Проект Закону України "Про державні секрети" [Електронний ресурс]. – Режим доступу : ttp://ssu.gov.ua/sbu/control/uk/publish/article;jsessionid=3581DAD591FB53EE22E9011877B4ADC2?art_id=72055&cat_id=8054.

8. Виноградова Г. Професійна таємниця в міжнародно-правових джерелах: окремі питання регулювання та використання досвіду в законодавстві України / Г.Виноградова // Юридичний журнал. – 2006. – № 4.

*Климчук О.О.,*
*кандидат юридичних наук, доцент,*
*Національна академія Служби безпеки України*

## ПРАВОВІ ОСНОВИ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ВЕЛИКОЇ БРИТАНІЇ

Кібербезпеці в останні роки відводиться провідне місце серед складових інформаційної безпеки, що пояснюється швидким розвитком інформаційних технологій та можливістю використання їх у злочинних цілях. Однією з найрозвинутіших інформаційно держав, поряд із США, Японією та Німеччиною, на разі є Велика Британія. Тут також спостерігається небезпечна тенденція, пов'язана із збільшенням технічної й технологічної небезпеки від транскордонних проявів кіберзлочинності. Щорічні втрати змушують владу країни активно інвестувати створення та розвиток програм із забезпечення безпеки інформації від кібернетичних посягань. І Великій Британії у цілому вдається досягати стану захищеності від кіберзагроз завдяки низці нормативно-правових актів, які становлять базис такої діяльності.

Велике значення для забезпечення інформаційної безпеки держави мають *"Стратегія національної безпеки" (National Security Strategy)* і *"Доповідь стратегічної оборони і безпеки" (Strategic Defense and Security Review).* Перша була прийнята у жовтні 2010 року під назвою "Сильна Британія в епоху невизначеності". Стратегія зарахувала атаки на британський кіберпростір до загроз

першого порядку, разом із міжнародним тероризмом, широкомасштабними стихійними лихами і воєнними діями між державами. А в доповіді оголосила про старт *"Програми національної кібербезпеки" (National Cyber Security Program)*, на здійснення якої в найближчі чотири роки заплановано виділити 630 млн фунтів стерлінгів.

Основними напрямами державної політики національної безпеки Великої Британії в інформаційній сфері є :

- забезпечення інформаційного суверенітету держави;
- вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури й ресурсів, упровадження новітніх технологій у цій сфері;
- активне залучення засобів масової інформації до боротьби з тероризмом та іншими явищами, які загрожують національній безпеці;
- забезпечення неухильного дотримання прав громадян на свободу слова та доступу до інформації;
- вжиття комплексних заходів щодо захисту національного інформаційного простору й протидії монополізації інформаційної сфери Великої Британії.

Нова *Стратегія кібербезпеки (Cyber Security Strategy)* Великої Британії була опублікована 25 листопада 2011 року та становить рамкову програму дій, направлених на зміцнення національної кібербезпеки, а також підвищення надійності й життєстійкості британського кіберпростору в найближчі чотири роки.

Стратегія підкреслює необхідність співпраці уряду, організацій інформаційного простору, а також міжнародних партнерів і громадськості з метою забезпечення переваг країни у кіберпросторі. Останнє досягається за рахунок:

- зменшення загроз кібернетичних операцій шляхом зниження у мотивацій та можливостей противника;
- зниження уразливості інтересів Великої Британії від операцій у кіберпросторі;
- зменшення впливу атак кібернетичних операцій на інтереси держави.

Ці завдання будуть вирішуватись із використанням можливостей кіберпростору шляхом:

- збирання розвідувальної інформації про суб'єктів загроз;
- сприяння підтримці політики Великої Британії;
- розширення знань та поінформованості громадськості;
- підвищення технічних і людських можливостей.

Однією з головних цілей Стратегії є забезпечення більшої узгодженості в діяльності щодо кібернетичної безпеки. Для вирішення проблем кібернетичної безпеки уряд здійснить:

- створення міжвідомчої програми для виконання пріоритетних напрямів досягнення стратегічної безпеки Великої Британії;
- додаткове фінансування для розвитку інноваційного майбутнього технологій захисту мереж Великої Британії;
- налагодження контакту з широким сектором громадськості, промисловості, цивільних свобод і з міжнародними партнерами;
- започаткування Управління кібернетичної безпеки для забезпечення стратегічного керівництва та узгодженням з урядом, створення Центру операцій кібернетичної безпеки (Cyber Security Operations Centre (CSOC), через який уряд буде активно стежити за "здоров'ям" кібернетичного простору і координувати реагування на інциденти й атаки, а також забезпечувати консультування про ризики для бізнесу та громадськості.

Запропоновані заходи покликані стимулювати подальший розвиток онлайн-бізнесу і зменшити збитки, заподіювані національній економіці кібератаками. На думку авторів *Стратегії кібербезпеки*, запорукою успіху в реалізації цих цілей є посилення взаємодії державного і приватного секторів. Британці планують удосконалювати роботу на таких напрямах, як стимуляція інформаційного обміну між публічними і приватними структурами, розвиток вітчизняної індустрії мережевого захисту, підготовка спеціалізованих кадрів, стандартизація безпечного ведення бізнесу в інтернеті, профілактика кіберзлочинів і освіта населення, підвищення ефективності правової бази.

Особливу увагу планується приділити практичному застосуванню чинних правових норм. Згідно з британськими законами суд має право обмежити рецидивісту доступ до мережі Інтернету або накласти заборону на конкретний вид онлайн-діяльності, проте такі запобіжні заходи непопулярні, а нагляд за дотриманням умов звільнення неналежний. Щоб автоматизувати моніторинг мережевої активності кіберзлочинців, відпущених на свободу з обмеженням в інтернет-правах, запропоновано використовувати спеціальні кібертеги, які спрацьовуватимуть при порушенні чинних обмежень і автоматично оповіщатимуть відповідного контролера.

Пропаганду "кібергігієни" та сповіщення про нові інтенет-загрози планується покласти на урядових і приватних експертів, які зможуть звертатися до аудиторії через соціальні мережі. Щоб допомогти споживачам зорієнтуватися на ринку захисних рішень, у країні пропонується увести галузевий знак якості; британський уряд готовий до переговорів із стандартизації оцінки таких продуктів на національному, європейському і міжнародному рівні.

Для спрощення процедури подачі скарг на правопорушення у Великій Британії запущено портал, створений на базі центру допомоги жертвам шахрайства – *Action Fraud.* Його послугами можуть

скористатися індивідуальні й корпоративні користувачі, які зазнали фінансових збитків у результаті будь-кого кіберінцидента. Боротися з локальними інфекціями британці планують за участю інтернет-провайдерів – шляхом уведення зводу добровільних зобов'язань, галузевих нормативів або перегляду призначених для користувача угод.

Окрім нормативно-правових актів стратегічного рівня, у Великій Британії прийнято низку законів, які зокрема спрямовані на забезпечення кібербезпеки. Першим законом, прийнятим "для забезпечення захисту комп'ютерних матеріалів від несанкціонованого доступу або зміни", був "*Закон про неправомірне використання комп'ютерних технологій" (1990)*. У ньому, було виділено три види злочинів, пов'язаних із неправомірним використанням комп'ютерних технологій.

Відповідно до норм цього закону юрисдикція компетентних органів і судів країни поширюється на будь-яке з перерахованих діянь, при скоєнні якого хоча б один елемент складу злочину мав місце на території держави. Таким чином, за наявності лише діяння чи наслідків злочин уважається вчиненим на території Великої Британії. Це положення є виключно важливим у випадку вчинення злочину з комп'ютера, який знаходиться на території держави, що не встановила подібної відповідальності або тоді, коли кримінально-правові приписи мають матеріальний характер, визнаючи закінченим склад злочину лише за наявності шкідливих наслідків на території країни, де скоєно злочинне діяння.

У *"Законі про поліцію і юстицію"* 2006 року містилися поправки до *"Закону про неправомірне використовування комп'ютерних технологій"* – збільшено санкції та додано новий розділ. У 2007 році прийнято *"Закон про серйозні злочини"*, який було спрямовано на боротьбу із членами організованих злочинних угруповань шляхом застосування цивільними судами ухвал про превентивні заходи проти організованої злочинності. Він дає поліції можливість виявляти й попереджати серйозні злочини, у тому числі пов'язані з використанням комп'ютерних технологій.

Частково питання забезпечення кібербезпеки регулюються іншими нормативно-правовими актами. Зокрема, низка норм *"Закону про телекомунікації"* направлена на захист й охорону мереж зв'язку, комп'ютерних систем і мереж. "*Закон про захист даних*" Великої Британії визначає право на оброблення даних, регулює захист особистих даних та дає можливість особі контролювати інформацію про себе.

Таким чином, можна зробити висновок, що у Великій Британії існує добре відпрацьована законодавча система забезпечення інформаційної безпеки. Вона засновується на нормативно-правових ак-

тах стратегічного характеру *(Стратегія національної безпеки* та *Стратегія кібербезпеки)*, положення яких розробляються у нормативно-правових актах нижчого порядку, що дозволяє сформувати дієву систему забезпечення кібербезпеки.

Україна наразі потребує подальшого нормативного урегулювання забезпечення інформаційної безпеки у цілому та кібербезпеки зокрема. Для цього необхідно здійснити низку заходів із розроблення та прийняття Концепції інформаційної безпеки України, яка б базувалась на положеннях Доктрини інформаційної безпеки України та розвивала їх у напрямі визначення конкретних шляхів реалізації. Окрім цього, убачається нагальною потреба прийняття Закону України "Про кібербезпеку" як необхідного інструмента забезпечення кібернетичної безпеки держави.

*Конюшок С.М.,*
*кандидат технічних наук, доцент,*
*Інститут спеціального зв'язку*
*та захисту інформації НТУУ "КПІ"*

## РОЛЬ ТА МІСЦЕ БЕЗПЕКИ ІНФОРМАЦІЇ В СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Спрощене бачення першопричин зародження ідеї створення Держави [1] як соціального об'єднання громадян дозволяє стверджувати, що однією з ключових причин є інстинктивне спрямування особи та громади до Безпеки. Це і персональна безпека від фізичних загроз із боку інших осіб, і стабільний захист від загроз форс-мажорних обставин, наприклад, природних катаклізмів.

Розвиток покладених на Державу зобов'язань щодо своїх громадян зумовив розширення сутності поняття Безпека. Наразі, поняття "безпека" є неформалізованим і в роботах із відповідної тематики застосовується в контексті обраної проблематики [2].

Початкове заглиблення у сутність питання щодо термінології у галузі безпеки привело до висновку про неодностайне бачення фахівцями зазначених понять і фактичну відсутність спроб подолання зазначеної проблеми [2–5]. Нам не вдалося знайти у відкритих джерелах (доступних широкому загалу) будь-якого документа, який демонструє узгоджене колегіальне бачення фахівців щодо понять "безпека", "інформаційна безпека" та "безпека інформації".

Актуальність зазначеної роботи для практичної діяльності центральних органів виконавчої влади, військових формувань та

правоохоронних органів складно переоцінити, оскільки історія світової науки свідчить, що “єдина мова” науковців та практиків у будь-якій галузі сприяє збільшенню інтенсивності взаємодії фахівців і, як наслідок, прискоренню розвитку самої галузі.

В доповіді викладене наше бачення значення інформаційної безпеки для решти видів національної безпеки, а також сутності поняття “безпека” та низки пов’язаних із ним понять. Сподіваємось на плідну наукову дискусію, яка сприятиме формалізації вказаних важливих понять.

## ЛІТЕРАТУРА

1. Теорія виникнення держави [Електронний ресурс]. – Режим доступу : http://uk.wikipedia.org/wiki/Виникнення_держави. – Назва з екрану.

2. Горбулін В.П. Засади національної безпеки України : підруч. / В.П.Горбулін, А.Б.Качинський. – К : Інтертехнологія, 2009. – 272 с.

3. Качинський А.Б. Безпека, загрози і ризик: наукові концепції та математичні методи / А.Б.Качинський. – К., 2003. – 472 с.

4. Крутов В.В. Від патріотичного виховання, боротьби з тероризмом… до недержавної системи національної безпеки / В.В.Крутов – К : Вид-во “Преса України”, 2009. – 592 с.

5. Національний інститут стратегічних досліджень при Президентові України [Електронний ресурс]. – Режим доступу : http://www.niss.gov.ua. – Назва з екрану.

*Костюченко О.Є.,*
*кандидат юридичних наук, доцент,*
*Харківський інститут банківської справи*
*Університету банківської справи НБУ*

## ПРАВОВІ ПРОБЛЕМИ ДЕТЕРМІНАЦІЇ ІНФОРМАЦІЙНОЇ ТА ФІНАНСОВОЇ БЕЗПЕКИ В УКРАЇНІ

Останнім часом проблеми, зосереджені в інформаційній сфері, набувають загрозливого характеру для стану фінансової безпеки суб’єктів. Поряд зі злочинною діяльністю кардерів, хакерів, однією із загроз фінансовій безпеці суб’єктів господарювання є виток інформації про процеси здійснення їхньої основної діяльності. Як правило, така інформація належить до інформації з обмеженим доступом. Яким чином протидіяти цій загрозі? На нашу думку, вирішити це питання має правовий режим інформації з об-

меженим доступом, який гарантуватиме дотримання прав та інтересів усіх учасників інформаційних відносин.

Проаналізуємо законодавчі положення, які визначають правовий режим інформації в Україні. Правові засади інформаційної діяльності в Україні визначені в Законі України "Про інформацію"[1], ст. 9 якого встановлює, що основними видами інформаційної діяльності є створення, збирання, одержання, зберігання, використання, поширення, охорона та захист інформації. У ст. 21 визначено види інформації з обмеженим доступом. При цьому конфіденційною визнано інформацію про фізичну особу, а також інформацію, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом. Відносини, пов'язані із правовим режимом конфіденційної інформації, регулюються законом.

На перший погляд, цитовані положення вказують на умови обігу інформації та порядок визначення інформації з обмеженим доступом, однак, визначаючи правовий режим інформації, законодавець застосував техніко-юридичний прийом винятків. Виходячи з того, що власник інформації має право визначити її інформацією з обмеженим доступом, але не вся вона може бути обмежена в доступі, в законі наведені винятки із цього загального дозволу. Натомість п. 4 ст. 21 закріплено таке: "6) інші відомості, доступ до яких не може бути обмежений відповідно до законів та міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України". Ми вважаємо це формулювання некоректним, бо, установлюючи правовий режим інформації з обмеженим доступом шляхом загального дозволу із застосуванням винятків, потрібно укласти їх "вичерпні переліки". Тому цей пункт необхідно виключити, а ст. доповнити п. 5, де закріпити таке: "перелік може бути доповнений іншими видами інформації, доступ до яких не може бути обмежений відповідно до законів та міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України".

При цьому, розглядаючи в парламенті питання про ратифікацію певного міжнародного договору України, слід паралельно розглядати питання про внесення змін до ст. 21 Закону України "Про інформацію". Такі зміни нададуть регулюванню визначеності та виключать можливість вільного трактування цитованого положення.

Також незрозумілою є позиція законодавця щодо положень ст. 29 аналізованого закону, зокрема, передбачено, що інформація з обмеженим доступом може бути поширена, якщо вона є суспільно необхідною, тобто виступає предметом суспільного інтересу, і пра-

во громадськості знати цю інформацію переважає потенційну шкоду від її поширення. А предметом суспільного інтересу вважається інформація, яка свідчить про загрозу державному суверенітету, територіальній цілісності України; забезпечує реалізацію конституційних прав, свобод і обов'язків; свідчить про можливість порушення прав людини, уведення громадськості в оману, шкідливі екологічні та інші негативні наслідки діяльності (бездіяльності) фізичних або юридичних осіб тощо.

Ця стаття викликає низку запитань, замість того щоб урегулювати інформаційні відносини та окреслити їхні правові межі.

Наприклад, як визначати потенційну шкоду від поширення такої інформації? А за якими критеріями визначати суспільну необхідність поширення інформації з обмеженим доступом? Хто визначає "потенційну небезпеку" та "суспільну необхідність"? А що слід розуміти під негативними наслідками діяльності юридичної особи? Наприклад, візьмемо банк. Скажімо, банк у звітному періоді роботи вийшов на від'ємні показники діяльності, що свідчить про погіршення його фінансового стану. У банку, безперечно, є вкладники та кредитори, інтереси яких у цьому випадку наражаються на небезпеки неотримати прибутки або зазнати збитків. Що в цьому випадку необхідно робити? Поширювати інформацію з обмеженим доступом, яка розкриває причиново-наслідкові зв'язки такого результату діяльності, чи ні? Припустимо, ми її поширили і про це було надруковано статтю в пресі та зроблено репортаж на телебаченні. Імовірно, якщо це буде поодиноким випадком доведення інформації, то говорити про загрозу фінансовій безпеці банку буде перебільшенням, але якщо цю статтю роздрукують кілька видань, а на телебаченні репортаж транслюватимуть безліч разів, реакція вкладників цілком передбачувана − терміново забрати з банку свої гроші. Така ситуація в підсумку не просто погіршить фінансове становище банку, а може призвести до його неспроможності виконати свої зобов'язання перед вкладниками та кредиторами. Думаємо, що зазначене доводить нездатність ст. 29 Закону України "Про інформацію" забезпечити адекватне регулювання процесу поширення суспільно необхідної інформації. Це питання потребує додаткового аналізу та розроблення пропозицій щодо вдосконалення положень аналізованого закону.

Поряд із цим, окрім проблем загального характеру щодо регулювання інформації з обмеженим доступом, виникають питання щодо її захисту та охорони. Охорона інформації у ст. 7 базового закону описана так: "Право на інформацію, створену в процесі діяльності фізичної чи юридичної особи, суб'єкта владних повноважень або за рахунок фізичної чи юридичної особи, Державного бюджету України, місцевого бюджету, охороняється в порядку, визначеному

законом”. Знову запитання, якого закону? Якщо закону “Про інформацію”, то в ньому визначено таке: захист інформації − сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї. А право на інформацію передбачає можливість вільного одержання, використання, поширення, зберігання та захисту інформації, необхідної для реалізації своїх прав, свобод і законних інтересів. Реалізація права на інформацію не повинна порушувати громадські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи й законні інтереси інших громадян, права та інтереси юридичних осіб. Отже, окрім того що незрозуміле розмежування понять “захист інформації” та “охорона інформації”, аналіз закону ускладнює розуміння правового режиму інформації з обмеженим доступом загалом. Таке розмивання меж правового режиму призводить до проблем в організації охорони інформації з обмеженим доступом.

У підсумку зазначимо таке:

1. Інформаційна безпека детермінує з фінансовою безпекою, таким чином, що проблеми невизначеності правового режиму інформації з обмеженим доступом слід визнати загрозою фінансовій безпеці суб’єкта господарювання.

2. Покладати визначення правового режиму інформації тільки на суб’єктів господарювання є неправильним, бо загальний рівень безпеки держави визначально впливає на її соціально-економічний розвиток. Тому чинне законодавство про інформацію потребує вдосконалення, яке необхідно проводити з дотриманням технікоюридичних прийомів.

*Красноступ Г.М.,*
*кандидат юридичних наук,*
*старший науковий співробітник,*
*Науково-дослідний інститут*
*інформатики і права НАПрН України*

## ПЕРСПЕКТИВИ ПРАВОВОГО РЕГУЛЮВАННЯ НОВИХ МЕДІА

“Сиділи колись за залізною завісою, ловили кожну вісточку зі світу, – інформація була нашою здобиччю. Тепер ми – здобич інформації. Що б де не сталося, всім віддає в плече” [1, с. 13].

На сьогодні діяльність засобів масової інформації регулюється низкою законів України, зокрема такими, як: “Про державну підтримку

засобів масової інформації та соціальний захист журналістів", "Про друковані засоби масової інформації (пресу) в Україні", "Про телебачення і радіомовлення", "Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування засобами масової інформації", "Про доступ до публічної інформації".

9 травня 2011 р. набрала чинності нова редакція Закону України "Про інформацію", розділом ІІІ якої врегульовано питання діяльності журналістів та засобів масової інформації.

Статтею 22 вказаного Закону визначено поняття "масова інформація" та "засоби масової інформації". Так, під масовою інформацією слід розуміти інформацію, що поширюється з метою її доведення до необмеженого кола осіб.

Засоби масової інформації – це засоби, призначені для публічного поширення друкованої або аудіовізуальної інформації.

Слід зауважити, що чинне законодавство не містить дефініції поняття "нові медіа", а також спеціального нормативно-правового акта, який би визначав їх статус.

Аналізуючи досвід правового регулювання порушеного питання законодавством деяких країн СНД, можна дійти висновку, що до засобів масової інформації зокрема віднесено "способи розповсюдження масової інформації" (стаття 3 Закону Азербайджанської Республіки "Про засоби масової інформації") та "веб-сайти в суспільно доступних телекомунікаційних мережах Інтернет та інші" (стаття 1 закону Республіки Казахстан "Про засоби масової інформації"), "інші установи, що випускають та розповсюджують масову інформацію" (стаття 1 закону Республіки Грузія "Про пресу та інші засоби масової інформації").

Традиційні засоби масової інформації активно поширюють інформацію в інтернеті. Загальною тенденцією у світі є існування "нових медіа" поза межами правового поля, оскільки правове регулювання відповідних суспільних відносин наразі у законодавстві відсутнє.

Все частіше виникають ситуації, коли в інтернеті розміщується неперевірена інформація, яка не відповідає дійсності. Таку інформацію передруковують газети з посиланням на відповідне джерело знову-таки в мережі. У зв'язку з цим авторів подібних матеріалів неможливо притягти до відповідальності, а честь, гідність та ділову репутацію осіб захистити правовими засобами.

Окрему увагу слід звернути на проблему захисту авторських прав.

На сьогодні здійснюються спроби суб'єктів права законодавчої ініціативи врегулювати питання захисту авторських прав під час

поширення, у тому числі засобами масової інформації, аудіовізуальної інформації в інтернеті.

12 грудня 2012 р. у Верховній Раді України зареєстровано проект Закону України "Про внесення змін до деяких законодавчих актів щодо врегулювання питань авторського права і суміжних прав" (реєстр. № 0902), внесений народними депутатами України Луцьким М.Г., Самойлик К.С., Зарубінським О.О. [2]. Законопроектом зокрема пропонується викласти в новій редакції пункт 9 частини третьої статті 15 Закону України "Про авторське право і суміжні права", згідно з якою виключне право автора (чи іншої особи, яка має авторське право) на дозвіл чи заборону використання твору іншими особами дає йому право дозволяти або забороняти надання творів у користування широкого загалу таким чином, що бажаючі можуть здійснити доступ до творів із будь-якого місця і у будь-який час за їх власним вибором, у тому числі в інтерактивному режимі, через інтернет й інші телекомунікаційні мережі.

Вважаємо, що "нові медіа" повинні мати такі ж права, як і традиційні засоби масової інформації.

З огляду на наведене, можна вести мову про необхідність визначення статусу "нових медіа", порядку їх функціонування та легалізації (реєстрації).

Функція з реєстрації як друкованих засобів масової інформації, так і "нових медіа" має зосереджуватися в одному органі. Така реєстрація має здійснюватися за декларативним принципом. Тобто, нові медіа подають до органу реєстрації заяви, для внесення до відповідного Державного реєстру.

До перспектив регулювання діяльності нових медіа слід віднести підготовку проекту Закону України "Про внесення змін до Закону України "Про інформацію" щодо надання статусу засобів масової інформації новим медіа та визначення засад їх діяльності.

Уважаємо за доцільне під час підготовки законопроекту розділити такі поняття, як "нові медіа" (інтернетні ЗМІ) та "соціальні мережі" (Facebook, Livejournal, Twitter, YouTube, що можуть використовуватися не лише для розваг, але й для професійного розвитку, спілкування, отримання новин та обміну інформацією).

Оскільки реєстрація нових медіа відповідно до Закону України "Про адміністративні послуги" уважатиметься адміністративною послугою, законопроект також має містити такі положення:

– підстави для одержання адміністративної послуги (реєстрація нових медіа);

– суб'єкт надання адміністративної послуги (ЦОВВ) та його повноваження щодо реєстрації нових медіа;

– перелік та вимоги до документів, необхідних для реєстрації нових медіа;

– інформація про платність або безоплатність реєстрації;

– граничний строк надання адміністративної послуги з реєстрації нових медіа;

– перелік підстав для відмови в наданні відповідної адміністративної послуги.

Прийняття Закону сприятиме:

– надання співробітникам нових медіа статусу журналістів;

– відшкодуванню шкоди, завданої порушенням авторських прав;

– притягненню до відповідальності за порушення законодавства про інформацію та захист суспільної моралі.

Потенційна користь від запровадження пропонованих змін полягає в тому, що стане відомо, хто за яким ресурсом стоїть, несе відповідальність за розміщену інформацію.

На нашу думку, зазначене вище підлягає врахуванню під час законотворчої діяльності, що в подальшому сприятиме вдосконаленню інформаційного законодавства та відповідному забезпеченню державної інформаційної політики.

## ЛІТЕРАТУРА

1. Записки українського сумашедшого / Ліна Костенко. – К. : Вид-во “А-БА-БА-ГА-ЛА-МА-ГА”, 2011. – 416 с.

2. Про внесення змін до деяких законодавчих актів щодо врегулювання питань авторського права і суміжних прав : проект Закону України / внесений народними депутатами України М.Г.Луцьким, К.С.Самойлик, О.О.Зарубінським. – Режим доступу : http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=45099.

*Кузьмін С.А.,*
*кандидат юридичних наук,*
*Міжвідомчий науково-дослідний центр*
*з проблем боротьби з організованою злочинністю*
*при Раді національної безпеки і оборони України*

## КІБЕРНЕТИЧНА ІНФОРМАЦІЯ В КОНТЕКСТІ ОБ’ЄКТИВНИХ ОЗНАК СКЛАДУ ЗЛОЧИНУ

У 2001 році на міжнародному рівні нормативно було закріплено визначення комп’ютерної інформації як інформації, яка знаходиться

у пам’яті комп’ютера, на машинах або інших носіях, у формі, доступній сприйняттю ЕОМ, або яка передається по каналах зв’язку [1, с. 94–95]. Зауважимо, що, на нашу думку, було б цілком правомірним для усунення можливого подвійного тлумачення термінології використати і термін “кібернетична інформація”, оскільки їхній зміст є повністю синонімічним. При цьому в контексті застосування норм кримінального закону поняття комп’ютерної (кібернетичної) інформації необхідно ототожнювати з поняттям комп’ютерних даних, під якими, як зазначається у наукових джерелах, слід розуміти сукупність усіх даних, що оброблюються в електронно-обчислювальних машинах (комп’ютерах), автоматизованих системах, комп’ютерних мережах, передаються мережами електрозв’язку незалежно від засобу їх фізичного та логічного подання, а також зберігаються на електронних носіях інформації [2, с. 22].

На жаль, вітчизняна кримінально-правова наука, досліджуючи поняття предмета злочину в контексті загального вчення про склад злочину, явно недостатню увагу приділяла проблемним питанням визначення інформації, як предмета злочину, а тим більше, комп’ютерна інформація взагалі окремо не розглядалася як предмет злочину [3, с. 159–160]. Натомість, фактично лише опосередковано, в контексті коментування змісту конкретних норм розділу XVI Особливої частини кримінального закону, така інформація згадувалась як засоби і знаряддя учинення злочину.

Хоча традиційно при створенні законодавчих конструкцій спеціальних норм кримінального закону саме згадані факультативні ознаки об’єктивних елементів правової норми, у значній кількості випадків, знаходять найбільш повне нормативне відображення та мають за своїм змістом пріоритетне значення для забезпечення правильної кваліфікації діянь винного.

Загалом, сьогодні більшість науковців традиційно обов’язковою умовою предмета злочину, засобів і знарядь його вчинення визначають їх належність виключно до матеріальних об’єктів.

М.Й.Коржанський визначав предмет злочину як конкретний матеріальний об’єкт, у якому проявляються певні сторони, властивості суспільних відносин (об’єкта злочину), шляхом фізичного чи психічного впливу на який вчинюється суспільно небезпечна шкода у сфері цих суспільних відносин [4, с.134]. П.С.Матишевський під предметом злочину розумів речі, певні цінності матеріального світу, діючи на які особа посягає на блага, що належать суб’єктам суспільних відносин [5, с. 104]. Ю.В.Александров та В.А.Клименко вказували, що предмет злочину – це як речі, так і інші предмети матері-

ального світу, у зв'язку з якими або з приводу яких вчинюється злочин, або, впливаючи на які, винний посягає на суспільні відносини, що охороняються кримінальним законом [6, с. 54]. А.А.Музика та Є.В.Лащук ведуть мову про предмет злочину як факультативну ознаку об'єкта злочину, що знаходить свій вияв у матеріальних цінностях (котрі людина може сприймати органами чуття чи фіксувати спеціальними технічними засобами), з приводу яких і шляхом безпосереднього впливу на які (або без такого впливу) вчиняється злочинне діяння [7, с. 110]. Повністю аналогічні підходи науковців простежуються і щодо засобів та знарядь учинення злочину.

Вочевидь, що представлені підходи до концептуального визначення предмета злочину, його засобів і знарядь, жодним чином не відображають навіть можливість віднесення до них комп'ютерної (кібернетичної) інформації та підводять нас до висновку про штучну підміну при застосуванні такого підходу самої комп'ютерної (кібернетичної) інформації лише її матеріальним носієм.

Тут убачається доцільним доповнити і висновок О.Ф.Бантишева про те, що предмет злочину внаслідок його учинення може знищуватися, псуватися, втрачати свої якості, переміщатися у просторі, змінювати володільця, незаконно виготовлятися або вживатися, змінювати свій вигляд тощо [8, с. 92], у частині, що предмет злочину може перетворюватись на засоби та знаряддя вчинення злочину або одночасно ними бути вже із підготовчих дій (стадії готування до злочину). При цьому слід одночасно зауважити, що серед останніх двох термінів найбільше значення належить, безумовно, знаряддям злочину, оскільки вони не тільки безпосередньо використовуються для вчинення злочину, а й без їх застосування вчинення злочину, власне у такий спосіб, є неможливим [9, с. 18]

Отже, пропонуємо в теорії кримінального права визнати, що предмет, засоби і знаряддя вчинення злочину принципово не можна розглядати як матеріальну цінність (предмет), певну константу, щось незмінне та матеріально зафіксоване, нездатне до трансформації, отже, слід відходити від "укоріненого", виключно матеріально-речового сприйняття цих факультативних об'єктивних ознак складу злочину.

Зокрема, предметом злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку є саме кібернетична інформація, при цьому така інформація може бути використана одночасно або окремо як засоби знаряддя учинення таких або інших видів злочинів.

**ЛІТЕРАТУРА**

1. Словник термінів з кібербезпеки / [за заг. ред. Копана О.В., Скулиша Є.Д.]. – К. : ВБ “Аванпост-Прим”, 2012. – 214 с.

2. Бутузов В. М. Науково-практичний коментар до Кримінального кодексу України. Особлива частина. Розділ XVI. Злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку / В.М.Бутузов, С.А.Кузьмін, В.П.Шеломенцев. – К. : Паливода А.В., 2010. – 152 с.

3. Кузьмін С.А. Комп’ютерна (кібернетична інформація) як предмет учинення злочину (кримінально-правовий аспект) / С.А.Кузьмін // Інформація і право. – 2012. – № 3 (6). – С. 159–163.

4. Коржанський М.Й. Уголовне право України. Загальна частина : курс лекцій / М.Й.Коржанський. – К. : Наукова думка, 1996. – 334 с.

5. Матишевский П.С. Кримінальне право України : загальна частина : підруч. [для студ. юрид. вузів і фак-тів] / П.С.Матишевський. – К. : “А.С.К.”, 2001. – 347 с.

6. Александров Ю.В. Кримінальне право України : заг. частина : підруч. [для студ. вищ. навч. закл.] / Ю.В.Александров, В.А.Клименко. – К. : МАУП, 2004. — 328 с.

7. Музика А.А. Предмет злочину: теоретичні основи пізнання : моногр. / А.А.Музика, Є.В.Лащук. – К. : Паливода А.В., 2011. – 192 с.

8. Бантишев О.Ф. Кримінальна відповідальність за злочини проти основ національної безпеки України (проблеми кваліфікації) : моногр. / О.Ф.Бантишев. – К. : Вид-во НА СБ України, 2001. – 122 с.

9. Бантишев О.Ф. Науково-практичний коментар до Кримінального кодексу України. Загальна частина / О.Ф.Бантишев, С.А.Кузьмін. – К. : Паливода А.В., 2010. – 336 с.

*Кукін І.В.,*
*Науково-дослідний інститут*
*Державної прикордонної служби України*

## ОКРЕМІ ПІДХОДИ ДО ВРЕГУЛЮВАННЯ ДЕРЖАВНО-ПРАВОВИХ ПРОБЛЕМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Трудова діяльність людини, як правило, ототожнюється з виробництвом товарів або послуг. У зв’язку з цим виникає питання кла-

сифікації результатів виконання органами державної влади нормативно визначених завдань та функцій у сфері інформаційної безпеки.

Починаючи з 1990-х років, у практику роботи державних органів впроваджуються міжнародні стандарти ISO 9000 серії щодо управління якістю діяльності. Необхідність адаптації національних нормативно-правових актів до міжнародних стандартів потребує дослідження особливостей діяльності персоналу у сфері інформаційної безпеки як процесів надання послуг.

Сучасні підходи щодо визначення понятійного апарату державних послуг та застосування органами державної влади стандартів ISO 9000 серії наведені у роботах В.В.Голубь, В.Я.Малиновського, О.І.Момота, Н.М.Муравйової. Проте в останніх дослідженнях недостатньо уваги приділяється розгляду діяльності персоналу державних установ, яка пов'язана із застосуванням правоохоронних повноважень як процесів надання послуг.

Метою дослідження є визначення підходів до використання термінології державних послуг для врегулювання державно-правових проблем у сфері інформаційної безпеки.

У теорії державного управління під державними послугами розуміються "послуги, що надаються органами державного управління суспільству та окремим його членам для задоволення їх потреб, гарантованих громадянам демократичної, соціальної і правової країни її конституцією" [1, с. 446]. На думку В.Я.Малиновського, "державні послуги ... є результатом реалізації законодавчо встановлених завдань і функцій державних органів, спрямованих на виконання зобов'язань держави перед громадянами, їх об'єднаннями, фізичними та юридичними особами (споживачами) у сфері забезпечення їх прав і свобод" [2, с. 240].

Можна погодитися з думкою О.І.Момота та Н.М.Муравйової, що у сучасному менеджменті все більше уваги приділяється керуванню якістю діяльності організацій та стандартизації якості послуг з метою гарантування їх споживчих властивостей [3, с. 25; 4 с. 18] Проте зазначені підходи не враховують правоохоронні аспекти діяльності органів державної влади, а саме:

– гарантований законами України захист інформації та персоніфікованих даних [5, ст. 27; 6, ст. 24 та ст. 28];

– встановлення кримінальної та адміністративної відповідальності за скоєні злочини й правопорушення у сфері інформаційної безпеки [7, ст. 328-330; 8, ст. $212^2$].

Діяльність правоохоронних органів потребує удосконалення понятійного апарату державних правоохоронних послуг, які можна розподілити на одноадресні (мають одного споживача) та багатоад-

ресні (два і більше споживачів) [9, с. 473]. Прикладом багатоадресної послуги може бути реалізація прав однієї особи за умов забезпечення інформаційної безпеки інших членів суспільства.

Це зумовлює необхідність розподілу багатоадресних державних правоохоронних послуг на гармонізовані (за умов збігу інтересів особи та суспільства) та з конфліктом інтересів (щодо випадків, коли інтереси особи не збігаються з інтересами суспільства) [9, с. 473]. Конфлікт інтересів споживачів державної правоохоронної послуги у сфері інформаційної безпеки може виникати внаслідок невідповідності необхідних та доступних для захисту інформації ресурсів, а також у випадках, коли стосовно певної особи проводяться слідчі або інші передбачені законами України заходи.

Наведена класифікація державних правоохоронних послуг може бути використана для удосконалення нормативно-правових актів органів державної влади щодо організації, планування, забезпечення, мотивації та контролю за діяльністю персоналу. Результати контрольних заходів можуть застосовуватись для визначення переліку необхідних змін щодо елементів технологічних процесів, удосконалення порядку застосування загальних функцій державного управління.

Система управління якістю діяльності у сфері інформаційної безпеки може полягати у:

– документуванні потреб груп споживачів інформації з урахуванням конфліктів їх інтересів в умовах ресурсних обмежень органів державної влади;

– установленні методів та порядку вимірювання характеристик державних правоохоронних послуг і пов’язаних із ними процесів для оцінки результативності та ефективності діяльності персоналу;

– визначенні процесів, відповідальності персоналу, переліку необхідних ресурсів для гарантованого надання споживачам державних правоохоронних послуг нормативно встановленої якості, а також запобігання та усунення відхилень показників якості діяльності персоналу від нормативних вимог;

– удосконаленні контролю за якістю послуг та відстеженні змін реальних потреб і очікувань споживачів інформаційних ресурсів в інтересах постійного поліпшення якості діяльності органів державної влади.

Розглянуті підходи до описання процесів забезпечення інформаційної безпеки як надання державних правоохоронних послуг можуть сприяти запровадженню в органах державної влади рекоме-

ндацій ДСТУ ISO 9000 серії щодо постійного поліпшення якості діяльності. Також правоохоронна спрямованість посадових обов'язків окремих категорій працівників органів державної влади потребує врахування в нових редакціях ДСТУ ISO 9000 серії особливостей державних правоохоронних послуг.

Напрямом подальших досліджень може бути описання характеристик державних правоохоронних послуг у сфері інформаційної безпеки, способів їх вимірювання для розроблення системи відповідних державних стандартів.

## ЛІТЕРАТУРА


1. Публічне врядування : Енциклопедія державного управління : у 8 т. / наук. ред. кол. : В.С.Загорський (голова), С.О.Телешун (співголова) [та ін.]. – Львів : ЛРІДУ НАДУ, 2011. – Т. 8. – 630 с.

2. Маліновський В.Я. Державне управління : навч. посіб. – 3-тє вид., переробл. та допов. / В.Я.Маліновський. – К. : Атіка, 2009. – С. 240–246.

3. Момот О.І. Менеджмент якості та елементи системи якості : навч. посіб. / О.І.Момот. – К. : Центр учбової літератури, 2007. – 368 с.

4. Муравьева Н.Н. Маркетинг услуг : учеб. пособ. / Н.Н.Муравьева. – Ростов-на-Дону : Феникс, 2009. – 251 с.

5. Про інформацію : Закон України від 02.10.1992 № 2657-XII [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/2657-12.

6. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/229717.

7. Кримінальний кодекс України [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/2341-14.

8. Кодекс України про адміністративні правопорушення [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/80731-10/page13.

9. Кукін І.В. Удосконалення термінологічного апарату у сфері надання послуг Державною прикордонною службою України / І.В.Кукін // Актуальні проблеми державного управління : зб. наук. пр. – Х. : Вид-во ХарРІ НАДУ "Магістр", 2012. – № 1 (41). – С. 470–475.

*Курок Р.О.,*
*Національна академія Служби безпеки України*

# ІНФОРМАЦІЙНА БЕЗПЕКА В ДІЯЛЬНОСТІ СБ УКРАЇНИ: СУЧАСНІ ПРОБЛЕМИ ТА ШЛЯХИ ЇХ ВИРІШЕННЯ

Інформаційне забезпечення діяльності СБ України є одним з основних напрямів її функціонування, значення якого зростає. Діяльність СБ України як правоохоронного органу спеціального призначення, який забезпечує державну безпеку України [1], пов'язана з постійним збиранням, передачею, фіксацією, збереженням, пошуком та опрацюванням інформації, необхідної для виконання законодавчо визначених завдань, які на неї покладаються. Робота з інформацією є невід'ємною складовою повсякденної діяльності, супроводжує та пронизує увесь процес управління в СБ України.

Під інформаційним забезпеченням діяльності СБ України розуміють сукупність організаційних, правових, матеріально-технічних та інших заходів щодо цілеспрямованого збору, обліку, опрацювання інформації, її збереження, документального оформлення та реалізації.

На практиці органи та підрозділи СБ України залежно від характеру покладених завдань, компетенції і визначених повноважень займаються інформаційним забезпеченням своєї діяльності, а його результати використовують для аналітичних досліджень, прийняття управлінських рішень, розроблення заходів, методичних рекомендацій тощо.

На виконання положення ст. 24 закону України "Про Службу безпеки України" для ведення інформаційно-аналітичної діяльності в СБ України створюються та автоматизовані інформаційні системи, а також використовуються групи відповідних обліків. Інформаційні системи створюються для збору, збереження та розповсюдження необхідної органам і підрозділам СБ України інформації, під якою згідно зі ст. 1 Закону України "Про інформацію" розуміють будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [2].

Враховуючи характер завдань, які покладені на Службу безпеки України, а також форми і методи роботи спецслужби, інформація, яка циркулює в системі СБ України, як правило, має обмежений доступ, її несанкціонований витік та розголошення може заподіяти суттєву шкоду інформаційній безпеці держави.

Інформаційна безпека розглядається в декількох аспектах, а саме як забезпечення стану захищеності:

- особи, суспільства, держави від впливу неякісної інформації;

- інформації та інформаційних ресурсів від неправомірного впливу сторонніх осіб;

- інформаційних прав і свобод громадянина.

Акцентуємо увагу на перших двох аспектах. Захищеність від впливу неякісної інформації передбачає відсутність впливу на індивідуальну та колективну свідомість небезпечної (деструктивної) інформації, маніпулювання свідомістю, дезінформування, формування хибних морально-етичних установок у населення тощо.

Захист інформації та інформаційних ресурсів характеризується стійкістю інформаційних систем стосовно впливу на них загроз, результатом дії яких може бути витік інформації, її несанкціонована модифікація або знищення.

Джерелами дестабілізуючих чинників можуть бути як окремі особи, так і організації та спецслужби іноземних держав. Так, у доступі до інформації, що характеризує діяльність Служби безпеки України та обробляється у її автоматизованих системах, можуть бути зацікавлені як окремі особи з кримінального середовища, так і розвідувальні органи, які цілеспрямовано займаються збором інформації з обмеженим доступом. Сукупність джерел разом із властивими їм видами дестабілізуючих чинників формують сукупність загроз інформаційній безпеці, які складаються, з одного боку, з інформаційних загроз, що впливають на стан поінформованості особи, суспільства і держави, та загроз інформації, які впливають на можливість її безперешкодного оброблення (у т.ч. з використанням автоматизованих систем) та забезпечення встановленого режиму доступу до неї.

Тому на сучасному етапі проблемними залишаються питання, пов’язані з захистом службової інформації, яка циркулює в Службі безпеки України, від несанкціонованого доступу до неї з використанням комплексу організаційно-правових, інженерно-технічних та інших заходів, спрямованих на запобігання розголошенню інформації з обмеженим доступом і втратам її матеріальних носіїв.

## ЛІТЕРАТУРА

1. Закон України “Про Службу безпеки України” від 25 березня 1992 року № 2229–XII // Відомості Верховної Ради України. – 1992. – № 27. – Ст. 382.

2. Закон України “Про інформацію” від 2 жовтня 1992 року // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650.

*Логінов І.В.,*
*кандидат юридичних наук, старший науковий співробітник,*
*Національна академія Служби безпеки України*

*Тищенко Є.Ф.,*
*кандидат юридичних наук, доцент,*
*Національна академія Служби безпеки України*

# ШЛЯХИ УДОСКОНАЛЕННЯ КРИМІНАЛЬНОГО ЗАКОНОДАВСТВА У СФЕРІ НЕЗАКОННОГО ПРИДБАННЯ, ЗБУТУ АБО ВИКОРИСТАННЯ СПЕЦІАЛЬНИХ ТЕХНІЧНИХ ЗАСОБІВ НЕГЛАСНОГО ОТРИМАННЯ ІНФОРМАЦІЇ

У 2001 р. статтею 359 Кримінального кодексу України (далі – ККУ) криміналізовано відповідальність за протиправне використання спеціальних технічних засобів негласного отримання інформації (далі – СТЗ). Ужитими заходами була посилена юридична відповідальність за незаконні придбання, збут або використання СТЗ. Але на заваді широкому застосуванню статті 359 стало визначення СТЗ, закріплене у "Ліцензійних умовах провадження господарської діяльності з розроблення, виготовлення спеціальних технічних засобів для зняття інформації з каналів зв'язку, інших засобів негласного отримання інформації, торгівлі спеціальними технічними засобами для зняття інформації з каналів зв'язку, іншими засобами негласного отримання інформації". Тому в новій редакції "Ліцензійних умов…", яку було затверджено наказом Голови СБ України від 31.01.2011 р. № 35, подане розширене поняття СТЗ, що змінило диспозицію ст. 359 КК і, на нашу думку, призвело до порушення принципу справедливості й рівності осіб перед законом, та негативно впливає на авторитет СБ України, до компетенції якої віднесені виявлення, попередження і припинення злочинів, передбачених ст. 359 ККУ.

Для наочної демонстрації становища, що склалося, уявімо, що вулицею міста ідуть дві особи. Перша – в окулярах Google Glass [1], друга – у звичайних окулярах і з побутовою відеокамерою. Обидві особи записують за допомогою зазначених технічних засобів те, що відбувається на вулиці, тобто у загальнодоступному місці. Вони фіксують відкриту інформацію, збирати яку згідно із ст. 34 Конституції України ніхто не може заборонити. Але перша особа підлягає кримінальній відповідальності за ст. 359 ККУ, оскільки за технічними ознаками натільний комп'ютер, відомий як Google Glass, в Україні належить до категорії спеціального технічного засобу отри-

мання інформації, а друга особа – ні, хоча мотив, мета і результат їхніх дій однакові, а суспільно небезпечні наслідки відсутні більше того, дії обох осіб є реалізацією права, гарантованого Конституцією.

Інший приклад. На відкритій лекції з української філології в університеті поряд сидять два студенти. Один конспектує лекцію в зошиті за допомогою ручки SY-119 [2] і одночасно фіксує виступ викладача на вбудований у цю ручку диктофон. Другий конспектує текст ручкою, а виступ викладача записує за допомогою звичайного мініатюрного репортерського диктофону чи навіть MP3-плейєра. Перший студент підлягає кримінальній відповідальності за ст. 359 ККУ, оскільки ручка з диктофоном належить до СТЗ, другий – ні. Водночас, дії обох не становлять суспільної небезпеки, оскільки спрямовані на збирання відкритої інформації. Пересилання в бандеролі ручки і диктофону не є злочином, а ручки з вбудованим диктофоном кваліфікується як злочин.

З огляду на це інтернет переповнений наріканнями як на законодавців, так і на виконавця – СБ України, яка застосовує ст. 359 ККУ у численних випадках, схожих із наведеними прикладами [3; 4].

Раніше в низці наукових статей ми обґрунтували, що, поза сумнівом, кримінальна відповідальність повинна наступати за збирання інформації з обмеженим доступом (державної таємниці, службової інформації, комерційної й банківської таємниці, конфіденційної інформації про особу тощо – далі ІзОД) шляхом прихованого впровадження технічних засобів у простір, де оброблення ІзОД контролюється її власником. У технічному захисті інформації цей простір іменується "контрольованою зоною" [5]. Причому для кваліфікації таких дій як злочинних категорія технічного засобу (побутова техніка, СТЗ і т.д.) не має значення. Наприклад, якщо мініатюрний "петличний радіомікрофон" [6], що застосовується дикторами телебачення і не є СТЗ, буде конспіративно впроваджено у житло без дозволу його власника для прослуховування приватних розмов, то ідеться про злочин, передбачений ст. 182 ККУ "Порушення недоторканості приватного життя".

Аналогічного висновку про достатню захищеність від несанкціонованого отримання ІзОД і, відповідно, інформаційних прав держави, юридичних і фізичних осіб не статтею 359, а іншими статтями ККУ незалежно від нас дійшли анонімні автори публікації "Кримінальна відповідальність за користування спецзасобами" [7]. Не заперечують його також інші дослідники, зокрема, В.І.Возний [8]. Але далі наші погляди розходяться, оскільки вони пропонують виокремлювати СТЗ із-посеред іншої техніки за технічними параметрами.

Цю пропозицію реалізовано шляхом прийняття методики проведення судової експертизи спеціальних технічних засобів негласного отримання інформації. Вона створена Українським науково-дослідним інститутом спеціальної техніки та судових експертиз СБ України. 02.03.2011 р. Міністерство юстиції України прийняло рішення про державну реєстрацію цієї методики і внесення її до Реєстру методик проведення судових експертиз за № 383, реєстраційний код 17.0.01. Ми ж уважаємо, що мініатюризація і універсалізація технічних засобів оброблення інформації є результатом невпинного науково-технічного прогресу. Намагання визначити чіткі технічні критерії для виокремлення СТЗ є, на нашу думку, безперспективною спробою протидіяти науково-технічному прогресу, оскільки дуже скоро технічні параметри застарівають.

Таким чином, доходимо висновків:

1. Якщо особа використовує технічні засоби для незаконного здобування інформації з обмеженим доступом шляхом проникнення до "контрольованої зони", то кваліфікація її діяння як злочинного залежить не від виду (категорії) технічних засобів, а від змісту інформації, що здобувається, правового статусу суб'єкта злочину, способу його вчинення тощо. При цьому кримінальна відповідальність може наступати за статтями 111, 114, 162, 231, 182, 330 ККУ.

2. Практика застосування ст. 359 ККУ у значній кількості випадків свідчить про порушення принципу справедливості й рівності осіб перед законом у ситуаціях, коли дії осіб не мають суспільної небезпеки, що викликає численні нарікання громадян України і підриває авторитет СБ України як правоохоронного органу спеціального призначення.

3. За вказаних умов та в чинній редакції ст. 359 ККУ пропонуємо декриміналізувати передбачений нею злочин.

## ЛІТЕРАТУРА

1. Google Glass [Електронний ресурс] // Вебсайт "Википедия – свободная энциклопедия". – Режим доступу : http://ru.wikipedia.org/wiki/Google_Glass.

2. Ручка с диктофоном и камерой высокого разрешения со встроенным датчиком движения [Електронний ресурс] // Вебсайт інтернет-магазину "4safe.com.ua". – Режим доступу : http://www.4safe.com.ua/cat35/SY-119.

3. Открытое письмо "Про внесення змін до Кримінального кодексу України [Електронний ресурс] // Вебсайт "Антикоррупционный протал". – Режим доступу : http://job-sbu.org/otkryitoe-pismo-provnesennya-zmin-do-kriminalnogo-kodeksu-ukrayini.html.

4. Как украинцам “шьют” дела за СТС — в письме читателя “УК” // Вебсайт “Украина криминальная”. – Режим доступу : http://cripo.com.ua/print.php?sect_id=13&aid=137069.

5. ДСТУ 3396.2-97 Технічний захист інформації. Терміни та визначення. – К. : Держстандарт України, 1997. – С. 65-80.

6. Петличный микрофон [Електронний ресурс] / Вебсайт “SoundMaster” – Режим доступу : http://soundmaster.kiev.ua/shop/petlichnyj-mikrofon/all/all.

7. Кримінальна відповідальність за користування спецзасобами [Електронний ресурс] / Вебсайт “Юридична компанія “Юрисконсалт”. – Режим доступу : http://www.uris-c.com.ua/2012/04/10/кримінальна-відповідальність-за-кор/.

8. Возний В.І. Генеза законодавства про відповідальність у сфері спеціальних технічних засобів негласного отримання інформації [Електронний ресурс] / В.І.Возний // Вебсайт “Scientific World”. – Режим доступу : www.sworld.com.ua/konfer30/975.pdf.

*Матяш О.І.,*
*кандидат технічних наук,*
*старший науковий співробітник,*
*Національна академія Служби безпеки України*

## СЕКРЕТНЕ ДІЛОВОДСТВО В СИСТЕМІ УПРАВЛІННЯ ДІЯЛЬНІСТЮ ПІДПРИЄМСТВ, УСТАНОВ, ОРГАНІЗАЦІЙ

Діяльність підприємств, установ, організацій (далі – установи) спрямована на досягнення поставленої мети шляхом виконання поточних завдань. Управління діяльністю установи передбачає послідовне виконання таких загальних функцій, як планування, організація, мотивація і контроль.

Усі ці функції об’єднані процесами комунікації та прийняття рішень [1]. Кожна функція під час виконання передбачає наявність матеріальних носіїв для передачі інформації, здебільшого певних типів документів. Так, наприклад, функція планування передбачає оформлення мети та завдань установи, основних напрямів її діяльності. Для цього створюють та приймають такі документи, як статути, положення.

Функція організації передбачає створення певної структури для виконання запланованого. Для цього розроблюються й затверджу-

ються штатні розклади. Для виконання конкретних завдань керівником визначаються виконавці, яким надаються певні повноваження та права. Діяльність персоналу установи регламентується функціональними обов'язками, планами-завданнями, облік матеріальних цінностей відбувається за книгами обліку, накладними.

Функція мотивації направлена на створення умов для успішного вирішення поставлених завдань та полягає у визначенні потреб підлеглих, сприянні їх розвитку та вдосконаленню, проведенні навчань.

Функція контролю передбачає визначення на певний проміжок часу результатів роботи, виявлення проблемних аспектів та подолання перешкод до виконання запланованих результатів.

Діловодні операції – складова діяльності установи, а установи – складові економіки держави. Останні теоретичні розробки обґрунтування необхідності діловодства в економіці належать Рональдові Гаррі Коузу (США), якому в 1991 році за це присуджено Нобелівську премію. До нього економіка аналізувалася у рамках інституційної структури і це сприймалося як теорема. Тобто існування установ сприймалося як само собою зрозуміле. Зміни форм контрактів теж розглядалися як аксіоматичні факти, а юридичні закони й положення – як принесені ззовні правила економічної діяльності.

Коуз ставить питання: чому управлінці та робітники воліють працювати разом, замість того щоб продавати свою працю одне одному? І відповідає: в разі відмови від такого порядку речей були б потрібні набагато більші витрати на підготовку і виконання контракту, у тому числі на організаційне управління цими процесами. Вчений доводить, що мікроекономічна теорія була неповною, бо не враховувала ці витрати, розглядаючи лише виробничі й транспортні. За його теорією саме "вартість укладання та виконання контрактів і утримання організацій" становить значну частину загальних ресурсів економіки [2].

Для підвищення ефективності управлінської діяльності установи завжди актуальна мінімізація витрат для досягнення поставленої мети:

$$E = \min \sum_{i=1}^{K} n_i ,$$

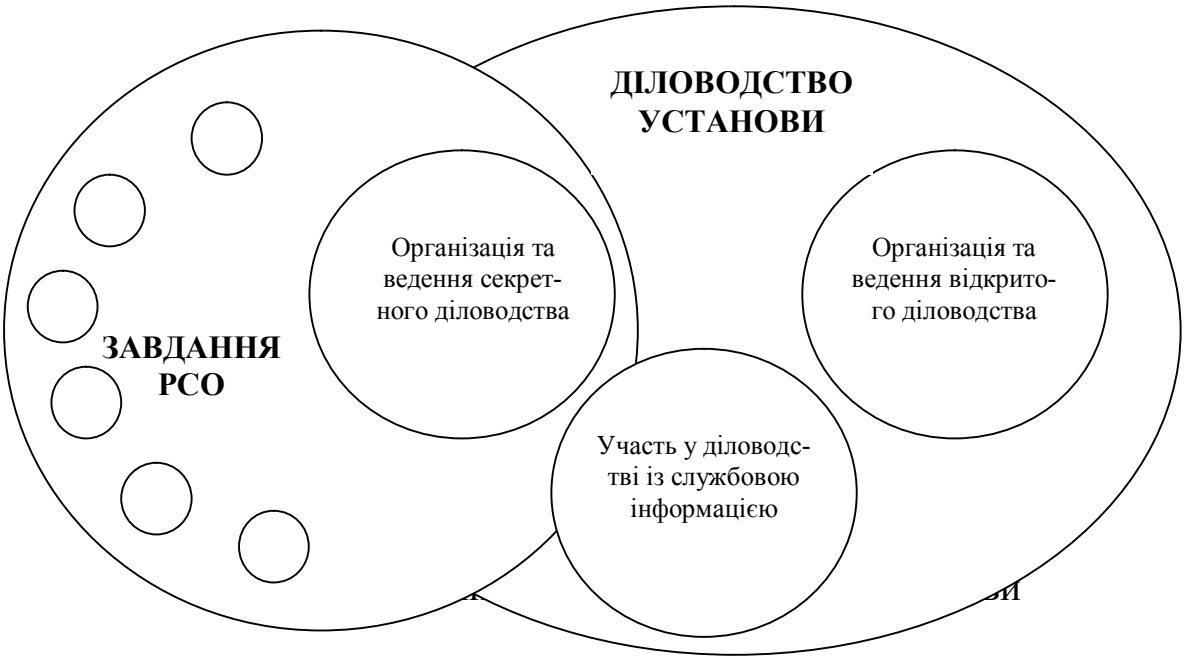
де E – ефективність управління діяльністю установи;

$n_i$ – і-та витрата для досягнення поставленої мети;

[1,К] – множина витрат для досягнення поставленої мети.

Витрати на організацію та здійснення діловодства входять до складу витрат для досягнення поставленої мети, у зв'язку з чим їх мінімізація буде сприяти підвищенню ефективності управління діяльністю установи.

Згідно із ст. 21 Закону України “Про державну таємницю” організація та ведення секретного діловодства – одне із семи основних завдань режимно-секретного органу установи (рис. 1).




Секретне діловодство, а також відкрите діловодство та діловодство із службовою інформацією становлять систему діловодства установи. Кожна складова діловодства регламентується окремим нормативно-правовим актом [3, 4], які в деяких питаннях дублюються, а в деяких суперечать один одному.

Відокремленість кожного з видів діловодства поряд із певним упорядкуванням створює і деякі незручності, а саме, стримує процеси розвитку, гальмує впровадження сучасних досягнень в управлінні діяльністю установи.

Тому при організації секретного діловодства в установах необхідно враховувати потреби в організації інших видів діловодства. При цьому постає питання організаційно-штатної структури, підпорядкованості сектору секретного діловодства, узгодженості з іншими структурними підрозділами.

## ЛІТЕРАТУРА

1. Організація планування роботи режимно-секретних органів : навч.-метод. посіб. / А.І.Підлісний, І.В.Пішко, С.О.Князєв, О.А.Колесник. – К. : Вид-во НА СБ України, 2003. – 75 с.

2. Електронне діловодство : навч.-метод. посіб. для студентів денної та заочної форми навчання зі спеціальності 7.050102 “Економічна кібернетика” / О.В.Шпортько, В.В.Ступницький, Л.В.Шпортько, Н.І.Ступницька; / за ред. О.В.Шпортька. – Рівне : РДГУ, 2006. – 88 с.

3. Типова інструкція з діловодства у центральних органах виконавчої влади, Раді міністрів Автономної Республіки Крим, місцевих органах виконавчої влади, затверджена постановою Кабінету Міністрів України від 30.11.2011 р. № 1242 // Офіційний вісник України. – 2011 р., № 94. – Ст. 3433.

4. Інструкція про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію, затверджена постановою Кабінету Міністрів України від 27.11.1998 р. № 1893 // Офіційний вісник України. – 2011. – № 94. – Ст. 3433.

*Мервінський О.І.,*
*кандидат технічних наук,*
*Голова Державної служби України*
*з питань захисту персональних даних*

*Мельник К.С.,*
*заступник начальника управління юридичного забезпечення,*
*Державна служба України з питань захисту персональних даних*

## РОЗВИТОК ПРАВОВОГО РЕГУЛЮВАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В УКРАЇНІ

З моменту здобуття незалежності Україною було обрано орієнтир на побудову демократичної, правової держави, найвищою соціальною цінністю якої є людина, її життя і здоров'я, честь та гідність, недоторканність і безпека. Право на недоторканність приватного життя, зокрема на захист персональних даних, є одним із невід'ємних особистих немайнових прав сучасної людини в Україні, гарантованих міжнародними стандартами у галузі захисту прав людини та Конституцією України.

У зв'язку з поширенням та використанням інформаційних технологій у XX-XXI століттях, методів автоматизованого оброблення даних, формуванням глобальних інформаційних систем перед світовою спільнотою гостро постало питання постійного удосконалення правового та технічного регулювання захисту приватного життя людини. З одного боку, всі переваги вільного доступу до інформації забезпечують особі реалізацію одного з головних її прав – на свободу інформації, а ведення масштабних автоматизованих баз даних суттєво полегшує особі доступ до різного роду матеріальних та не-

матеріальних благ, до послуг цифрового ринку: від використання платіжних банківських карток до дистанційного замовлення різного роду соціальних послуг. З іншого боку, широке використання персональних даних органами державної влади, комерційними та громадськими організаціями суттєво збільшує ризик незаконного доступу певних осіб до приватного життя людини, а отже, створює загрозу порушення права людини на недоторканність приватного життя та захист персональних даних.

До 2010 року в України здебільшого різні аспекти порушеної проблематики розглядались у межах конституційного, частково – інформаційного та міжнародного права.

Конституцією України гарантовані основні права та свободи людини і громадянина. Так, статтями 31, 32 та 34 кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції, ніхто не може зазнавати втручання в особисте і сімейне життя, крім деяких випадків, передбачених Конституцією України, кожному гарантується право на свободу думки і слова, вільне вираження своїх поглядів і переконань [1]. Згадані положення Конституції України знаходили своє впровадження в законодавстві України, зокрема в законах "Про інформацію", "Про захист інформації в інформаційних та телекомунікаційних системах", "Про адвокатуру", "Про банки та банківську діяльність", Основах законодавства України про охорону здоров'я, Цивільному кодексі України, Кодексі законів про працю та інших нормативно-правових актах. Проте цьому процесу бракувало системності.

Прийняття 1 червня 2010 року Закону України "Про захист персональних даних", що набув чинності 1 січня 2011 року [2], ратифікація Верховною Радою України у липні 2010 року Конвенції Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до неї щодо органів нагляду та транскордонних потоків даних, створення спеціального уповноваженого органу у сфері захисту персональних даних (Державної служби України з питань захисту персональних даних) стало важливим етапом підвищення ефективності системи захисту персональних даних в Україні як у правовому, так і інституційному значенні.

З метою встановлення відповідальності за порушення законодавства України у сфері захисту персональних даних Верховною Радою України 2 червня 2011 року прийнято Закон України "Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних даних", який набув чинності 01.07.2012 р.

Протягом 2011 року прийнято низку підзаконних актів у сфері захисту персональних даних, направлених на належне урегулювання питання функціонування Державної служби України з питань захисту персональних даних, Державного реєстру баз персональних даних, визначення порядку здійснення державного нагляду та контролю за додержанням вимог законодавства у сфері захисту персональних даних тощо.

На саміті Україна – ЄС, що відбувся 22 листопада 2010 р. у м. Брюсселі, Україна отримала від Євросоюзу План дій щодо лібералізації Європейським Союзом візового режиму для України (далі – План дій). Однією з вимог ЄС до України відповідно до Плану дій є прийняття відповідного законодавства про захист персональних даних та створення незалежного наглядового органу у сфері захисту персональних даних, а також імплементація Закону України "Про захист персональних даних" та забезпечення ефективного функціонування незалежного наглядового органу з питань захисту персональних даних, у тому числі шляхом передбачення необхідних фінансових і людських ресурсів. Створення дієвої вітчизняної системи захисту персональних даних є також передумовою для укладення Україною угоди про співробітництво з Європейською організацією з питань юстиції (Євроюст) та угоди про оперативне співробітництво з Європейським поліцейським офісом (Європол).

У листопаді 2011 року відбулись експертні місії в Україну Європейської комісії та Євроюсту з метою обстеження поточного функціонування уповноваженого органу України з питань захисту персональних даних (ДСЗПД). За результатами цих місій було надано звіти, в яких серед основних питань, які потребують подальшого вирішення, згадувались такі:

– внесення змін до Закону України "Про захист персональних даних" на основі рекомендацій європейських експертів;

– забезпечення незалежності уповноваженого органу України з питань захисту персональних даних.

Верховною Радою України 20 листопада 2012 року прийнято Закон України №5491-VI "Про внесення змін до Закону України "Про захист персональних даних", який вступив у силу 20 грудня 2012 року.

Зазначений Закон розроблено з метою удосконалення правового регулювання у сфері захисту персональних даних відповідно до рекомендацій Європейської комісії, Євроюсту та Ради Європи. Його спрямовано на зміну сфери дії Закону України "Про захист персональних даних" і визначено, що його дія поширюється на всі дії з оброблення персональних даних, а не тільки в базах персональних даних.

Серед основних завдань потребує урегулювання відповідно до рекомендацій ЄС питання незалежності уповноваженого органу із захисту персональних даних.

На розгляді Верховної Ради України знаходяться декілька законопроектів (реєстраційні номери 2282, 2282-1, 2282-2), покликаних урегулювати питання удосконалення інституційної системи захисту персональних даних, зокрема забезпечення ефективного функціонування незалежного наглядового органу з питань захисту персональних даних. Це значною мірою сприятиме реалізації Національного плану з виконання Плану дій щодо лібералізації Європейським Союзом візового режиму для України.

## ЛІТЕРАТУРА

1. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/254%D0%BA/96 %D0%B2%D1%80

2. Закон України від 01.06.2010 № 2297-VI "Про захист персональних даних" [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/2297-17.

*Настюк В.Я.,*
*доктор юридичних наук, професор,*
*Науково-дослідний інститут інформатики і права*
*Національної академії правових наук України*

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

## ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ: КОНЦЕПТУАЛЬНІ ПІДХОДИ ДО ВИЗНАЧЕННЯ ТА КЛАСИФІКАЦІЇ

Українська держава посилює свою увагу до проблеми зміцнення та забезпечення інформаційної безпеки. Так, у Законі України "Про основи національної безпеки України" від 19.06.2003 р. № 964-IV відмічено, що "основними напрямами державної політики з питань національної безпеки України в інформаційній сфері є: забезпечення інформаційного суверенітету України; вдосконалення

державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури й ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну; активне залучення засобів масової інформації до запобігання і протидії корупції, зловживанням службовим становищем, іншим явищам, які загрожують національній безпеці України; забезпечення неухильного дотримання конституційного права громадян на свободу слова, доступ до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері й переслідування журналістів за політичні позиції; вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України".

Правовий аспект у системі забезпечення інформаційної безпеки виражається в наявності права на інформацію, правотворчості, реалізації права на доступ до інформації, контролі щодо законності у сфері інформаційних правовідносин тощо. Наразі цим питанням приділяють значну увагу науковці, серед яких слід відзначити І.В.Арістову, К.І.Бєлякова, О.П.Дзьобаня, А.І.Марущака, В.Г.Пилипчука, В.С.Цимбалюка та багатьох інших.

Слід відмітити, що будь-яка можлива небезпека стосовно охоронюваних законом інформаційних прав і свобод особи, інформаційних ресурсів держави, інформаційних інтересів суспільства тощо вбачається загрозою інформаційній безпеці у цілому. Під такою небезпекою розуміється передусім правопорушення, що є суспільно небезпечним, винним, протиправним діянням, яке завдає шкоди особі, власності, державі або суспільству в цілому. При цьому така можлива небезпека означає, що правопорушення цілком допускається або неодмінно може відбутися по відношенню до об'єкта інформаційної безпеки. Отже, за загальним визначенням загрози інформаційній безпеці доцільно розглядати як суб'єктивні наміри та об'єктивні можливості, що можуть бути представлені як види загроз.

Натомість загрози інформаційній безпеці можна класифікувати за різними підставами, або критеріями; життєво важливими інтересами людини в інформаційній сфері; правовими галузями, що забезпечують безпеку людини в інформаційній сфері. Наприклад, можна виділити такі види загроз інформаційній безпеці, як майнові, рейдерські, техногенні, медійні тощо.

Залежно від того, звідки виходять загрози, вони можуть бути розподілені на два великі класи: внутрішні й зовнішні. Це й розподіл значною мірою умовний, оскільки в одному випадку можуть домінувати внутрішні характеристики юридичного характеру, а в іншому – зовнішні. Наприклад, стосовно особи можна говорити про такі її внутрішні (внутрішньоособові) юридичні властивості, як правовий інфантилізм, нігілізм, протиправні орієнтації, установки тощо. Зовнішніми можна визначити загрози, що виходять від інших осіб, зважаючи на зловживання правом на інформацію, соціально-правову пасивність, ухилення від виконання певних обов'язків тощо.

Особливо гострою є сьогодні проблема загроз інформаційній безпеці людини, інформаційні права і свободи якої є вищою цінністю; їх визнання, дотримання і захист Конституцією України визначені як обов'язок держави.

Натомість інформаційна безпека – це ознака, що характеризує відсутність загрози людському співтовариству, певній групі людей, конкретному індивідууму і (або) навколишньому середовищу від використання засобів чи продуктів сучасної інформаційної технології.

Наразі намітилися дві тенденції у визначенні поняття і структури інформаційної безпеки. Прихильники гуманітарного напряму пов'язують інформаційну безпеку лише з інститутом таємниці. Представники органів сектору безпеки пропонують поширювати сферу інформаційної безпеки практично на усі питання й відносини в інформаційній сфері, тобто ототожнюють інформаційну безпеку з інформаційним середовищем.

Структуру інформаційної безпеки можна подати, як об'єкт інформаційної безпеки, загрози об'єкту, забезпечення інформаційної безпеки. Законодавчо загрози інформаційній безпеці України закріплені в Законі України "Про основи національної безпеки України", Указі Президента України "Про Стратегію національної безпеки України".

У науці виділяють також інформаційні, програмно-математичні, фізичні, радіоелектронні, організаційно-правові загрози інформаційній безпеці. Науковці неодностайні, класифікуючи загрози інформаційній безпеці. Так, одні автори усі загрози інформаційній безпеці поділяють на природні та штучні. Серед штучних виділяють ненавмисні й навмисні. Останні класифікують на внутрішні і зовнішні, а зовнішні, у свою чергу, поділяють на локальні та віддалені атаки. Дослідження учених у сфері інформаційного протиборства показали, що останній вид боротьби стає якщо не основним, то вирішальним у XXI столітті.

З метою запобігання і нейтралізації загроз інформаційній безпеці застосовуються правові, програмно-технічні, організаційно-економічні методи. Правові методи передбачають розроблення і реалізацію комплексу нормативно-правових актів, що регламентують інформаційні відносини в суспільстві, а також забезпечують інформаційну безпеку. Зокрема, слід виділити Закон України від 04.02.1998 р. № 75/98-ВР "Про Концепцію Національної програми інформатизації" та Указ Президента України від 08.07.2009 р. № 514/2009 "Про Доктрину інформаційної безпеки України", де простежується серед інших принципів забезпечення інформаційної безпеки принцип настання юридичної відповідальності за порушення законодавства про інформацію.

Програмно-технічні методи включають застосування різних технічних засобів захисту інформації під час її передачі та обігу по каналах зв'язку.

Організаційно-економічні методи передбачають формування системи захисту секретної й конфіденційної інформації за допомогою їх сертифікації, ліцензування, стандартизації на відповідність вимогам інформаційної безпеки.

У зв'язку з проведенням в Україні адміністративної реформи, істотними змінами в організації місцевого самоврядування усе більш виявляються проблемні питання інформатизації. В адміністративно-територіальних одиницях України починають реалізовуватися програми інформатизації місцевих органів влади шляхом їх підключення (об'єднання) в єдину (локальну) мережу органів влади держави. Забезпечення доступу до баз даних органів влади, електронний обмін різного роду інформацією (ділове листування, кореспонденція, нормативно-правові акти тощо) вимагають забезпечення безпеки проходження такої інформації через канали зв'язку, недопущення несанкціонованого доступу до неї, а також її модифікації або знищення.

Інформаційні технології усе більше зачіпають судову систему України. Так, фахівці у сфері інформаційного права уважають, що справи, пов'язані з інформаційними технологіями, необхідно виділити в окрему категорію і вирішити питання про створення спеціальних колегій у судах, що спеціалізуються на питаннях інтелектуальної власності. Судді, які працюватимуть у подібних колегіях, повинні мати відповідну підготовку.

Таким чином, питання забезпечення інформаційної безпеки повинні неодмінно бути враховані при проведенні сучасної політики з питань забезпечення національної безпеки, а також новітніх процесів реформування в Україні економічної, адміністративної та судової сфер.

*Ожеван М.А.,*
*доктор філософських наук, професор,*
*заслужений діяч науки і техніки України,*
*Національний інститут стратегічних досліджень*

# НАЦІОНАЛЬНА КОНКУРЕНТНА РОЗВІДКА У ВИМІРАХ КОНКУРЕНТОСПРОМОЖНОСТІ КРАЇНИ ТА ЇЇ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Глобальна економічно-торговельна конкуренція "за правилами" зовсім не знімає, а ще більше загострює питання економічно-торговельних війн, у яких за необхідності відіграють далеко не останню роль різноманітні спецслужби.

Одним зі світових "правил" конкурентної боротьби є "економічна" або "конкурентна" розвідка (англ. "economic&competitive intelligence"), яка успішно поєднує відповідні зусилля вихідців із державних спецслужб ("безпекарів" та "силовиків") і знавців сучасних ринків ("маркетологів") та перетворилася упродовж останніх 30 років на Заході на важливий елемент прийняття рішень, стратегічного прогнозування та планування діяльності бізнесових компаній (корпорацій) в умовах гострої ринкової конкуренції. Така конкурентна розвідка стосується різноманітних операцій зі збору та аналізу інформації, необхідної для стратегічних оцінок реального стану і перспектив зовнішнього бізнесового довкілля, а також реальної й потенційної активності на різноманітних ринках компаній-конкурентів.

Синонімічний ряд до терміна "конкурентна розвідка" включає такі поняття: – "*менеджмент знань*" ("knowledge management");

– "*ринкова розвідка*" ("market intelligence");

– "*ринковий інсайт*" ("market insight");

– "*розвідка конкурента*" ("competitor intelligence");

– "*технічна розвідка*" ("technical intelligence");

– "*бізнес-розвідка*" ("business intelligence") тощо.

Водночас, деякі джерела не ототожнюють "конкурентну розвідку" з названими видами розвідувальної діяльності, а, навпаки, наголошують на їх відмінностях. При цьому підкреслюється, що "бізнес-розвідка", на відміну від "конкурентної розвідки", фокусується виключно на внутрішніх процесах у компанії, спрямованих на підсилення її ринкової конкурентоспроможності за посередництвом ліпшого усвідомлення ринкової ситуації та позиціонування конкурентів, удаючись при цьому до методів, не завжди етично виправданих.

Тобто у подібній інтерпретації "бізнес-розвідка" є майже тотожною *контррозвідувальній діяльності* й доменом "безпекарів" та

“силовиків”, вихідців із державних спецслужб, тоді як “конкуренту розвідку” в “чистому вигляді” вважають доменом діяльності “маркетологів”.

“Конкурентну розвідку” органічно доповнюють “культурна розвідка” й “культурне вимірювання” (“cultural intelligence” (CQ; CULTINT), які пропонують PR-підрозділам компаній різноманітні методи мінімізації репутаційних ризиків компаній, знешкодження “чорного піару” тощо.

Прототипом “конкурентної розвідки” сучасного типу став “*бенчмаркінг*” (англ. bench mark – “початок відліку”), свого часу започаткований компанією “Xerox”, яка, наштовхнувшись на конкуренцію з боку японських виробників, створила методику об’єктивного зіставлення прийомів і способів своєї діяльності для завоювання ринків із прийомами, способами й методами діяльності конкурентів, порівняла себе за низкою показників із провідними “гравцями” цього сегменту ринку. Зокрема, “HR – бенчмаркінг” стосується нині управління людськими ресурсами (HR – human resourses) і зводиться до порівняльних оцінок витрат компанії на оплату праці, підвищення кваліфікації співробітників тощо.

Згодом до “бенчмаркінгу” долучилися пристосовані в максимально можливому обсязі до світу бізнесу розвідувальні технології:

– “*профілювання конкурентів*” (“competitor profiling”);

– “*стратегічна розвідка й раннє попередження*” (“strategic & early warning & -reconnaissance”);

– “*розвідка даних щодо клієнтів компанії*” (“customer intelligence”);

– “*дейт-майнінг*” (“data mining”);

– “*моніторинг та аналіз соціальних мереж*” (“social media monitoring & analysis”) тощо.

На жаль, Україна поки що належить до того кола держав, які навчилися “планувати власне майбутнє”, оволодівати на національному рівні стратегіями конкурентної боротьби в глобалізованому світі та ефективно цим стратегіям опонувати, якщо вони виходять від країн-конкурентів. Щоправда, усе це не заважає Україні посідати достойні позиції у найрізноманітніших рейтингах міжнародних організацій, які за різними критеріями визначають конкурентоспроможність країни. Утім, подібними рейтингами не слід втішатися, бо вони дуже рідко відображають об’єктивну ситуацію, а радше мають пропагандистське, маніпулятивне значення, оскільки акцент робиться на окремих суто формальних аспектах, без їх поглибленого аналізу.

Зокрема, Швейцарська бізнес-школа IMD-Lausanne проголосила у травні 2013 року поліпшення рівня міжнародної конкурентосп-

роможності України, оскільки в новому глобальному рейтингу цієї структури Україна піднялася відразу на сім пунктів – до 49-го місця (роком раніше додавши собі лише одну позицію) у загальному списку із 60 країн. Тепер Україна розташовується між Колумбією (48) та Угорщиною (50). У цьому рейтингу враховуються чотири критерії: ефективність економіки, якість роботи органів влади, ефективність бізнесу та рівень інфраструктури [10].

Зростання конкурентоспроможності України фіксує й аналогічний рейтинг Всесвітнього економічного форуму (ВЕФ), у якому враховується більш широкий спектр критеріїв. В останньому звіті ВЕФ, оприлюдненому у вересні 2012 року, Україна піднялася з 82-го на 73-е місце (із 144 держав). У рейтингу Doing Business Україна піднялася аж на 15 позицій. Щоправда, уся ця позитивна динаміка є докризовою, тобто відображає з певним запізненням стан, який передував спадові української економіки, що розпочався у другому півріччі 2012 року [10].

Економічна розвідка національного рівня – це добре відпрацьовані розвиненими країнами світу механізми взаємодії політичної й економічної розвідки, які дозволяють співробітникам державних розвідок (“спецслужб”) отримувати інформацію розвідувального змісту від співробітників служб конкурентної розвідки бізнесових (корпоративних) структур й, навпаки, у необхідних випадках ділитися з ними інформацію, яка дозволить приватним транснаціональним структурам отримувати конкурентні переваги на світових ринках.

Альянс “ТНК – національні спецслужби” є парадоксальним тільки на перший погляд. Мовляв, інтереси корпорацій виходять за межі національних держав, бо вони “транснаціональні” (транскордонні), тоді як державні спецслужби міркують категоріями національних кордонів. Насправді у глобалізованому світі неможливо забезпечити національні інтереси поза забезпеченням глобальних, транскордонних інтересів усіх належних до певної держави суб’єктів і передусім – ТНК. Звичайно, така точка зору поки що не є загальновизнаною навіть у розвинених країнах, але кількість її прибічників дедалі зростає, тоді як традиціоналісти мусять відступати. “Рицарям плаща й кинджалу” та “акулам світового імперіалізму” доводиться об’єднувати зусилля [7]. Саме тому й відбуваються невпинні процеси передачі державою своїх традиційних функцій (із розвідувальними й безпековими включно) приватним структурам.

Щодо США, то процесам державно-приватного партнерства в такій делікатній сфері, як розвідка, тут сприяють традиції переходу в бізнесові структури колишніх політиків та розвідників високого рівня, які, використовуючи свої попередні зв’язки й відому їм із на-

дійних джерел інформацію розвідувального змісту, звичайно застосовують увесь цей арсенал для лобіювання інтересів певної корпорації як усередині країни, так і за її межами з метою здобуття цією корпорацією конкурентних переваг.

Узагальнюючи подібний досвід державної розвідувально-інформаційної підтримки економічно-торговельної експансії національних фірм та корпорацій КНР й інших східно-азійських "тигрів", російські теоретики доходять логічного висновку, що між економічною та військовою думкою має відбутися зближення й одним із варіантів такого зближення є "конкурентна розвідка" [2].

Разом із тим, загальновизнаний той факт, що така "чутлива" сторона роботи американської розвідки, як зв'язок із великим бізнесом, коли його інтереси перетинаються з інтересами держави, а іноді й суперечать їм, постійно перебуває в "тіні". Це той "зворотний бік місяця" ("dark side of the moon"), про який наважуються говорити й писати лише сміливі журналісти, відставні співробітники розвідки й опозиційні політики. Жоден офіційний документ американських спецслужб, щодо стратегії розвідки й контррозвідки, матеріалів і доповідей аналітичного та прогностичного характеру, які регулярно виходять із надр розвідувального співтовариства США, ніколи безпосередньо не стосується теми співпраці державних та приватно-корпоративних розвідок [7]. Зате у США вистачає друкованих матеріалів на тему подібної розвідувальної співпраці в країнах-конкурентах, що переважно відносять до "недоброчесної конкуренції".

Зокрема, відповідно до викладених у роботі Марка Леонарда "*Про що думають у Китаї*" уявлень китайських "експертів" на цьому етапі розвитку КНР не може кинути виклик військовій могутності свого головного конкурента – США, – зате може успішно конкурувати зі Штатами, використовуючи дві інші групи методів – трансмілітарні та немілітарні, "зав'язані" на торгівлі, інвестиціях та експорті. Тому КНР надає, мовляв, такого значення розширенню виробництва "сірих" товарів, транскордонним злиттям та поглинанням, використанню наукового потенціалу китайської діаспори у США, активному промисловому шпигунству тощо. [6].

В оприлюдненому на початку 2013 року звіті американської фірми "Mandiant" із питань кібербезпеки безапеляційно сказано, що експерти фірми, проаналізувавши численні випадки спроб зламу електронних систем різних компаній і відомств США, дійшли висновку, що сліди зламів ведуть до Китаю, зокрема до розташованої в одному з районів Шанхаю 12-поверхової будівлі, у якій згідно з американськими даними розміщено китайський військовий спецпідрозділ 61398. Китайська сторона рішуче відкинула усі ці звинувачення і підозри на свою адресу [1].

У визначеннях конкурентної розвідки, які пропонують “Товариство професіоналів стратегічної й конкурентної розвідки” (“Strategic & Competitive Intelligence Professionals” (SCIP) та інші подібні професійні об’єднання, підкреслюється етична й легальна виправданість цієї інформаційної діяльності, що відрізняє її від “промислового шпигунства” (“industrial espionage”).

Першою ґрунтовною працею з “конкурентної розвідки” уважається книга Майкла Портера “*Конкурента стратегія: технології аналізу галузей та конкурентів*”, яка вперше вийшла друком у 1980 р. (Michael Porter “Competitive-Strategy: Techniques for Analyzing Industries and Competitors”, 1980).

Власне, питанням “*методики аналізу конкурента*” присвячений третій розділ цієї роботи, де пропонуються чотири “діагностичних компоненти”:

– *майбутні цілі;*

– *наявна стратегія;*

– *уявлення;*

– *потенційні можливості.*

Аналіз першого компонента має, за задумом автора, дати відповідь на запитання: “*Що рухає конкурентом?* ”. Аналіз другого присвячений пошуку відповіді на запитання: “*Що робить конкурент і на що він спроможний?*”.

Компонент “*уявлення*” стосується “*припущень конкурента*” стосовно самого себе й галузі. І, нарешті, компонент “потенційні можливості” присвячений аналізу *переваг та слабких сторін конкурента*. Синтетичне зведення усіх даних, які стосуються зазначених чотирьох компонентів, за задумом Майкла Портера, має дати “на виході” характеристику наступальних або оборонних дій конкурента на певному “полі битви” [8, с. 109-111].

До честі Майкла Портера, у спеціальному додатку до своєї праці він навів детальні переліки всіх інформаційних джерел, які підлягають аналізу, й принагідно дійшов слушного висновку щодо необхідності створення системної конкурентної розвідки: “Вочевидь, щоб отримати дані для всебічного аналізу, самої лише впертої праці недостатньо. Ефективний збір інформації потребує організованого механізму – своєрідної системи конкурентної розвідки” [8, с. 114].

Згодом, у 1990 р., М.Портер надрукував іншу фундаментальну працю – “*Конкурентні переваги країн*”, – у якій, по суті, поняття конкурентної розвідки вивів на національно-державний рівень [9].

Водночас доводиться констатувати, що слабкі конкуренті позиції вітчизняного бізнесу чітко корелюють із відсутністю інтересу ділових людей у просторі СНД до питань конкурентної розвідки.

Зокрема, про те, що більшість із них досі не усвідомила необхідність подібної діяльності, свідчать дані опитування, яке перманентно проводить казахський інформаційно-аналітичний портал конкурентної, економічної розвідки, бізнес-розвідки й аналітики SPY. KZ. Станом на 15.03.2013 із загальної кількості 1515 респондентів на запитання "Чи користуєтеся Ви послугами конкурентної розвідки? " лише 212 (14%) відповіли, що в їхніх бізнес-структурах є такі підрозділи; 108 (7,13%) заявили, що їхні бізнес-структури користуються послугами "сторонніх компаній". 326 (21,52%) уважають, що в конкурентній розвідці немає потреби. Більше половини від усіх опитаних респондентів – 869 (57,36%) – взагалі не знайомі з поняттям "конкурентна розвідка" [5].

Зазначені тенденції свідчать про те, що для вітчизняного бізнесу, який тільки-но виходить на міжнародні ринки і невпевнено почувається навіть на внутрішньому ринку, теза щодо невідворотності конкуренції ще не стала аксіомою. Вітчизняний бізнес успадкував чимало неправильних патерналістського плану уявлень про роль і значення держави в конкурентній боротьбі та все ще сподівається уникнути конкуренції на внутрішніх та зовнішніх ринках за рахунок або державного протекціонізму, або різноманітного "піратства", або "товарного патріотизму" вітчизняного споживача.

Однак із цими ілюзіями доводиться прощатися. Зокрема, після вступу України до СОТ й очікуваного підписання Угоди про асоціацію з ЄС поле протекціоністського маневру й "внутрішнього лобіювання", недоброчесної конкуренції тощо дедалі звужуватиметься. "Піратство", тобто грубі порушення прав інтелектуальної власності, випуск різноманітних "сірих" товарів, обертатиметься й уже обертається різноманітними міжнародними санкціями.

Зрештою, український споживач теж усе більше виявляється "антипатріотичним" і кволо реагує на заклики деяких політиків: "Будь українцем – купуй українське!". Впродовж останніх років українському бізнесу (як імпортерам, так і експортерам) довелося навіть розпрощатися з ілюзією виживання за рахунок запозиченого з арсеналу "рейганоміки" маніпулювання курсом національної валюти.

Усе зазначене має як у загальнонаціональному, так і в масштабі окремих виробництв, компаній, корпорацій тощо позитивний сенс, бо відмова держави від грубих методів утручання у функціонування різноманітних ринків на користь вітчизняних виробників чи учасників експортно-імпортних операцій підводить бізнес до усвідомлення необхідності модернізації та інноваційності як стабільних факторів конкурентних переваг, а також потреби "грати" за світовими правилами конкурентної боротьби. Одним із цих жорстких імперативних правил є економічна або конкурентна розвідка.

Тісні взаємозв'язок і взаємодія національної економіки й національної безпеки та оборони ще ніколи не були настільки очевидними, як у нинішню епоху глобалізації, коли національна економіка, яка бажає бути конкурентоспроможною, має перебувати у стані перманентної "війни" (або ж, іншими словами, гострої конкуренції) за ринки збуту й сировини, за інновації, доступ до фінансів, "мізки" талановитих співробітників тощо.

Не дивно, що така "війна" часто-густо перестає бути умовною метафорою й переростає у справжні торговельно-економічні війни без участі держав та їхніх блоків і коаліцій, що загрожує трансформацією у великі та малі (локальні) політичні війни, які також неможливі без потужної "економіки війни". Коло замикається. За нинішніх глобалізаційних умов жодна країна світу, задіяна у світовій ринковій конкуренції, не може дозволити собі такої "розкоші", як переведення економіки, за взірцем сталінського СРСР, на суто "воєнні рейки".

У стратегічному вимірі це означає необхідність підпорядкування політичної конкуренції країн потребам їхньої економічної конкуренції, адаптації до вітчизняних умов кращого світового досвіду пристосування, а в певних випадках – швидкісної переорієнтації ринковоорієнтованої економіки на економіку мобілізаційного типу.

## ЛІТЕРАТУРА


1. Америка обвиняет Китай в кибернападениях // Военно-промышленный курьер. – 2013. – № 8. – 27 февраля. – С. 3.
2. Бобылов Ю.А. "Третьи отделы" в условиях глобальной конкуренции / Ю.А.Бобылов // Атомная стратегия. – 2012. – № 69.
3. D'Aveni, Richard. Waking up to the New Era of Hypercompetition // The Washington Quarterly. – 1997 p. – 183–195.
4. Inkster, Nigel. Chinese Intelligence in the Cyber Age // Survival: Global Politics and Strategy. – Vol. 55. – 2013. – № 1. Pp. 45-66.
5. Информационно-аналитический портал SPY. Kz. [Електронний ресурс]. – Режим доступу : http://spy.kz/modules.
6. Леонард, Марк О чем думают в Китае. / Леонард Марк ; пер. с англ. – М. : АСТ, 2010. – 222 с.
7. Минакова Н.В. Американские спецслужбы и крупный бізнес / Н.В.Минакова, Н.Л.Семин // США – Канада. Экономика, политика, культура. – 2010. – № 2. – С. 45–63.
8. Портер Е. Майкл. Конкурентная стратегия: методика анализа отраслей и конкурентов / Майкл Е.Портер ; пер. с англ. – М. : Альпина Бизнес Букс, 2005. – 454 с.

9. Портер Е. Майкл. Конкурентные преимущества стран / Портер Е.Майкл. [Електронний ресурс]. – Режим доступу : http://www.seinstitute.ru/Files/Veh6-35_Porter.pdf

10. Украина по конкурентноспособности обогнала Колумбию. Рейтинг // Экономические известия. – 2013. – 31 мая.

*Панченко В.М.,*
*кандидат технічних наук,*
*старший науковий співробітник,*
*Національна академія Служби безпеки України*

## НОВЕЛИ ЗАКОНОДАВСТВА ЄС У СФЕРІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

З появою в інтернеті соціально орієнтованих інформаційно-комунікаційних сервісів (соціальних мереж, мікроблогів, блогів тощо), з одного боку, людство отримало якісно нові комунікаційні засоби, а з іншого – несподівані виклики, пов'язані із захистом персональних даних. Так, технології, які надають можливість об'єднати дані про користувача з різних інтернет-сервісів, визначити фізичне місцезнаходження користувача за його IP-адресою, створюють передумови для втручання у приватне життя особи.

Останнім часом постійно зростає кількість заяв до Європейського суду з прав людини, поданих проти відомих компаній, які надають соціальні інтернет-сервіси, в яких констатуються порушення законодавства ЄС у сфері захисту персональних даних [1–6]. Це свідчить про системний характер проблеми, пов'язаної з реалізацією захисту персональних даних в інтернет-сервісах. З метою її вирішення комісія Європейського Союзу з питань юстиції та громадянських прав (далі – Європейська комісія) розробила низку законодавчих ініціатив, які на сьогодні активно обговорюються науковцями, законодавцями та іншими зацікавленими суб'єктами.

Проблеми правового захисту персональних даних неодноразово висвітлювались у публікаціях зарубіжних та вітчизняних науковців Ф.Альбрехта, А.Гевлич, Ф.Рудинського, Е.Іщенко, А.Марущака, М.Шумила, В.Козака та інших. Однак питання реалізації права користувача інтернет-сервісу на захист його персональних даних досліджені недостатньо.

Метою нашого дослідження є аналіз проектів нових нормативно-правових актів ЄС у сфері захисту персональних даних та оцінка ефективності їх упровадження в умовах соціалізації інтернет-сервісів.

На сьогодні основним чинним нормативно-правовим актом ЄС щодо захисту персональних даних є Директива 95/46/ЕС "Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних", прийнята в 1995 році [7]. Вона була доповнена Директивою 97/66/ЄС "Стосовно обробки персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі" [8], Директивою 2002/58/ЄС "Про обробку персональних даних та захист таємниці сектора електронних комунікацій" [9], рішенням Framework 2008/977/JHA як загальним інструментом на рівні ЄС щодо захисту персональних даних у сфері співпраці правоохоронних органів і судової співпраці за кримінальними справами [10], Директивою 2009/136/ЄС, яка доповнює Директиву 2002/22/ЄС [11], рішенням ЄС № 2006/2004 "Про взаємодію національних органів, відповідальних за забезпечення виконання законів про захист споживачів" [12].

Згідно з останніми ініціативами від 25.01.2012 р. Європейська комісія запропонувала створити новий нормативно-правовий акт щодо захисту персональних даних, узявши за основу Директиву 95/46/ЄС [7]. За результатами діяльності відповідної робочої групи було розроблено: 1) нове положення про захист персональних даних, що посилює відповідальність приватних осіб, компаній та державних органів; 2) правила захисту персональних даних, що використовуються в інтересах попередження, розслідування, розкриття чи обвинувачення у скоєнні кримінальних злочинів, виконання кримінальних покарань, та щодо вільного руху таких даних [13].

Можна виділити такі основні новації: 1) запровадження інституту службовців із захисту персональних даних – контролерів, які мають здійснювати спостереження за виконанням нормативних вимог; 2) уведення "права бути забутим", яке передбачає, що кожна особа має право вимагати від контролера видалити власні дані та утриматись від подальшого їх поширення; 3) уведення "права на переміщення", яке надає суб'єкту даних право отримати копії персональних даних із метою подальшого використання для інших цілей; 4) уведення "права суб'єкта даних", яке передбачає інформування користувача у зрозумілій формі, як оброблення його персональні дані. Нові правила оброблення персональних даних поширюється на всі ресурси, якими користуються громадяни ЄС, незалежно від міс-

ця їхньої реєстрації. Крім того, законодавець зобов'язав сайти увести так зване правило приватності за замовчанням, яким передбачається, що користувачі соціальних мереж і сайтів повинні давати згоду на публікацію своїх персональних даних. Як механізм відповідальності запропоновано стягувати штраф із компаній-порушників у розмірі 2% від їх прибутків.

Із критикою нових правил виступили представники найбільших компаній, які надають інтернетні послуги, – Facebook, Google, Microsoft [9; 10]. Зокрема, на їх думку, реалізація "права бути забутим" становить загрозу свободі слова, оскільки новий порядок:

- містить обмеження на право суб'єкта даних видаляти власні дані в окремих випадках (наприклад, коли вони необхідні в інтересах розслідування злочинів);
- надає право на підставі звернення користувача видаляти дані, скопійовані з його профілю, з альбомів друзів без згоди останніх (наприклад, якщо друзі користувача скопіювали спільні фотографії й відмовляються їх видалити);
- надає право на підставі звернення користувача видаляти відомості про нього зі сторінок третіх осіб, навіть якщо ці відомості правдиві.

Натомість, на нашу думку, ризики, пов'язані із зберіганням надлишкової інформації про особу, є більш небезпечними, аніж загроза свободі слова. А під гаслом "загрози свободі слова" насправді лобіюються комерційні інтереси, які суперечать демократичним цінностям. Отже, проекти нормативно-правових актів ЄС, які визначають новий порядок оброблення персональних даних, слід підтримати.

## ЛІТЕРАТУРА

1. Facebook звинувачують у зборі особистих даних [Електронний ресурс] // Портал журналістів України. – Режим доступу : http://knuj.org/ua/partition.html?id=1145.

2. Facebook можуть оштрафувати за зберігання вилучених особистих даних [Електронний ресурс] // Дзеркало тижня. – Режим доступу : http://news.dt.ua/TECHNOLOGIES/facebook_mozhut_oshtrafuvati_za_zberigannya_viluchenih_osobistih_danih-90057.html?print.

3. Німеччина знову озброїлася проти Facebook [Електронний ресурс] // Портал Tochka.net. – Режим доступу : http://man.tochka.net/ua/41652-germaniya-vnov-opolchilas-protiv-facebook.

4. Баловсяк Н. Facebook знову звинуватили в порушенні приватності [Електронний ресурс] / Н.Баловсяк // Портал Tochka.net. – Режим доступу : http://man.tochka.net/ua/39584-facebook-snova-obvinili-v-narushenii-privatnosti/.

5. Приватне життя в мережі [Електронний ресурс] // Euronews. – Режим доступу : http://ua.euronews.net/programs/right-on/privatne-zhyttya-merezhi.

6. Дані приватні, правила державні: як захищають найбільші інтернет-ринки світу [Електронний ресурс] // Тиждень. – Режим доступу : http://tyzhden.ua/World/41235.

7. Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних : Директива 95/46/ЄС Європейського Парламенту і Ради від 24 жовтня 1995 року [Електронний ресурс]. – Режим доступу http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=994_242.

8. Стосовно обробки персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі : Директива 97/66/ЄС Європейського Парламенту і Ради від 15 грудня 1997 року [Електронний ресурс]. – Режим доступу : http://zakon1.rada.gov.ua/cgi-bin/laws.

9. Про обробку персональних даних та захист таємниці сектора електронних комунікацій : Директива 2002/58/ЄС Європейського Парламенту і Ради від 12 липня 2002 року [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/994_b34.

10. Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 ьber den Schutz personenbezogener Daten im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden [Електронний ресурс]. – Режим доступу : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32008F0977:EN:NO.

11. Директива 2009/136/ЄК Європейського Парламенту та Ради від 25 листопада 2009 р., яка доповнює Директиву 2002/22/ЄС про універсальні послуги та права користувачів стосовно електронних мереж зв'язку і послуг, Директиву 2002/58/ЄС про обробку персональних даних та захист таємниці сектору електронних комунікацій [Електронний ресурс]. – Режим доступу : www.nkrz.gov.ua/img/zstored/File/Directive_2009_136.doc.

12. Рішення (ЄС) № 2006/2004 про взаємодію національних органів відповідальних за забезпечення виконання законів про захист споживачів [Електронний ресурс]. – Режим доступу : www.nkrz.gov.ua/img/zstored/File.

13. Proposal for a regulation of the european parliament and of the councilon the protection of individuals with regard to the processing of personal

data and on the free movement of such data (General Data Protection Regulation) [Електронний ресурс]. – Режим доступу : http://ec.europa.eu/justice/data-protection/document/review2012/com_201.

14. Fleischer P. Foggy Thinking About the Right to Oblivion Privacy [Електронний ресурс] / Peter Fleischer. – Режим доступу : http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-to-oblivion.

15. Rosen J. The Right to Be Forgotten [Електронний ресурс] / Jeffrey Rosen. – Режим доступу : http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotte.

*Пашков А.С.,*
*кандидат філософських наук,*
*старший науковий співробітник,*
*Національна академія Служби безпеки України*

## ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ: ІНОЗЕМНИЙ ДОСВІД

Незважаючи на бурхливий розвиток технічної складової забезпечення правоохоронної діяльності в сучасних умовах, роль і значення конфіденційних джерел як класичного, ефективного та апробованого часом засобу негласного запобігання й розслідування злочинів постійно зростає. Використання конфідентів є важливим напрямом у боротьби зі злочинністю, спрямованим на отримання якісної, достовірної та найбільш повної інформації щодо її проявів. Робота з конфіденційними джерелами – одна з головних складових діяльності правоохоронних органів та необхідна умова їх інформаційного забезпечення.

Керівники поліцейських служб у розвинених країнах виходять із того, що, поряд з іншими спеціальними методами, використання конфіденційних джерел є найбільш ефективною “зброєю” у боротьбі з організованою злочинністю, корупцією та терористичними організаціями. Саме у цих сферах від конфідентів надходить основний обсяг найціннішої інформації. Тому якісне функціонування правоохоронних органів, адекватність їх протидії сучасним викликам і загрозам безпосередньо залежать від інформаційного забезпечення, здійснюваного за участю конфіденційних джерел, та соціально-правових гарантій їх безпеки й діяльності.

Із початку XVIII століття у Британії, ще до створення постійної поліцейської системи, діяла, кажучи сучасною мовою, програма "Зроби для себе". Суть її полягала в тому, що кожний підданий мав можливість самостійно передати правосуддю злочинця, розраховуючи при цьому на частину повернутого викраденого майна або іншу винагороду. Вроджена повага до закону більшості громадян дозволяє сьогодні широко використовувати у розвинутих країнах такі стандартні поліцейські програми, як, наприклад, канадські "Сусідський догляд" або "Схопи за руку". Ідея останньої полягає в тому, що будь-який мешканець Оттави, помітивши дії особи, які здалися йому підозрілими, може зателефонувати до поліції та розповісти про свої підозри. Якщо вони виявляться виправданими й приведуть до арешту злочинця, джерело інформації одержує матеріальну винагороду. При цьому гарантується повне інкогніто, що мінімізує побоювання з приводу можливої помсти злочинця: належну суму можна отримати у банку, назвавши індивідуальний номер, який видається особі-заявнику в поліції.

Століттями глибоко вкорінені в японському суспільстві дисципліна, конформізм і корпоративні традиції дозволяють поліції та спецслужбам цієї країни розраховувати на конфіденційне інформаційне сприяння практично кожного громадянина.

Власним шляхом пішла Грузія, в якій поліцейські та контррозвідувальні органи об'єднані в одну державну структуру. Кожен громадянин країни, який добровільно заявить про свої протиправні контакти зі спецслужбами іншої держави та надасть допомогу правоохоронним органам, звільняється від кримінальної відповідальності.

Інший тип правосвідомості, з характерними рисами правового нігілізму, українці успадкували значною мірою від росіян завдяки багатовіковій спільній історії (традиція приховування від влади порушників і злодіїв, співчуття й допомога арештантам).

Із цього приводу ще у 1902 році влучно висловився завідувач закордонною агентурою Департаменту поліції Російської імперії, наш земляк, уродженець Херсонщини, П.І.Рачковский. Зокрема, він відмітив, що навіть в офіційних сферах укорінилися забобони проти агента як продажної, аморальної й зрадницької особи. "У нас майже ніхто не схильний бачити в агенті особу, яка виконує скромний обов'язок перед батьківщиною всупереч, наприклад, французам або англійцям, котрі як приватні особи самі допомагають поліції у розкритті злочинів і прилюдно пишаються кожним таким випадком, що дає їм можливість виконати цей патріотичний обов'язок. Таким чином, при бесідах із новими агентами необхідно найбільше переконувати їх, що вони аж ніяк не знехтувані шпигуни, а лише свідомі

прихильники Уряду, котрі борються із пройдисвітами, які зазіхають на спокій, честь і національну гідність".

Законодавча і судова влади розвинутих країн також постійно й активно підтримують зусилля із посилення інституту конфідентів, які посідають значне місце у поліцейських операціях.

Верховний суд США незмінно підкреслює право поліції отримувати інформацію із задіянням інформаторів. "Використання таємних інформаторів чи агентів, – зазначається в одному з рішень цього органу, – є законною та правильною практикою виконання закону й виправдано інтересами держави" (Laird v. Tatum. 408 U.S. 12 (1972) .

Цікавими в контексті забезпечення безпеки джерела інформації та створення умов для отримання оперативно важливих даних є й інші унормовані положення, що визначають організацію діяльності ФБР. Відповідно до "Вказівок генерального прокурора США по секретним операціям ФБР" від 1987 року "секретний агент" – це штатний співробітник, працюючий у певному розслідуванні під керівництвом і контролем ФБР, чиї відносини з Бюро під час операції приховуються від третіх осіб шляхом використання вигаданих установчих даних. "Таємна операція" – операція негласного розслідування, в якій використовується "секретний агент". У важливих операціях зазвичай допускається участь "секретних агентів" та інформаторів. Нерідко інформатор уводить до організації секретного агента, який виступає у відповідній ролі. "Таємна операція", як правило, закінчується судовим процесом за участю секретного агента як головного свідка обвинувачення.

Аналогічні методи застосовує й французька поліція. Зокрема співробітники "Бригад розшуку і захоплення" співробітники здійснюють спостереження за злочинним середовищем ізсередини. Практикою швейцарських правоохоронців в останні роки стало використання поряд зі звичайними агентами штатних співробітників поліції, яких називають "кротами". Угорська поліція має у своєму розпорядженні підрозділи глибоко законспірованих співробітників, спеціально підготовлених для роботи у злочинній сфері. Оперативна діяльність кримінального відділу Гамбурзького поліції ґрунтується на використанні так званих "прикритих співробітників" у криміногенному середовищі. Подібно діють спеціальні й поліцейські служби інших країн.

Один із важливих принципів конфіденційного співробітництва, який використовується поліцейськими службами у розвинених країнах, полягає в тому, щоб особи, які залучені до такого співробітництва, мали довіру до правоохоронних органів. Основою такої довіри

є правові та законодавчі гарантії, які жорстко й постійно підтримуються правоохоронними інститутами держави. Тому, забезпечуючи надійний захист відомостей стосовно конфіденційних джерел та отриманої від них інформації, держава може бути впевнена у якісному інформаційному забезпеченні правоохоронної діяльності відповідних органів і підрозділів.

*Петров С.Г.,*
*Національна академія Служби безпеки України*

## ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ДЕРЖАВИ У БАНКІВСЬКІЙ СФЕРІ

Питання інформаційної безпеки різноманітних суб'єктів досліджувалося як представниками юридичної науки, так і дослідниками інших наук. Предметом наукових пошуків виступають проблеми забезпечення інформаційної безпеки людини як споживача телекомунікаційних послуг у контексті дотримання балансу інтересів держави, суспільства та людини в цій сфері [1]. Дослідники державного управління розглядають також політико-правові механізми управління інформаційно-психологічною безпекою України [2], представники філософської науки здійснюють дослідження інформаційної безпеки України як складної, динамічної, цілісної системи, компонентами якої є підсистеми безпеки особи, держави та суспільства [3].

Звернімо увагу на інформаційну безпеку держави в такій складній і неоднозначній сфері суспільних відносин, як банківська система.

На перший погляд, питання забезпечення інформаційної безпеки в банківській сфері стосуються таких суб'єктів, як комерційні банки. На підтвердження актуальності подібного підходу свої роботи публікували А.І.Марущак щодо структури та системи забезпечення інформаційної безпеки банківської установи [4], І.Г.Пугачов – у контексті інтеграції електронного бізнесу у внутрішньобанківські інформаційні системи комерційного банку [5], С.М.Яременко – стосовно включення інформаційної безпеки до системи економічної безпеки діяльності банків [6] та інші дослідники. Однак поза увагою залишилися питання визначення загроз інформаційній безпеці держави у банківській сфері.

Національний банк України (НБУ) як основний регулятор банківської системи у 2010 році затвердив два стандарти, пов'язані із системою управління інформаційною безпекою [7], які побудовані

на кращих світових практиках і у яких визначено методику оцінювання ризиків відповідно до стандартів НБУ. У стандартах використовується поняття "ризик інформаційної безпеки", під яким розуміється ймовірність того, що визначена загроза, впливаючи на вразливості ресурсу або групи ресурсів, може спричинити шкоду банку.

Однак у цих стандартах відсутні системні загрози, характерні для інформаційної безпеки держави.

Закон України "Про банки і банківську діяльність" також обмежується рівнем банку в контексті регулювання загроз (ризиків) інформаційної безпеки: банк зобов'язаний з урахуванням специфіки його роботи створити адекватну систему управління ризиками, яка має забезпечувати на постійній основі виявлення, вимірювання, контроль і моніторинг усіх видів ризиків за всіма напрямами діяльності банку на всіх організаційних рівнях та відповідати ризикам, що приймаються банком; …утворити постійно діючий підрозділ з управління ризиками, в якому зосереджені функції з управління ризиками та який відповідає за розроблення, впровадження внутрішніх положень і процедур управління ризиками, інформує керівництво про ризики, прийнятність їх рівня та надає пропозиції щодо необхідності прийняття керівництвом відповідних рішень [8, ст. 44].

НБУ відповідно до Конституції України забезпечує стабільність грошової одиниці України, при цьому виходить із пріоритетності досягнення та підтримання цінової стабільності в державі [9]. Разом із тим, Закон України "Про Національний банк України" визначає перелік функцій, безпосередньо пов'язаних із інформаційною безпекою держави. Більшість із них були віднесені до функцій НБУ у 2012 році [10, 11]:

– регулює діяльність платіжних систем та систем розрахунків в Україні, визначає порядок і форми платежів, у тому числі між банками;

– визначає напрями розвитку сучасних електронних банківських технологій, створює та забезпечує безперервне, надійне й ефективне функціонування, розвиток створених ним платіжних та облікових систем, контролює створення платіжних інструментів, систем автоматизації банківської діяльності та засобів захисту банківської інформації;

– визначає особливості функціонування банківської системи України в разі уведення воєнного стану чи особливого періоду, здійснює мобілізаційну підготовку системи Національного банку;

– здійснює методологічне забезпечення з питань зберігання, захисту, використання та розкриття інформації, що становить банківську таємницю;

– визначає порядок здійснення в Україні маршрутизації, клірингу та взаєморозрахунків між учасниками платіжної системи за операціями, які здійснені в межах України із застосуванням платіжних карток, емітованих банками-резидентами;

– створює Засвідчувальний центр для забезпечення реєстрації, засвідчення чинності відкритих ключів та акредитації центрів сертифікації ключів, визначає порядок застосування електронного підпису, у тому числі електронного цифрового підпису в банківській системі України та суб'єктами переказу коштів;

– веде реєстр платіжних систем, систем розрахунків, учасників цих систем та операторів послуг платіжної інфраструктури;

– здійснює нагляд – (оверсайт) платіжних систем і систем розрахунків.

Ці функції безпосередньо пов'язані з інформаційною безпекою держави, тому можемо визначити загрози, які негативно впливатимуть на стабільність банківської системи і виникають у сферах розвитку сучасних електронних банківських технологій: платіжних систем, систем розрахунків, обігу платіжних карток, електронного документообігу й використання електронного цифрового підпису в банківській системі України, систем автоматизації банківської діяльності та засобів захисту банківської інформації, а також при мобілізаційній підготовці системи Національного банку.

Визначенню загроз інформаційній безпеці держави в банківській сфері також сприятиме аналіз концептуальних документів із питань забезпечення національної безпеки у фінансовій сфері [12].

Розвиток і розширення спектра фінансових послуг створюють умови для активного залучення до ринків таких послуг споживачів, які зазвичай не мають достатньої інформації та необхідних знань про особливості й споживчі характеристики фінансових послуг. У процесі вибору послуги зазначені споживачі не завжди можуть оцінити рівень ризиків і ймовірні наслідки набуття додаткових фінансових зобов'язань та порівняти умови їх надання, що пропонуються банківськими установами.

Як показує досвід інших держав, стрімкий розвиток пропозицій ринків фінансових послуг в умовах недостатнього рівня забезпечення захисту прав споживачів може призвести до недовіри до таких ринків і, як наслідок, зниження попиту на пропоновані ними послуги.

Водночас недовіра населення до ринків фінансових послуг не дає можливості активно використовувати його вільні кошти як інвестиційні ресурси, що спрямовуються на розвиток економіки [12].

Таким чином, недостатність інформації та необхідних знань споживачів про особливості й споживчі характеристики фінансових

послуг також визнається загрозою безпеці держави в банківській сфері. Убачається, що така загроза має суто інформаційний характер.

## ЛІТЕРАТУРА


1. Сулацький Д.В. Організаційно-правові засади забезпечення інформаційної безпеки людини як споживача телекомунікаційних послуг : автореф. дис. ... канд. юрид. наук : 12.00.07 / Д.В.Сулацький ; Міжнар. ун-т бізнесу і права. – Херсон, 2011. – 20 с.
2. Коваль З.В. Політико-правові механізми державного управління інформаційно-психологічною безпекою України : автореф. дис. ... канд. наук з держ. упр. : 25.00.02 / З.В.Коваль ; Одес. регіон. ін-т держ. упр., Нац. акад. держ. упр. при Президентові України. – О., 2011. – 20 с.
3. Триняк В.Ю. Інформаційна безпека як соціокультурний феномен (соціально-філософський аналіз) : автореф. дис... канд. філософ. наук : 09.00.03 / В.Ю.Триняк ; Дніпропетр. нац. ун-т ім. О.Гончара. – Д., 2009. – 19 с.
4. Марущак А.І. Інформаційна безпека банківської установи: структура та система забезпечення / А.І.Марущак // Тези доповідей міжнародн. наук.-практ. конф., м. Севастополь, 1–2 жовтня 2010 року) / Державний вищий навчальний заклад "Українська академія банківської справи НБУ". – Суми : ДВНЗ "УАБС НБУ", 2010. – С. 21–24.
5. Пугачов І.Г. Моделювання процесів інтеграції електронного бізнесу в структуру комерційного банку : автореф. дис... канд. екон. наук: 08.00.11 / І.Г.Пугачов ; Донец. нац. ун-т. – Донецьк, 2007. – 20 с.
6. Яременко С.М. Забезпечення економічної безпеки діяльності банків : автореф. дис. ... канд. екон. наук : 08.00.08 / С.М.Яременко ; Київ. нац. екон. ун-т ім. В.Гетьмана. – К., 2010. – 20 с.
7. Лист НБУ від 03.03.2011 р. № 24-112/365 "Щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України".
8. Закон України "Про банки і банківську діяльність" від 07.12.2000 року (зі змінами) // Відомості Верховної Ради України. – 2001. – № 5-6. – Ст. 30.
9. Закон України "Про Національний банк України" від 20.05.1999 року (зі змінами) // Офіційний вісник України. – 1999. – № 24. – Ст. 2.
10. Закон України від 18.09.2012 р. № 5284-VI "Про внесення змін до деяких законодавчих актів України щодо функціонування платіжних систем та розвитку безготівкових розрахунків" // Офіційний вісник України. – 2012. – № 79. – Ст. 3191.

11. Закон України від 06.12.2012 р. № 5518-VI “Про внесення змін до деяких законодавчих актів України щодо подальшого удосконалення адміністрування податків і зборів” // Офіційний вісник України. – 2013. – № 1. – Ст. 6.

12. Розпорядження Кабінету Міністрів України від 15.08.2012 р. № 569-р “Про схвалення Концепції забезпечення національної безпеки у фінансовій сфері” // Офіційний вісник України. – 2012. – № 62. – Ст. 2533.

*Петров В.В.,*
*кандидат політичних наук, доцент кафедри,*
*Національна академія Служби безпеки України*

## ЩОДО ПРОБЛЕМНИХ ПИТАНЬ ІМПЛЕМЕНТАЦІЇ КОНВЕНЦІЇ РАДИ ЄВРОПИ “ПРО КІБЕРЗЛОЧИННІСТЬ”

Термін “кібернетична злочинність” (або “кіберзлочинність”) увійшов у вітчизняне правове поле після приєднання нашої держави до Конвенції Ради Європи про кіберзлочинність (ратифікована постановою Верховної Ради України від 7 вересня 2005 року № 2824) [1], яка закладає основу та міжнародні механізми боротьби з цим суспільно небезпечним явищем.

Зокрема, Конвенцією визначені перелік протиправних дій, які становлять кіберзлочини, порядок обов’язкового збереження комп’ютерних даних та механізми міжнародної взаємодії при розслідуванні комп’ютерних злочинів, у тому числі термінові, порядок транскордонного доступу правоохоронних органів до інформації та даних, які перебувають під юрисдикцією інших країн. Увага в Конвенції також приділена забезпеченню конфіденційності запитів при одночасному неухильному дотриманні прав людини, передбачене створення цілодобової контактної мережі 24/7 для термінового обміну оперативною інформацією між компетентними органами країн – учасниць Конвенції (в Україні це Міністерство внутрішніх справ).

Указаний міжнародний документ став модельним для розроблення аналогічних документів у рамках АТЕС, Африканського Союзу тощо. Наразі до Конвенції приєдналися 44 країни – члени Ради Європи, а також США, Канада, ЮАР, Японія. Ще близько 15 держав та низка впливових міжнародних організацій мають статус спостерігачів [2]. Наведене свідчить, що Конвенція Ради Європи про кіберзлочинність поступово виходить за межі регіонального механізму та набуває універсального характеру.

Серед недоліків цього документа слід зазначити, що Конвенція не охоплює такі прояви кіберзлочинності, як кібершпіонаж та кібертероризм, які набувають в останні роки дедалі більшого поширення. Так, у 2002 році внаслідок потрапляння в систему міжбанківських електронних платежів Південної Кореї комп'ютерного вірусу "K-virus" протягом трьох діб була паралізована платіжна система країни й оголошено надзвичайний стан.

Під час відомих подій у травні 2007 року в Естонії було фактично паралізовано систему державного управління, оскільки 100% документообігу в державі здійснювалось в електронному вигляді. Тільки Естонське відділення Шведбанку зазнало збитків у сумі 70 млн євро.

Виникнення якісно нового рівня загроз провідні фахівці світу пов'язують із появою комп'ютерного вірусу "STUXNET", навмисне впровадження якого в підприємства ядерного комплексу Ірану суттєво загальмувало уведення в дію Бушерської АЕС та мало геополітичні наслідки [3].

Незважаючи на викладене, Конвенція Ради Європи про кіберзлочинність на сьогодні лишається дієвим механізмом міжнародного співробітництва у сфері боротьби з цим явищем. Активним учасником Конвенції є Україна. Водночас, наявні певні проблеми, пов'язані з неповною її імплементацією у вітчизняне законодавство. Так, передбачені Конвенцією обов'язки та права операторів і провайдерів телекомунікаційних послуг у сфері боротьби з кіберзлочинністю встановлені Законом України "Про телекомунікації" [4], а повноваження правоохоронних органів – Законом України "Про оперативно-розшукову діяльність" [5] та Кримінальним процесуальним кодексом [6]. Зокрема, ст. 39 Закону України "Про телекомунікації" встановлені обов'язки операторів і провайдерів телекомунікацій *"зберігати записи про надані телекомунікаційні послуги протягом року позовної давності, визначеного законом, та надавати інформацію про надані телекомунікаційні послуги в порядку, встановленому законом"*. Незважаючи на достатній термін збереження інформації (в Україні термін позовної давності – три роки) ускладнює застосування цієї норми в правоохоронній діяльності те, що закон, на жаль, не визначає які саме записи про надані телекомунікаційні послуги мають зберігатись.

Таким чином, нагальною для України є необхідність удосконалення чинної законодавчої бази (у т.ч. Кримінального процесуального кодексу, законів "Про телекомунікації", "Про банки та банківську діяльність", "Про захист інформації в інформаційно-телекомунікаційних системах" та ін.), зокрема щодо надання право-

охоронним органам повноважень із видачі обов'язкових до виконання приписів володільцями комп'ютерних даних (провайдерами й операторами телекомунікацій, іншими юридичними та фізичними особами), про термінове фіксування й подальше зберігання комп'ютерних даних, які потрібні для розкриття злочину, впродовж 90 днів із можливістю його продовження до 3 років, а також щодо встановлення вимог із надання провайдером телекомунікацій правоохоронним органам інформації для ідентифікації постачальників послуг і маршруту, яким було передано інформацію.

Кримінальнальний процесуальний кодекс, який набрав чинності 19 листопада 2012 р., також потребує узгодження з положеннями Конвенції РЄ "Про кіберзлочинність", зокрема у частині належної імплементації статей 17 – Термінове збереження і часткове розкриття даних про рух інформації; 19 – Обшук і арешт комп'ютерних даних, які зберігаються; 20 – Збирання даних про рух інформації у реальному масштабі часу; 21 – Перехоплення даних змісту інформації; 30 – Термінове розкриття збережених даних про рух інформації; 33 – Взаємна допомога у збиранні даних про рух інформації у реальному масштабі часу; 34 – Взаємна допомога у перехопленні даних змісту інформації.

Негласні слідчі дії, які відповідають зазначеним статтям Конвенції, передбачені чинним Кримінальним процесуальним кодексом, – ст. 263 "Зняття інформації з транспортних телекомунікаційних мереж", а також ст. 264 "Зняття інформації з електронних інформаційних систем" – та є різновидом втручання у приватне спілкування. Відповідно до ст. 246 Кодексу втручання у приватне спілкування проводиться виключно у кримінальному провадженні щодо тяжких або особливо тяжких злочинів. При цьому практично усі злочини, передбачені розділом XIV Кримінального кодексу (окрім ч. 2 ст. 361 та ч. 3 ст. 362), не є тяжкими.

Слід зазначити, що в процесуальному законодавстві багатьох країн - учасниць Конвенції є окремі норми, які установлюють особливий порядок перехоплення та розкриття інформації про рух даних у комп'ютерній системі під час розслідування кіберзлочинів, навіть якщо вони не тяжкі.

Інша проблема – відсутність у вітчизняному правовому полі базового визначення кіберзлочинності. Кібернетичну злочинність за аналогією із традиційною злочинністю можна визначити як сукупність кібернетичних злочинів і осіб, які їх вчинили, кібернетичний злочин (кіберзлочин) – як суспільно небезпечне винне діяння, що полягає у протиправному використанні інформаційних та комунікаційних технологій, відповідальність за яке встановлена законодав-

ством про кримінальну відповідальність. Обидва визначення є авторськими, оскільки у вітчизняному праві їх немає.

Оскільки, кіберзлочинність має глобальний характер і не визнає державних кордонів, а ступінь загроз, які існують наразі у світі й Україні високий, назріла нагальна потреба внести, з урахуванням світового досвіду, зміни до розділу XVI Кримінального кодексу України "Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів) [7], зміни до розділу XVI Кримінального кодексу України, доповнивши його статтями 361-3 та 362-1, які б встановлювали кримінальну відповідальність за "несанкціоноване втручання в роботу державних електронних інформаційних ресурсів або інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури" та "несанкціоновані дії з інформацією, яка оброблюється в державних електронних інформаційних ресурсах або інформаційних, телекомунікаційних, інформаційно-телекомунікаційних системах об'єктів критичної інфраструктури, вчинені особою, яка має право доступу до неї".

Слід зазначити, що реалізація вказаних пропозицій матиме позитивний ефект за умови побудови національної системи кібербезпеки, передбаченої Стратегією національної безпеки [8], яка дозволить забезпечити належний рівень захисту національної інформаційної інфраструктури від реальних та потенційних викликів і загроз. Нагальним є прийняття Стратегії кібернетичної безпеки, а також розроблення законопроекту "Про кібернетичну безпеку України".

## ЛІТЕРАТУРА

1. Закон України "Про ратифікацію конвенції про кіберзлочинність" // Відомості Верховної Ради України., – 2006. – № 5-6. – С. 71.

2. Бюро договоров Совета Европы [Электронный ресурс]. – Режим доступа : http://conventions.coe.int/Treaty/Commun/ChercheSig.asp? CL=RUS&CM=&NT=185&DF=&VL=. – Название с экрана.

3. Петров В.В. Щодо створення єдиної загальнодержавної системи протидії кіберзлочинності [текст]: / В.В. Петров // Информационные технологии и безопасность. Проблемы правового обеспечения кибербезопасности в современном мире : сборник научных трудов. – Вып. 11. – К. : ИПРИ НАН Украины, – 2011. – Вып. 11 – с. 108 – 115.

4. Закон України "Про телекомунікації" // Відомості Верховної Ради України. – 2004. – № 12. – С. 155.

5. Закон України "Про оперативно-розшукову діяльність" // Відомості Верховної Ради. – 1992. – № 39. – С. 572.

6. Кримінальний процесуальний кодекс України // Голос України. – 2012. – № 90-91 від 19.05.2012 р.

7. Кримінальний кодекс України // Відомості Верховної Ради України. – 2001. – № 25–26. – С. 131.

8. Указ Президента України "Про Стратегію національної безпеки України" № 105/2007 від 12.02.2007 р. // Офіційний вісник України. – 2007. – № 11. – С. 7.

*Політова А.С.,*
*кандидат юридичних наук,*
*Донецький юридичний інститут МВС України*

## ІНФОРМАЦІЙНИЙ ТЕРОРИЗМ ЯК ЗАГРОЗА НАЦІОНАЛЬНІЙ БЕЗПЕЦІ

Глобальне поширення інформаційно-комунікативних технологій дало поштовх розвитку принципово нового виду тероризму – інформаційного або кібертероризму.

Як відзначає К.С.Герасименко, "інформаційна епоха розширила сферу діяльності тероризму, що привело до появи "інформаційного тероризму", який визначається як злиття фізичного насильства зі злочинним використанням інформаційних систем, а також умисне зловживання цифровими інформаційними системами, мережами або їх компонентами з метою сприяння здійсненню терористичних операцій або акцій" [1].

Інформаційний тероризм як глобальне явище визнано під час проведення 56 сесії Генеральної Асамблеї ООН, коли було прийнято резолюцію "Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки" № 56/19. У цій резолюції зазначено, що поширення й використання інформаційних технологій та засобів стосується інтересів усього міжнародного співтовариства. Утім, як було зафіксовано у резолюції ООН, ці технології та засоби потенційно можуть бути використані з метою дестабілізації міжнародної безпеки як у військовій, так і цивільній сферах, спричинити поширення на міжнародному рівні такого явища, як інформаційний тероризм [2].

Водночас у резолюції було наголошено, що навіть з огляду на те, що інформаційні технології сприяють вільному потоку інформації, демократизації суспільства та економічному прогресу, не можна не визнати, що існують потенційні загрози неправомірного та несанкціонованого використання інформаційних технологій у різних сферах життєдіяльності держав, що створює загрозу для міжнародної безпеки [2]. Не стала винятком і національна безпека України.

До кібертероризму (інформаційного тероризму) належать: незаконне втручання в роботу електронно-обчислювальних машин, систем та комп'ютерних мереж, крадіжка, присвоєння, вимагання комп'ютерної інформації, організація вилученої атаки на інформаційні ресурси, закладки та розробки комп'ютерних вірусів, які здійснюють знімання, модифікацію або знищення інформації. Також для інформаційних актів характерні такі інструменти, як комп'ютерні віруси, логічні бомби, "троянські коні" та інше [3].

В Указі Президента України від 12 лютого 2007 року № 105 (у редакції Указу Президента України від 8 червня 2012 року № 389/2012) "Про рішення Ради національної безпеки і оборони України від 8 червня 2012 року "Про нову редакцію Стратегії національної безпеки України" у пункті 3 ("Безпекове середовище та актуальні загрози національним інтересам і національній безпеці України") зазначено: *"3.3. На тлі зростання викликів і посилення загроз національній безпеці зберігається невідповідність сектору безпеки і оборони України завданням захисту національних інтересів, що характеризується*.... нездатністю України протистояти новітнім викликам національній безпеці (явищам і тенденціям, що можуть за певних умов перетворитися на загрози національним інтересам), пов'язаним із застосуванням інформаційних технологій в умовах глобалізації, насамперед кіберзагрозам" [4].

Щодо кількості вчинених злочинів, то якщо простежити виявлення злочинів у сфері високих інформаційних технологій, за статистикою МВС України у 2005 р. було виявлено 615 злочинів, 2006 р. – 583, 2007 р. – 656, у 2008 р. – 691, 2009 р. – 707. Із наведених даних ми бачимо, що у 2006 році порівняно з 2005 роком спостерігається падіння виявлення, але уже у 2007 році показники перевищили дані 2005 та 2006 років і продовжили зростання у 2008 і 2009 роках [5].

Разом із тим, у 2010 році відповідно до статистичних даних МВС України було зареєстровано 190 злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, 2011 році – 131 злочин, а за 11 місяців 2012 року – 138 злочинів.

Так званим "електронним злочинам" присвячено розділ XVI Особливої частини Кримінального кодексу України "Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку". Утім, це лише шість статей, хоча проблема має глобальний характер. Тому з упевненістю можна констатувати той факт, що в Кримінальному кодексі України недостатньо приділяється увага

злочинам, пов'язаним із крадіжкою, присвоєнням комп'ютерної інформації, і залишаються поза увагою вимагання комп'ютерної інформації, а також інші суспільно небезпечні дії, спрямовані на вчинення інформаційного тероризму (кібертероризму).

Отже, ця проблема має глобальний характер не тільки через масштаби, але й тому, що жодна країна не може подолати її самостійно. Особливо це стосується розвинутих держав, бо їх залежність від нових інформаційних технологій найбільша. Із зростанням такої залежності збільшуються збитки, що у свою чергу збільшує загрозу національній безпеці. З погляду на глобальність проблеми, необхідні великі кошти для створення, постійного оновлення дієвих систем захисту.

Також в Україні потребують вирішення питання, пов'язані з інформаційним тероризмом (кібезтероризмом) та кіберзлочинністю, а саме:

- по-перше, термінологічна невизначеність, відсутність належної координації діяльності відповідних відомств, залежність України від програмних і технічних продуктів іноземного виробництва та складнощі з кадровим наповненням відповідних структурних підрозділів.

- по-друге, у нормативно-правових документах, зокрема міжнародних, досі відсутні загальновизнані тлумачення термінів "кіберпростір", "кіберзлочинність", "кібертероризм" та "кібервійна", що дозволило б більш точно визначити межі суспільно небезпечного діяння, яке підпадає під це поняття.

Цей перелік не вичерпується означеними питаннями та потребує дискусійного обговорення під час проведення наукових симпозіумів з актуальних питань забезпечення інформаційної безпеки.

## ЛІТЕРАТУРА

1. Герасименко К.С. Сучасні ознаки загроз "інформаційного тероризму" / К.С.Герасименко // Форум права. – 2009. – № 3. – С. 162-166 [Електронний ресурс]. – Режим доступу : http://www.nbuv.gov.ua/e-journals/FP/2009-3/09gkczit.pdf.

2. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. Резолюция A/RES/56/19 ГА ООН. – [Электронный ресурс]. – Режим доступа : http://daccess-ods.un.org/TMP/4296577.html.

3. Голубев В.А. Проблемы борьбы с кибертерроризмом в современных условиях / В.А.Голубев [Электронный ресурс]. – Режим доступу : http://www.crime-research.org/library/e-terrorism.htm. – 11.04.2003.

4. Указ Президента України від 12 лютого 2007 року № 105 (в редакції Указу Президента України від 8 червня 2012 року № 389/2012) “Про рішення Ради національної безпеки і оборони України від 8 червня 2012 року “Про нову редакцію Стратегії національної безпеки України” [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/389/2012.

5. Статистика МВС України [Електронний ресурс]. – Режим доступу : http://mvs.gov.ua. – 15.04.2010.

*Радовецька Л.В.,*
*Національна академія Служби безпеки України,*

## ПРОБЛЕМИ ДІЯЛЬНОСТІ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ У СФЕРІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ В СУЧАСНИХ УМОВАХ

Розвиток інформаційних та телекомунікаційних технологій є невід’ємною прикметою сьогодення. Однак разом із перевагами у життя суспільства увійшли нові загрози, пов’язані з порушенням безпеки інформації та інформаційних мереж.

На думку провідних світових фахівців у сфері ІТ-технологій, почалась нова ера кібертероризму, що стала наслідком глобального процесу інформатизації, який охоплює усі сфери життєдіяльності суспільства.

Кібертероризм можна визначити як суспільно небезпечні, умисні, цільові дії в кіберпросторі країни або використання інформаційної інфраструктури засобу для порушення функціонування об’єктів критичної інфраструктури.

Під об’єктами критичної інфраструктури варто розуміти об’єкти, порушення (або припинення) функціонування яких призводить до втрати управління, знищення інфраструктури, незворотних негативних змін в економіці країни або окремої адміністративно-територіальної одиниці, а також суттєвого погіршення безпеки життєдіяльності населення на тривалий термін (урядові установи, основна ресурсна база, енергетичні й транспортні магістральні мережі, військові об’єкти, нафто- і газопроводи, морські порти, об’єкти і канали швидкісного та урядового зв’язку тощо).

Корпорація “Symantec” опублікувала результати дослідження захисту критичної інфраструктури, що охопила 1580 компаній із 15 країн, які оперують об’єктами критичної інфраструктури. Дані до-

слідження свідчать про те, що 53% постачальників критичної інфраструктури уважають, що їхні мережі піддавалися кібератакам із політичних мотивів.

Протягом 2011–2013 років періодично спостерігались хакерські DDoS-атаки на сайти центральних органів влади України, до здійснення яких залучались не лише транскордонні бот-мережі, але й вітчизняні рядові користувачі інтернету. Внаслідок таких атак було порушено функціонування близько 30 веб-сайтів державних органів і установ.

Указана проблема є надзвичайно серйозною і має розглядатись у контексті захисту національної безпеки, оскільки застосування кіберзлочинцями шкідливого програмного обладнання проти об'єктів критичної інфраструктури може призвести до катастрофічних наслідків.

Інформаційна безпека – поняття комплексне, а отже, і забезпечена вона може бути лише за допомогою комплексного підходу, що є відлунням проблем забезпечення інформаційної безпеки як міждисциплінарне, комплексне і системне питання.

Управління забезпеченням інформаційної безпеки в цілому є однією з важливих функцій держави. Його сутність полягає в забезпеченні скоординованої національної стратегії на державному, регіональних і локальних рівнях при взаємоузгодженому розподілі обов'язків нормативно-правого, інформаційного, морально-психологічного, документального і ресурсного забезпечення.

З боку держави необхідно постійно здійснювати зіставлення загроз і небезпек із наявними ресурсами щодо управління ними. Потрібна всебічна деталізація прав, обов'язків, повноважень і відповідальності усіх складових системи управління національною безпекою. Важливо на додаток до тих функцій, що вже містяться в державному реєстрі, створити нові класифікатори функцій органів виконавчої влади на всіх рівнях системи державного управління стосовно питань забезпечення внутрішньої інформаційної безпеки.

Одним із ключових суб'єктів забезпечення національної безпеки України, визначених ст. 4 Закону України "Про основи національної безпеки України", та одним із суб'єктів реалізації державної політики України в інформаційній сфері є Служба безпеки України.

З метою забезпечення системи адекватних заходів з протидії зовнішнім та внутрішнім загрозам в інформаційній сфері, зокрема кібертероризму, на початку 2012 року в структурі СБ України було створено новий орган – Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки.

На сьогодні зазначений орган, попри досить молодий вік, досягнув низку вагомих результатів, у т.ч. у взаємодії із зарубіжними партнерами, та набув певного позитивного досвіду. Утім, набутий досвід свідчить про необхідність суттєвої активізації усіх зацікавлених органів державної влади в напрямі розвитку та систематизації національної системи інформаційної безпеки.

На сучасному етапі в Україні поки що немає стратегічного та системного бачення забезпечення інформаційної безпеки як на правовому, так і на політичному рівні.

З метою оптимізації національного законодавства у сфері забезпечення інформаційної безпеки держави вважаємо за доцільне активізувати роботу з прийняття запропонованих РНБО України змін до Кримінального кодексу України, законів "Про основи національної безпеки", "Про оборону України", "Про захист інформації в ІТ системах", "Про основи внутрішньої і зовнішньої політики", "Про інформацію", "Про боротьбу з тероризмом".

Серед першочергових змін слід визначити кіберагресію як надзвичайну ситуацію техногенного та природного характеру в законі "Про захист населення і територій від надзвичайних ситуацій техногенного та природного характеру". Потрібне чітке законодавче визначення функціональних обов'язків конкретних органів виконавчої влади в контексті протидії кіберзагрозам; нормативне закріплення таких ключових понять, як "кібернетична безпека держави", "об'єкти критичної інфраструктури", "кібернетичний тероризм" тощо.

Важливим нововведенням має стати розширення повноважень СБ України у сфері протидії загрозам в інформаційній сфері. Зокрема, варто було б внести зміни до ст. 258 Кримінального кодексу України, криміналізувавши поняття "кібертероризм".

З огляду на досвід Російської Федерації, актуальним є прийняття програмного документа, який би визначав державну політику у сфері забезпечення безпеки автоматизованих систем управління виробничими і технологічними процесами об'єктів критичної інфраструктури, а також конкретні терміни й етапи її реалізації.

Серед інших напрямів удосконалення національної системи забезпечення інформаційної безпеки слід визначити:

- підвищення рівня координації діяльності державних органів щодо виявлення, оцінювання й прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їх наслідків, здійснення міжнародного співробітництва з цих питань;

- запровадження міжвідомчого підходу та ієрархічності в організації системи забезпечення інформаційної безпеки держави. Її структура й організація мають відповідати чинній структурі державного управління з чіткою координацією дій окремих сегментів.

*Рижков Е.В.,*
*кандидат юридичних наук, доцент,*
*Донецький юридичний інститут МВС України*

*Шавиркін Борис Б.Б.*
*Донецький юридичний інститут МВС України*

# СКЛАДОВІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИ РОЗСЛІДУВАННІ КІБЕРЗЛОЧИНІВ

У зв'язку зі стрімким розвитком інформаційних технологій та комп'ютерної техніки, який спостерігається протягом останніх років, велику небезпеку становить поява нових форм злочинної діяльності, пов'язаних із використанням кіберпростору. З такими проявами поки що досить складно вести ефективну боротьбу як із точки зору кримінального процесу, так і оперативно-розшукової діяльності. В умовах реформування зазначених сфер правоохоронної діяльності необхідно напрацювати нові форми організаційно-управлінських рішень та заходів щодо забезпечення ефективної взаємодії слідчих, оперативних працівників, представників прокуратури та суду.

Одним із перших етапів підвищення ефективності попередження, виявлення, припинення та розслідування кіберзочинів є розуміння сутності, статусу комп'ютерної інформації та потенційних загроз від процесів її неправомірного використання.

Інформаційний розвиток суспільства й запровадження на державному рівні використання мережі Інтернету та інших комп'ютерних систем в усіх сферах суспільного життя, поряд із позитивними здобутками, зумовлюють і негативні явища. Особливу занепокоєність викликає збільшення кількості злочинів у сфері використання високих технологій – (так званих кіберзлочинів).

Кіберзлочин (неофіційне визначення) – злочинна діяльність, у процесі якої комп'ютери, комп'ютерні мережі, комп'ютерні дані, а також їхні продукти в матеріальній або електронній формі виступають знаряддям злочину або об'єктом атаки.

*Типи кіберзлочинів* (за класифікацією Євросоюзу):

1) злочини проти безпеки комп'ютерних даних (злочини проти конфіденційності, цілісності та доступності комп'ютерних даних та систем, власне, *кіберзлочини*);

2) злочини, пов'язані із комп'ютерами (*злочини, пов'язані з комп'ютерною технікою, обладнанням, мережевим обладнанням,* тощо);

3) злочини, пов'язані із змістом даних (*злочини, пов'язані із змістом*);

4) злочини, пов'язані з порушенням авторських та суміжних прав (*піратство*).

Сучасні кіберзлочини мають такі характеристики:

– поява перших організованих кіберзлочинних угрупувань;

– спілкування через Інтернет;

– використання інформаційних технологій при скоєнні організованих злочинів;

– відмивання коштів через інтернет.

Завжди є проблема вибору між необхідним рівнем захисту та ефективністю роботи в мережі. У деяких випадках користувачами або споживачами заходи щодо забезпечення безпеки можуть бути розцінені як заходи з обмеження доступу та ефективності. Однак такі засоби, як, наприклад, криптографія, дозволяють значно посилити ступінь захисту, не обмежуючи доступ користувачів до даних.

Широке застосування комп'ютерних технологій в автоматизованих системах оброблення інформації та *управління* призвело до загострення проблеми захисту інформації, що циркулює в комп'ютерних системах, від несанкціонованого доступу. *Захист інформації* в комп'ютерних системах має низку специфічних особливостей, зумовлених, тим, що *інформація* не є жорстко пов'язаною з носієм, може легко і швидко копіюватися й передаватися по каналах зв'язку. На сьогодні виявлена та в достатній мірі досліджена велика кількість загроз комп'ютерній інформації, які можуть реалізовувати як злочинці, так і правоохоронні органи.

При проведенні пошукових заходів необхідно пам'ятати про те, що будь-яка мережева активність розшукуваних злочинців може бути використана для їх ідентифікації та пошуку. Власники електронних адрес, акаунтів у соціальних мережах, електронних платіжних системах при реєстрації зазвичай залишають телефон, П.І.Б. (потрібно перевіряти), поштову скриньку та, найцікавіше, IP-адресу, з якої заходили під час реєстрації та користування. Отримання вказаної інформації в межах України можливо за наявності відповідного рішення суду в рамках кримінального провадження, за межами України – на підставі Міжнародної конвенції про боротьбу з кіберзлочинністю за наявності кримінального провадження.

Одним із способів, який дозволяє отримати первинні дані про злочинця або вчинені злочини (наприклад, злочини, які пов'язані з виготовленням, збутом та розповсюдженням продукції порнографі-

чного характеру), є систематичний і цілеспрямований моніторинг загальнодоступних інформаційних ресурсів. Він здійснюється шляхом використання пошукових систем, що дозволяють знаходити потрібну інформацію у величезному масиві даних шляхом складання елементарних запитів (наприклад, “google.ru”, “yandex.ru”, “rambler.ru” тощо).

Отже, основною метою такого моніторингу є отримання та фіксація достовірної первинної інформації про:

– факти скоєння невстановленою особою злочинів, передбачених чинним Кримінальним кодексом України;

– особу злочинця або дані, які в подальшому допоможуть його ідентифікувати (ім’я, вік, місце проживання або роботи, освіта чи місце навчання, сімейний стан, зовнішній вигляд, доменні імена в мережі тощо);

– інформаційні ресурси, які використовуються для вчинення протиправних дій (назви інтернет-магазинів, рекламних сайтів чи ресурсів з обмеженим доступом, форумів, електронних дошок оголошень та інше);

– способи встановлення контакту зі злочинцем (листування через електронну пошту, відправлення повідомлень через інтернет-пейджери, засоби стільникового зв’язку, поштові скриньки тощо);

– способи оплати придбаної забороненої продукції (поштові або банківські перекази, використання електронних платіжних систем, передача готівки і т.д.).

Використання електронних листів із відкритих джерел (шляхом аналізу заголовків цих листів, які, крім змістового повідомлення – контенту, – містять службову інформацію (метадані), надає додаткові оперативно-розшукові можливості для отримання інформації про IP-адреси, фізичне місцезнаходження під час листування та особисті дані користувача.

Крім електронної пошти, для отримання оперативно-розшукової інформації з контенту можна скористатися такими сервісами інтернету:

– чати;

– пейджингові повідомлення;

– групи новин.

Деяка прихована та вбудована персональна інформація (метадані) може бути вбудована в будь-який документ пакету MS Office: автор, адреса електронної пошти, останній збережений каталог, назва компанії та її адреса.

При проведенні онлайн-розслідувань слід пам'ятати, що більшість вузлів мережі оснащені функціями автоматичного моніторингу та майже вся мережева діяльність якимось чином фіксується. Наприклад, будь-який сервер у мережі містить детальні електронні журнали для кожного запиту будь-якої сторінки. Кожний запит до серверу включає дату, час, кількість байтів і, найголовніше, IP-адресу комп'ютера, який запитав дані.

Отже, відправлення повідомлення електронної пошти зазвичай розкриває адресу інтернет-протоколу (IP-адресу); відвідування веб-сайту показує IP-адресу, діяльність користувача за цією адресою (використані посилання або закачувані файли, що закачувалися) і раніше відвідані веб-сайти (референтна інформація); всі операції в мережі можуть розкрити IP-адресу.

Додаткову користь, передусім у вигляді необхідної інформації, можуть надати фахівці відповідних служб безпеки тих суб'єктів, які спеціалізуються на кібернетичному просторі. Проте такі контакти повинні здійснюватись без розкриття позицій слідства та матеріалів оперативно-розшукових справ.

Також слід ураховувати, розробники більшості програмних продуктів, якими активно послуговуються представники правоохоронних органів при збиранні інформації, практикують реалізацію шпигунських функцій у програмному забезпеченні. Тому виникає необхідність дотримання відповідних процедур і порядку для запобігання витоку інформації.

## ЛІТЕРАТУРА

1. Конвенція про кіберзлочинність : підписано від імені України 23.11.2001 р. в м. Будапешті ; ратифіковано Законом України від 07.09.2005 р. № 2824-IV [Електронний ресурс] / Веб-сайт Верховної Ради України. – Режим доступу : http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi? nreg=994_575&p= 1258319103877184.

2. Ярочкин В.И. Информационная безопасность : учеб. для студентов вузов / В.И.Ярочкин. – М. : Академический Проект; Гаудеамус, – 2004. – 544 с. (Gaudeamus).

3. Протидія кіберзлочинності в Україні: правові та організаційні засади : навч. посіб. / [О.Є.Користін, В.М.Бутузов, С.С.Чернявський та ін.].

*Розвадовський О.Б.,*
*кандидат юридичних наук,*
*Національна академія Служби безпеки України*

# ЮРИДИЧНА ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ ЗАКОНОДАВСТВА У СФЕРІ ОХОРОНИ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

Наукові дослідження проблем юридичної відповідальності мають давню історію. Попри вагомі здобутки радянської та української правничої науки у цій галузі знань, є ще чимало законодавчих та доктринальних проблем, вирішення яких потребує нових підходів. На часі потреба системного аналізу юридичної відповідальності за законодавством України, порівняльний аналіз із відповідними нормами інших держав Європи [1, с. 101]. У цьому плані не є винятком сфера забезпечення охорони інформації з обмеженим доступом.

Слід зауважити, що вивчення численних наукових праць, присвячених дослідженню правової природи юридичної відповідальності, показує, що донині в теорії права немає єдиного розуміння її сутності і змісту. Зокрема, одні вчені розглядають юридичну відповідальність як санкцію, інші – як аналог зобов'язання, треті – як обов'язок, четверті – як реакцію держави на правопорушення.

Різноманітність поглядів щодо розуміння сутності й змісту юридичної відповідальності як правового інституту свідчить про її багатоаспектність і різноплановість. Водночас, більшість науковців є одностайними в тому, що її слід визначати крізь призму правопорушення, тобто питання щодо юридичної відповідальності виникає при вчиненні порушення правових норм [2]. Основними ознаками (складовими) юридичної відповідальності є охоронювані правовідносини, правопорушення та правозастосовна діяльність.

Конституція України [3] й законодавчі акти визначають основні види юридичної відповідальності, які застосовуються у сфері охорони інформації з обмеженим доступом, а саме: конституційна; міжнародно-правова; кримінальна; адміністративна; цивільно-правова; дисциплінарна та матеріальна. Вони переслідують різні цілі й мають свої особливості, на розгляді яких ми зупинимось окремо.

Конституційно-правова відповідальність у сфері забезпечення охорони інформації з обмеженим доступом безпосередньо пов'язана з конституційним законодавством та спирається на його приписи, що можна віднести до її особливостей. Її слід розглядати, насамперед, як відповідальність державних органів та їх посадових осіб перед народом за неналежну реалізацію тих владних повноважень у

сфері охорони державної таємниці та службової інформації, які народ як єдине джерело влади їм передав.

Відповідальність держав за їх міжнародно-протиправні діяння визначається терміном "міжнародно-правова відповідальність". До особливостей цього виду відповідальності слід віднести те, що суб'єктами правовідносин, як правило, виступають суверенні й незалежні держави або міжнародні організації та жодна зі сторін не має формальних переваг щодо наявності важелів впливу на іншу. Поряд із цим, на відміну від інших видів юридичної відповідальності, вона не передбачає застосування заходів державно-владного примусу.

Кримінальна відповідальність як різновид юридичної відповідальності посідає особливе місце у сфері забезпечення охорони державної таємниці та службової інформації. Це передусім пов'язано із суспільною небезпекою діянь, за які передбачена така відповідальність, та вирішуваними завданнями із правового забезпечення охорони прав і свобод людини і громадянина, власності, громадського порядку та громадської безпеки, довкілля, конституційного устрою України від злочинних посягань, забезпечення миру й безпеки людства, а також запобігання злочинам.

Адміністративна відповідальність (поряд із кримінальною, дисциплінарною та цивільно-правовою) є особливим видом юридичної відповідальності. Їй притаманні ознаки останніх, проте вона має свої особливості, зокрема: настає за вчинення адміністративного правопорушення (проступку); результатом притягнення особи до адміністративної відповідальності є накладення на неї адміністративного стягнення; заходи адміністративної відповідальності вживають визначені КУпАП [4] та законодавчими актами державні органи і їхні посадові особи; характеризується особливим процесуальним порядком реалізації – провадженням у справах про адміністративні правопорушення тощо.

Застосування дисциплінарної відповідальності завжди пов'язане з виконанням трудових або службових обов'язків. У трудових правовідносинах роботодавець має дисциплінарну владу над працівником, а працівник несе дисциплінарну відповідальність саме перед роботодавцем, а не перед державою (державним органом), як це відбувається при адміністративній та кримінальній відповідальності. Особливістю дисциплінарної відповідальності є застосування стягнень, що становлять її зміст, як правило, суб'єктом трудових відносин, а саме роботодавцем. У зв'язку з цим дисциплінарна відповідальність є одним із проявів владних повноважень роботодавця стосовно працівника, з яким укладено трудовий договір [5].

Нормами Кодексу законів про працю України [6] також визначаються загальні підстави й умови матеріальної відповідальності працівників за шкоду, заподіяну установі внаслідок порушення покладених на них трудових обов'язків, які пов'язані із забезпеченням охорони інформації з обмеженим доступом. Така відповідальність установлюється тільки за пряму дійсну шкоду за умови, якщо така шкода заподіяна установі винними протиправними діями (бездіяльністю) працівника. Вона може бути покладена незалежно від притягнення працівника до дисциплінарної, адміністративної чи кримінальної відповідальності.

Цивільно-правова відповідальність настає за порушення договірних зобов'язань майнового характеру або заподіяння майнової чи немайнової (моральної) шкоди, тобто за скоєння цивільно-правового делікту, і може виражатись у позбавленні правопорушника певних благ матеріального характеру, заміні невиконаного обов'язку новим, приєднанні до невиконаного обов'язку нового, додаткового [7, с. 219]. Основними формами посягань на цивільні права та інтереси суб'єктів в інформаційній сфері є їх порушення, невизнання та оспорювання.

Все зазначене вище дає підстави дійти висновку, що до видів юридичної відповідальності у сфері охорони державної таємниці та службової інформації слід віднести конституційну, міжнародно-правову, кримінальну, адміністративну, цивільно-правову, дисциплінарну та матеріальну. Вони об'єднані спільною метою – врегулювання й охорони суспільних відносин у сфері охорони інформації з обмеженим доступом, водночас, переслідують різні цілі та мають свої особливості. Дослідження особливостей юридичної відповідальності та її видів має важливе значення для подальшого розвитку і вдосконалення вказаного правового інституту.

## ЛІТЕРАТУРА

1. Петрицин Н.Т. Про питання про сутність юридичної відповідальності // Часопис Академії адвокатури України. – 2012. – № 1(14). – С. 101-107. – Національна бібліотека України ім. В.І.Вернадського [Електронний ресурс]. – Режим доступу : http://www.nbuv.gov.ua/e-journals/Chaau/2012-1/12pntvsa.pdf.

2. Корнєєв Ю.В. Особливості юридичної відповідальності за екологічні правопорушення на залізничному транспорті / Ю.В.Корнєєв // Національна бібліотека України ім. В.І.Вернадського [Електронний ресурс]. – Режим доступу : http://www.nbuv.gov.ua/portal/soc_gum/misb/2011_3-4/Korneev.pdf.

3. Конституція України [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/964-15.

4. Закон України від 21 вересня 1999 року № 1080-XIV “Про внесення змін до Кодексу України про адміністративні правопорушення щодо встановлення відповідальності за порушення законодавства про державну таємницю” // Відомості Верховної Ради. – 1999. – № 49. – Ст. 429.

5. Кім К.В. Дисциплінарна відповідальність за порушення законодавства про інформацію // Сайт Національної бібліотеки України ім. В.І.Вернадського [Електронний ресурс]. – Режим доступу : http://www.nbuv.gov.ua/portal/soc_gum/vkhnuvs/2011_55/55/51.pdf.

6. Кодекс законів про працю України // Офіційний сайт Верховної Ради України [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/322-08.

7. Марущак А.І. Правові основи захисту інформації з обмеженим доступом : навч. посіб. / А.І.Марущак. – К. : Наук.-вид. відділ НА СБ України, 2007. – 245 с.

*Романенко І.В.,*
*Національна академія Служби безпеки України*

## ПИТАННЯ УНІФІКАЦІЇ ЗАСТОСУВАННЯ В ЗАКОНОДАВСТВІ ПОНЯТТЯ “ДОПУСК ДО ДЕРЖАВНОЇ ТАЄМНИЦІ”

Основним призначенням спеціального порядку допуску та доступу громадян до державної таємниці є обмеження кількості осіб, обізнаних із державною таємницею, та унеможливленні допуску осіб, які можуть допустити небажану для охорони державної таємниці поведінку. Для забезпечення цієї функції законодавством установлено необхідність проходження обов’язкової процедури – оформлення допуску до державної таємниці, під час якої визначається відповідність громадянина чітким вимогам. Водночас, для певної категорії осіб передбачено виняток із цього правила. Так, без оформлення допуску, доступ до державної таємниці надається вищим посадовим особам (за посадою), іноземцям, особам без громадянства та особам, залученим до конфіденційного співробітництва. Використання ж на законодавчому рівні таких понять, як “допуск”, “доступ за посадою”, “одержання дозволу на доступ іноземця”, які є різними за формою, але однаковими за змістом поняттями, призводить до колізій у нормативному регулюванні та проблем під час застосування законодавства на практиці. Таким чином, ці дефініції

потребують детального дослідження для належного урегулювання їх особливостей на законодавчому рівні.

Відповідно до Закону України "Про державну таємницю"[1, ст. 1] *допуск* до державної таємниці – це оформлення права громадянина на доступ до секретної інформації, а *доступ* – надання повноважною посадовою особою дозволу громадянину на ознайомлення з конкретною секретною інформацією. Виходячи з цих понять, можна припустити, що допуск і доступ до державної таємниці передбачається виключно для громадян України. Водночас, стаття 3 поширює сферу дії закону на іноземців та осіб без громадянства, яким у встановленому порядку також може бути наданий доступ до державної таємниці.

Порядок доступу до державної таємниці встановлено ст. 27 Закону, яка передбачає *загальне правило доступу* – доступ надається до конкретної секретної інформації (категорії секретної інформації) рішенням керівника установи, та *особливі порядки надання доступу*:

- *доступ за посадою після надання допуску* – для керівників державних органів;
- *доступ за посадою без оформлення допуску* – Президентові України, Голові Верховної Ради України, Прем'єр-міністрові України та іншим членам Кабінету Міністрів України, Голові Верховного Суду України, Голові Конституційного Суду України, Генеральному прокурору України, Голові Служби безпеки України, народним депутатам України після взяття ними письмового зобов'язання щодо збереження державної таємниці;
- *доступ до державної таємниці іноземцям та особам без громадянства* – у виняткових випадках на підставі міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України, або письмового розпорядження Президента України з урахуванням необхідності забезпечення національної безпеки України на підставі пропозицій Ради національної безпеки і оборони України;
- *доступ осіб, залучених до конфіденційного співробітництва,* – у визначеному відповідними керівниками органів, що проводять оперативно-розшукову, розвідувальну та контррозвідувальну діяльність порядку, погодженому із СБ України.

При чому, як бачимо, назва статті "доступ громадян до державної таємниці" не відповідає її змісту, оскільки встановлює порядок доступу не лише громадянам України, а й іноземцям та особам без громадянства.

Порівняємо механізм надання допуску та доступу за посадою. Надання допуску передбачає:

1) визначення необхідності роботи громадянина із секретною інформацією;

2) перевірку у зв'язку з допуском;

3) взяття громадянином на себе письмового зобов'язання щодо збереження державної таємниці, яка буде йому довірена;

4) одержання у письмовій формі згоди на передбачені законом обмеження прав у зв'язку з допуском до державної таємниці;

5) ознайомлення громадянина з мірою відповідальності за порушення законодавства про державну таємницю.

Доступ за посадою передбачає наявність визначеної необхідності роботи із секретною інформацією – це відповідна посада, а також взяття письмового зобов'язання щодо збереження державної таємниці. Зобов'язання передбачає як, безпосередньо, взяття громадянином на себе зобов'язань у зв'язку з допуском, так і його згоду на обмеження прав і підтвердження ознайомлення з мірою відповідальності за порушення законодавства про державну таємницю. Таким чином, при наданні доступу за посадою здійснюються практично всі заходи, передбачені при наданні допуску, за винятком перевірки органами СБ України. В результаті посадова особа має *оформлене у встановленому порядку право на доступ до секретної інформації* (або *допуск до державної таємниці*).

Наведений аналіз дозволяє запропонувати уведення в законодавство нового поняття "спрощена процедура допуску", тобто надання допуску до державної таємниці без проведення перевірних заходів органами СБ України.

Проблема надання допуску за спрощеною процедурою стосується не лише посадових осіб, зазначених у статті 27 Закону України "Про державну таємницю". В науковій літературі неодноразово порушуються проблеми, пов'язані з наданням допуску захисникам у кримінальному та цивільному судочинстві [2, с.46-49].

Утім, запровадження поняття "спрощений порядок допуску" не врегульовує питання доступу іноземців та осіб без громадянства до державної таємниці. Для цієї категорії осіб порядок надання доступу передбачено указом Президента України, яким затверджено "Положення про порядок підготовки документів щодо надання доступу до державної таємниці іноземцям та особам без громадянства" [3]. Слід зазначити, що такий порядок відповідає основним загальним правилам надання допуску, а необхідність перевірки у зв'язку з ознайомленням з державною таємницею передбачена відповідними міждержавними угодами (у більшості, до речі, вказано, що інформація може бути надана лише тим особам, які отримали *допуск* до неї після необхідних дій і процедур, що вимагаються законодавством кожної держави).

Таким чином, іноземець чи особа без громадянства фактично отримує допуск (право на доступ до державної таємниці), але не в загальному порядку, а в спеціальному, такому, що враховує особливості її правового статусу.

Підсумовуюче викладене, вважаємо за доцільне запропонувати зміни до Закону України "Про державну таємницю":

1. Визначити допуск до державної таємниці як "право *особи* на доступ до секретної інформації, оформлене у встановленому порядку". Відповідно, надання допуску стане обов'язковою для всіх категорій осіб умовою ознайомлення з секретною інформацією (доступу до державної таємниці).

2. Враховуючи особливості правового статусу окремих категорій осіб, увести поняття *спрощений порядок допуску*, що буде стосуватися:

- Президента України, Голови Верховної Ради України, Прем'єр-міністра України та інших членів Кабінету Міністрів, Голови Верховного Суду України, Голови Конституційного Суду України, Генерального прокурора України, Голови Служби безпеки України, народних депутатів України;

- захисників у кримінальному, цивільному та адміністративному судочинстві по справах, пов'язаних з відомостями, що становлять державну таємницю;

та поняття *спеціальний порядок допуску* – для іноземців та осіб без громадянства; осіб, які залучені до конфіденційного співробітництва з правоохоронними органами.

Слід наголосити, що на вказаних осіб поширюються норми щодо обов'язків збереження державної таємниці та обмеження деяких прав у зв'язку з допуском, оскільки вимоги відповідних норм мають загальний характер і не залежать від того, надавався допуск на загальних підставах, за спрощеною чи спеціальною процедурою.

## ЛІТЕРАТУРА

1. Закон України "Про державну таємницю" від 19.04.1994 р.

2. Романенко І.В. Допуск до державної таємниці в Російській Федерації та Україні: порівняльно-правовий аналіз: аналітичний огляд / І.В.Романенко, В.В.Макаренко, В.П.Ворожко. – К. : Вид-во НА СБ України, 2005. – С. 46-49.

3. Положення про порядок підготовки документів щодо надання доступу до державної таємниці іноземцям та особам без громадянства, затверджене Указом Президента України від 17.07.2006 р. № 621.

*Савінова Н.А.,*
*кандидат юридичних наук,*
*Науково-дослідний інститут інформатики і права*
*Національної академії правових наук України*

# ІНФОРМАЦІЙНА ЕКСПАНСІЯ

Із розвитком інформаційного суспільства здійснення певного кола намірів із завдання шкоди віддаленим предметам і посягання на об'єкти, які раніше були фактично недосяжні, стало повсякденною реальністю. Значна низка суспільно небезпечних діянь, спрямованих на заподіяння шкоди державним інтересам, сьогодні може вчинюватися як у кібернетичному, так і в інформаційному просторі.

Психологічні впливи на свідомість актуалізуються в інформаційному суспільстві через можливість їх здійснення з використанням сучасних ІТ, унаслідок чого засоби впливу можуть спрямовуватися на свідомість необмеженої у кількості аудиторії. Здійснюватися вони можуть як через ЗМІ, так і інтернет, а в окремих випадках і при посередництві телекомунікацій.

В інформаційному суспільстві актуалізується (а також видозмінюється стосовно своїх попередників) група суспільно небезпечних діянь, які доцільно умовно називати "*інформаційна експансія*" – *явище, що створює ґрунт для подальших психологічних впливів на свідомість у процесі спілкування.*

Експансія (лат. expansio – розширення) означає поширення (кордонів, впливів тощо), відповідно, *інформаційна експансія спрямована на опанування інформаційного простору, полягає в захопленні з метою подальшого використання на свою користь саме інформаційного простору певної держави (включаючи кібернетичний простір).*

Основним полем інформаційної експансії виступає сегмент інформаційного простору, що "покривається" ЗМІ. І хоча з початку 2000-х років і Президент України, і РНБО України[1] наголошували на необхідності убезпечення інформаційного суверенітету від інформаційної експансії, це явище охоплює все більшу аудиторію нашої країни.

Фізичне покриття телемовлення прикордонних територій природно. У той же час, ЗМІ нерідко створюють умови інформаційної

[1] Прес-служба президента України В. Ющенка. Під головуванням Президента України відбулося засідання РНБОУ [Електронний ресурс] // Офіційний сайт Президента України. – 21.03.2008. Режим доступу : http://www.president.gov.ua/news/9385.html.

експансії шляхом закупівлі й трансляції на території власних держав продукту, який орієнтований на іншу аудиторію, з притаманними їй етносоціальними рисами, що створює загрози впливу на ментальність власного населення. П.М.Лисовський зазначає: "Щодо маніпулятивних практик у сучасному світі, то тут важливі ЗМІ, де формуються узагальнені інтереси великих і малих соціальних груп населення. Для різних соціальних груп запускається своєрідний механізм становлення необхідних "системі" життєвих цілей. На певному етапі "система" ініціює розвиток у конкретній людині, що належить до відповідної соціальної групи, домінуючих стандартів життєвого успіху, стимулюючи її природні здібності через освітянську мережу, мораль соціального середовища тощо"[1].

Звичайно, *недопустимим є передання іншій державі панування в інформаційному просторі суверенної держави,* з метою захисту свідомості населення, національного менталітету, який має виступати одним з базових національних чинників відповідного суспільства. Завдяки інформаційним впливам, які можуть здійснюватися на базі інформаційної експансії, суспільство втрачає свої первинні, цінні якості, що відображуються на свідомості індивідів і, відповідно, у суспільній свідомості.

Питання забезпечення безпеки інформаційного простору в умовах розвитку глобального ІС може покладатися виключно на державу. Медійний продукт, що закуповується і транслюється національними телевізійними компаніями, має відповідати системі цінностей, притаманних суспільній свідомості відповідного суспільства, системі цінностей, що панують у певній державі. Якщо держава обирає для свого розвитку принципи демократії, відкритості, гуманізму і т.д., в її інформаційному просторі не повинно бути телевізійних продуктів, які пропагують тоталітаризм, авторитарність і порушення прав людини, не лише підривають основні проголошені в державі принципи, а й руйнівно впливають на свідомість індивідів, породжуючи перекручення суспільної свідомості. Саме в такий спосіб може діяти суб'єкт інформаційної експансії проти держави, на інформаційний простір якої вчинюється посягання.

З урахуванням розвитку ЗМІ, інтернету і можливостей використання ІКТ, у т.ч. телекомунікацій, ІКТ повною мірою належать до засобів, за допомогою яких впливи на свідомість можуть вчинюватися щодо мільйонів індивідів одночасно. Результати психологічних впливів на свідомість можуть безпосередньо іти на користь осіб,

[1] Лісовський П.М. Питання методології національної безпеки / П.М.Лісовський. – К. : Вид-во НПУ ім. М.П. Драгоманова, 2006. – С. 101.

груп, держав та міждержавних об'єднань або створювати поле для потенційних додаткових сигналів для активізації наслідків цих впливів.

Базою для таких впливів є саме захоплення інформаційного простору. Таким чином, інформаційна експансія створює поле можливих у подальшому психологічних впливів на свідомість у процесі спілкування. Такі впливи можуть здійснюватися з різною метою: від викликання у свідомості населення негативного ставлення до певного індивіда або соціальної, зокрема етнічної, групи до спричинення внутрішніх конфліктів на національному рівні.

Найпоширеніші види впливів на свідомість, які визнаються правниками-фахівцями, такі: впливи, вчинені шляхом застосування нейролінгвістичного програмування (т. зв. NLP-технологій, від Neuro-linguistic programming, англ.), поширенням інформаційно-психологічних вірусів, застосування гіпнозу тощо.

Всі ці технології можуть використовуватися як зброя інформаційної війни. *"Інформаційні війни"* – агресивні дії в інформаційному просторі[1], які проводяться шляхом психологічних впливів на свідомість[2]. Інформаційні війни можуть створювати загрозу суспільним інтересам, починаючи від суверенітету держав, інформаційний простір яких не убезпечений належним чином; вони відрізняються від можливих мілітаристичних війн, але можуть виступати елементами стратегії останніх. Очевидне визначення свідомості індивіда чи групи як остаточного об'єкта спрямування інформаційної атаки як елементу інформаційної війни.

Інформаційна експансія утворює, фактично готує "поле бою" у свідомості населення захоплюваної території.

Таким чином, *під інформаційною експансією слід розуміти умисне захоплення з метою подальшого використання на свою користь інформаційного простору або значного сегменту інформаційного простору певної держави чи групи держав, яке здійснюється окремою державою, групою держав або індивідом чи групою індивідів. Інформаційна експансія має розцінюватися як явище, що утворюється з метою подальшого використання інформаційного простору для ведення інформаційних війн.*

---

[1] Тэтчер М. Искусство управления государством: Стратегии для меняющегося мира / Маргарет Тэтчер ; [пер. с англ. В. Ионова]. – М. : Альпина Паблишер, 2003. – С. 71; Політологічний словник : [навч. посіб. для студ. вищ. навч. закл.] / [за ред. М.Ф.Головатого та О.В. Антонюка]. – К. : МАУП, 2005. – С. 340.

[2] Степанов О.А. Развитие информационно-электронных систем как объект правового анализа в условиях нарастающей угрозы киберпреступности / О.А.Степанов // Государство и право. – 2008. – № 8 – С. 82-85.

*Саржан С.Л.,*
*кандидат юридичних наук,*
*Національна академія СБ України*

# ПРАВО НА ІНФОРМАЦІЮ ЯК ОБ'ЄКТ ПРАВОВІДНОСИН

В умовах формування інформаційного суспільства в Україні поняття "інформація" набуває центрального значення.

У теорії інформаційних систем інформація ототожнюється з будь-якими відомостями (даними), тобто тлумачиться як сукупність відомостей про будь-що або будь-кого. Згідно з кібернетичним підходом інформацією є лише нові, корисні, вагомі для користувача відомості.

Інформація – це специфічна правова категорія. Ознаки, що її характеризують, здебільшого притаманні тільки їй. На науковому рівні їх виділив А.Б.Венгеров, який зазначив, що це:

- незалежність інформації стосовно свого носія;
- можливість багаторазового використання однієї й тієї самої інформації;
- вона не зникає при споживанні;
- збереження інформації у суб'єкта, який її передає;
- здатність до збереження, агрегування, інтегрування, накопичення, "стискання";
- кількісна визначеність інформації;
- системність.

Серед характерних рис інформації О.В.Кохановська зазначає нематеріальний характер. Інформація – благо неспоживче, яке піддається лише моральному, але не фізичному старінню.

Згідно із статтею 177 Цивільного кодексу України інформація є об'єктом цивільних прав. Багатогранністю і специфічністю інформації зумовлюється те, що вона може бути об'єктом як майнових, так і немайнових цивільних прав. Суб'єктивні права особи на інформацію можна поділити на майнові й особисті немайнові права.

Право на інформацію як одне з особистих немайнових благ, що забезпечує і соціальне буття фізичної особи, з'являється в людини в момент народження й нерозривно пов'язане з нею протягом усього життя, тобто набувається фізичною особою і внаслідок народження. Згідно із статтею 302 Цивільного кодексу України "фізична особа має право вільно збирати, зберігати, використовувати і поширювати інформацію". Цей перелік доцільно доповнити правом шукати інформацію, яке згідно із Рекомендацією Ради Європи № 854(1979) "Про доступ громадськості до державної документації

та свободу інформації" також передбачається серед правомочностей суб'єктів інформаційних відносин, що дозволило б розширити можливості доступу до державної документації.

Право на інформацію як результат творчої, інтелектуальної діяльності набувається завдяки закону. Будь-який твір за своєю природою є інформацією, яка виникла в результаті творчої діяльності людини і набула певної об'єктивної форми. При цьому інформацію неможливо відділити від форми її подання. В цьому випадку інформація виступає як особливий об'єкт виключних цивільних прав.

Дискусійним залишається питання розуміння права власності на інформацію. Наприклад, у низці країн є право власності на інформацію. Так, англійський Закон про власність 1925 року, судова практика і доктрина включають інформацію до категорії "майна", а саме до персонального рухомого майна, на яке поширюється право власності.

В українському законодавстві поняття "права власності на інформацію" було і вилучено із Закону України "Про інформацію" в редакції 2011 р. Такий підхід законодавця, на нашу думку, зрозумілий. Виходячи із природи права власності, до поняття інформації не можливо застосувати в повному обсязі "тріаду", на якій базується це право щодо речей: володіння, користування і розпоряджання. За наявності згаданих вище ознак інформація легко тиражується і не відчужується: вона залишається в того, хто її передав. Тобто поняття "володіння інформацією" досить умовне – нею володіють усі, хто був із нею ознайомлений, проте не всі мають права її використовувати та розпоряджатися.

Утім, у системі цивільно-правових відносин інформація може виступати як продукт-предмет, що має попит на ринку, вартісну оцінку і властивість товару у формі нематеріальних активів. У такому випадку інформація у формі інформаційного продукту або інформаційних послуг виступає об'єктом майнових цивільних прав, змістом яких можуть бути дві правомочності: користування і розпорядження. При цьому перше полягає в можливості вчиняти будь-які можливі й не заборонені законом або договором дії з інформацією та на її основі, а друге – передавати інформацію в будь-якій формі будь-якій третій особі як за плату, так і безоплатно.

Закон України "Про інформацію" як один із видів інформації виокремлює правову інформацію – сукупність документованих або публічно оголошених відомостей про право, його систему, джерела, реалізацію, юридичні факти, правовідносини, правопорядок, правопорушення і боротьбу з ними та їх профілактику тощо.

*Сидоренко С.М.,*
*Національна академія Служби безпеки України*

# ХАРАКТЕРИСТИКА ДЕРЖАВНО-ПРАВОВИХ МЕХАНІЗМІВ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ В РЕСПУБЛІЦІ СЛОВЕНІЇ

Словенія за формою правління є парламентською республікою. Її конституція формулює принцип поділу влади в його класичному конституційному викладенні: діяльність Національної асамблеї, президента республіки, уряду та судів здійснюється за принципом поділу й збалансування влад. Отже, система вищих органів державної влади Словенії достатньо традиційна. Законодавчу владу здійснює парламент – Національна асамблея, главою держави є президент. Виконавча влада належить уряду.

Внутрішній контроль за дотриманням правил поводження із класифікованою інформацією покладається на керівників установ. У Міністерстві внутрішніх справ, Міністерстві закордонних справ та Службі розвідки і безпеки, а за потреби, і в інших установах уведено посаду (підрозділ) спеціально уповноваженого, до обов'язків яких входить контроль за правильністю визначення класифікованої інформації та її захистом. В Міністерстві оборони такого роду діяльність уповноважена здійснювати Інспекція з питань оборони.

Всі установи шляхом здійснення внутрішнього нагляду повинні забезпечувати регулярний моніторинг та оцінку діяльності кожного співробітника й установи в цілому в напрямі дотримання положень законодавства стосовно обігу класифікованої інформації.

Законодавство Словенії про державну таємницю базується на конституції країни. Основний нормативно-правовий акт, яким регламентовано статус державної таємниці, – Акт Республіки Словенія "Про класифіковану інформацію". Ним визначено, що класифікованою є інформація, яка стосується діяльності управлінських структур Республіки Словенії у сферах громадської безпеки, оборони, зовнішніх справ, діяльності розвідувальних та безпекових структур країни; віднесена до такого виду інформації та має відповідний гриф. Відповідальність за збереження такої інформації покладається на того, кому така інформація довірена.

Доступ до класифікованої інформації мають лише особи, повноваження чи виконання службових завдань яких передбачають необхідність роботи з таким видом інформації.

Допуск до інформації з грифом таємно, цілком таємно та особливої важливості надається Міністерством внутрішніх справ, Міністерством оборони й Агенцією з питань розвідки та безпеки. Посадовим особам і співробітникам зазначених структур, яким необхідний допуск до класифікованої інформації у зв'язку із виконанням своїх повноважень чи завдань, він може бути наданий Міністром внутрішніх справ, Міністром оборони й керівником Агенції з питань розвідки та безпеки відповідно до чинного законодавства. Повідомлення про надання допуску конкретній особі надсилається до Бюро Республіки Словенії з питань захисту класифікованої інформації. Допуск особам, яким він необхідний для виконання своїх завдань у інших організаціях, надається міністром внутрішніх справ, а в разі, якщо передбачено виконання завдань, пов'язаних з обороною або проходженням військової служби, міністром оборони (проведення спеціальної перевірки в такому випадку регламентується окремими положеннями).

Особа, яка отримала допуск до класифікованої інформації, зобов'язується підписати ознайомлення з положеннями Акта Словенії "Про класифіковану інформацію", а також іншими нормативно-правовими документами, які регламентують питання захисту класифікованої інформації. У разі відмови підписання допуск анулюється.

Особи, які мають допуск до інформації з грифом "таємно" проходять спецперевірку кожні десять років, а ті, хто мають допуск до інформації з грифом "цілком таємно" та "особливої важливості", – кожні 5 років.

Правом доступу до класифікованої інформації без отримання допуску володіють:

- президент республіки;
- прем'єр-міністр;
- державні радники;
- мери та муніципальні радники;
- міністри й керівники урядових служб, безпосередньо підпорядковані прем'єр-міністру;
- омбудсмен та заступники омбудсмена;
- керівник, заступник керівника й віце-керівник центрального банку;
- члени суду присяжних;
- судді;
- прокурори;
- генеральний прокурор.

Усі посадові особи та співробітники державних установ отримують допуск до інформації визначеної форми після вступу на посаду, підписання заяви про ознайомлення з документами, що регламентують порядок охорони класифікованої інформації та взяття зобов'язань про належне поводження з класифікованою інформацією відповідно до зазначених нормативно-правових актів.

Керівник установи для виконання термінових завдань може дозволити особі тимчасовий доступ до класифікованої інформації до закінчення проведення спецперевірки, якщо оцінка даних, поданих у анкеті, не виявила підстав для відмови у наданні допуску. Тимчасовий допуск закінчується з моменту отримання допуску на законних підставах.

Інформація, яка була засекречена для покриття кримінального злочину, перевищення службових повноважень або з будь-якою іншою протиправною метою не може уважатися класифікованою.

Інформація може бути віднесена до класифікованої уповноваженими на те особами на умовах, визначених Актом. Уповноваженими особами є:

1) керівник установи;

2) обрана чи призначена посадова особа органу державної влади, уповноважена класифікувати інформацію відповідно до законодавства або відповідно до розпоряджень керівництва;

3) працівники установи, яких керівник уповноважив надавати інформації статусу класифікованої, шляхом видання письмового розпорядження.

Особи, зазначені у п. 2 та п. 3, не можуть нікому делегувати свої повноваження.

Право надання інформації грифу "особливої важливості" належить президенту країни, президенту Національної асамблеї, прем'єр-міністру, міністрам та керівникам установ при міністерствах, окремим воєначальникам, визначеним міністром оборони, керівникам установ, безпосередньо підпорядкованим прем'єр-міністру.

Спосіб та процедура віднесення інформації до класифікованої у комерційних структурах, закладах чи організаціях, які у зв'язку з виконанням своїх повноважень отримують чи мають у своєму розпорядженні інформацію, яка відповідає ознакам класифікованої, розробляє міністр оборони за погодженням із міністром внутрішніх справ.

Особа, яка своєю дією або бездіяльністю порушила положення про використання чи захист державної таємниці, несе дисциплінар-

ну або кримінальну відповідальність у встановленому законом порядку.

Прийняття у Словенії Акта “Про класифіковану інформацію” відображає ставлення цієї країни до класифікованої інформації, зокрема регламентацію охорони державної таємниці, притаманну державам – членам НАТО.

*Скулиш Є.Д.,*
*доктор юридичних наук, професор,*
*заслужений юрист України,*
*Національна академія Служби безпеки України*

## СТРАТЕГІЧНІ БЕЗПЕКОВІ ПРІОРИТЕТИ ЗАРУБІЖНИХ КРАЇН В ІНФОРМАЦІЙНІЙ СФЕРІ

Бурхливий розвиток інформаційних технологій наприкінці XX ст. –початку XI ст., їх вплив на стан захищеності національної державності та основних суспільних цінностей зумовили необхідність перегляду стратегій національної безпеки провідними країнами світу.

Зміна стратегічних пріоритетів безпекової сфери окремих держав, безумовно, вимагає оновлення концепції забезпечення національної безпеки України. При цьому слід ураховувати інтегральні чинники впливу, які формуються внаслідок синергетичної взаємодії іноземних суб’єктів сектору безпеки в процесі забезпечення національних інтересів відповідно до нових стратегій. З огляду на це комплексна оцінка стратегічних безпекових намірів зарубіжних країн в інформаційній сфері потребує наукового дослідження.

Аналіз досліджень і публікацій щодо нормативно-правового забезпечення інформаційної безпеки [1–3] свідчить, що питання впливу сучасних стратегічних пріоритетів інших країн в інформаційній сфері на стан національної безпеки України раніше не вивчались. Ми ж розглядали питання забезпечення інформаційної безпеки держави в епоху розбудови інформаційного суспільства та фактори впливу на формування системи інформаційної безпеки в Україні [4; 5].

Особливості стратегій національної безпеки окремих країн досліджували К.Артамонова, Н.Бєлоусова, О.Колотуха, О.Хилько, С.Чирков [6–10]. Водночас, не проводився їх порівняльний аналіз та не вивчався комплексний вплив цих системоутворювальних для безпекової сфери нормативно-правових актів на формування конце-

пції забезпечення національної безпеки України з урахуванням останніх змін, зумовлених високим рівнем інформатизації суспільства.

Визначимо сучасні виклики національній безпеці України на основі узагальнення особливостей безпекових стратегій зарубіжних країн в інформаційній сфері.

Зміни концептуального характеру, які відбулись у стратегії національної безпеки Сполучених Штатів Америки, відображені у Доповіді комісії з національної оборони [11]. Згідно з нею головною стратегічною метою держави Комітет начальників штабів США визначив "усеосяжне панування", основною складовою досягнення якого виступає інформаційне домінування в усіх сферах: воєнній, фінансовій, торгівельній, психологічній, юридичній та інших.

У процесі виникнення та розвитку новітніх інформаційних технологій, формування й становлення інформаційного суспільства в США було розроблено декілька моделей забезпечення інформаційної безпеки держави.

Серед численних аналітичних напрацювань у цій сфері на особливу увагу заслуговує концепція Джозефа С.Ная та Уільяма А.Оуенса [12], яка передбачає створення абсолютної системи захисту США як держави-інфолідера від будь-якого виду наступальної інформаційної зброї, що зумовлює пошук іншими державами альянсу взаємодії у військово-інформаційних діях із державою-інфолідером. При цьому може бути використано систему жорсткого контролю над інформаційним озброєнням противника на підставі потенційних міжнародних безпекових документів.

Таким чином, розглядаючи еволюцію підходів до місця і значення інформаційної складової в забезпеченні національної безпеки США, можна дійти висновків, що трансформація суспільства під впливом інформаційних технологій спричинила необхідність перегляду поняття інформаційної безпеки як ключової ланки системи національної безпеки та появу нових підходів і моделей щодо її забезпечення з їх подальшим практичним утіленням.

Основним документом *Великої Британії* у сфері забезпечення національної безпеки є Стратегія національної безпеки [13], яка називається "Сильна Британія в епоху невизначеності". У цьому програмному документі виділяється 16 найбільш серйозних загроз. Згідно із Стратегією національної безпеки Великої Британії пріоритетними напрямами забезпечення оголошені інформаційна безпека й антитерористичні заходи. У документі зазначається, що кібератаки держав, злочинців й екстремістських груп є однією з найбільш актуальних проблем національній безпеці. Кібершпигунство з боку інших урядів, терористичні атаки на системи електро-, газо- й водопо-

стачання і злочини, які вчиняються в інтернеті, розглядаються тепер як найбільш вагомі загрози.

У березні 2011 року уряд Великої Британії опублікував ІКТ-стратегію [14], яка покликана радикально скоротити витрати і підвищити ефективність державних інформаційно-телекомунікаційних систем. Відповідно до цієї стратегії, крім стимулювання програмного забезпечення з відкритим кодом і відкритих стандартів, уряд має намір істотно спростити доступ невеликих та середніх компаній до участі в державних ІТ-проектах. На увагу заслуговують також плани британського уряду зі створення єдиного реєстру державних ІТ-систем.

Особливістю стратегії забезпечення національної безпеки Великої Британії в інформаційній сфері є значна увага до заходів розвитку власної ІТ-інфраструктури, а також короткостроковість планування, що надає конкретності їх реалізації.

Базовим нормативним актом, у якому визначаються стратегічні напрями державної політики *Франції* у сфері забезпечення безпеки, є Біла книга оборони та національної безпеки від 2008 року [15]. У ній серед найбільш імовірних загроз територіям Франції та європейській спільноті названі: масштабні атаки на інформаційні системи, шпіонаж й стратегічний вплив. Загроза шпіонажу та стратегічного впливу обґрунтовується поширенням застосування у міждержавних відносинах засобів "м'якої сили", маніпулювання свідомістю через ЗМІ та інтернет; небезпекою культурної експансії.

Слід зауважити, що загрози, пов'язані з використанням інформаційних систем та засобів інформаційного впливу, є особливістю Білої книги оборони та національної безпеки Франції 2008 року. Концепція забезпечення безпеки орієнтована на досягнення лідерства в інформаційному просторі, але не заперечує провідної ролі адміністративних органів ЄС в організації заходів безпеки для інформаційно-телекомунікаційних систем, що зумовлюється необхідністю захисту взаємозалежної критичної інфраструктури.

Стратегія національної безпеки *Російської Федерації* до 2020 року [16] в умовах переходу до нової державної політики у сфері безпеки висуває вимоги до подолання технологічного відставання найважливіших галузей інформатизації, телекомунікації та зв'язку, зокрема систем державного й військового управління, управління екологічно небезпечними виробництвами і критично важливими об'єктами, а також забезпечення умов для гармонізації національної інформаційної інфраструктури з глобальними інформаційними мережами й системами.

Ключовим моментом політики РФ із питань забезпечення національної безпеки в інформаційній сфері є усвідомлення необхідності захисту будь-яких інформаційних ресурсів та інформаційних тех-

нологій, неправомірне поводження з якими може завдати збитку їх власнику, користувачу або іншій особі і всій державі в цілому. Такий підхід, на нашу думку, з одного боку забезпечує охоплення усього спектра "інформаційних" загроз, натомість з іншого – розпорошує зусилля суб'єктів сектору безпеки.

Порівняльний аналіз чинних стратегій національної безпеки США, Великої Британії, Франції, Російської Федерації свідчить, що на сьогодні найбільш актуальними загрозами сучасності є проблеми кібернетичної безпеки та поширення засобів інформаційного впливу. Стратегічні наміри провідних країн світу у сфері безпеки спрямовані на розвиток потужних інформаційно-телекомунікаційних засобів і досягнення домінування в інформаційному просторі. Останнє вочевидь суперечить національним інтересам інших держав, зокрема України.

З огляду на викладене подальше удосконалення вітчизняного законодавства у сфері національної безпеки слід здійснювати з урахуванням стратегічних пріоритетів зарубіжних країн в інформаційній сфері.

## ЛІТЕРАТУРА

1. Горовий В. Інформаційний суверенітет: актуальні питання теорії і практики / В.Горовий // Інформаційна безпека людини, суспільства, держави. – 2010. - № 1 (3). – С. 19–25.

2. Хлевицький В. Проблемні питання забезпечення інформаційної безпеки держави – стан і шляхи їхнього вирішення в Україні / В.Хлевицький // Інформаційна безпека людини, суспільства, держави. – 2010. – № 1 (3). – С. 66–70.

3. Солодка О.М. Інформаційна безпека України в умовах сучасних інтеграційних процесів / О.Д.Довгань, О.М.Солодка // Інформаційна безпека людини, суспільства, держави. – 2011. – № 1 (5). – С. 28–37.

4. Скулиш Є. Інформаційна безпека в епоху розбудови інформаційного суспільства / Є.Скулиш // Інформаційна безпека людини, суспільства, держави. – 2010. – № 1 (3). – С. 6–9.

5. Скулиш Є.Д. Фактори впливу на формування системи інформаційної безпеки в Україні / Є.Скулиш // Інформаційна безпека людини, суспільства, держави. – 2011. – № 2 (6). – С. 22–27.

6. Артамонова К.О. Політика інформаційної безпеки як стратегія кіберзлочинності у Франції [Електронний ресурс] / К.О. Артемонова. – Режим доступу : http://www.nbuv.gov.ua/portal/Soc_Gum/Gileya/2011_55/Gileya55/SL1_doc.pdf.

7. Бєлоусова Н.Б. Концептуальні засади стратегії інформаційної безпеки США за адміністрації Барака Обами [Електронний ресурс] / Н.Б.Бєлоусова. – Режим доступу : http://www.kymu.edu.ua/vmv/v/p02/02%20belousova.pdf.

8. Чирков С.Ю. Нові стратегічні концепції Росії, США та НАТО: можливість подолання існуючої ворожості [Електронний ресурс] / С.Ю.Чирков. – Режим доступу : http://www.nbuv.gov.ua/portal/Soc_Gum/Vonu_sip/2010_14/pdf/str_164-170.pdf.

9. Хилько О.Л. Французьке бачення сучасної європейської безпеки і оборони [Електронний ресурс] / О.Л.Хилько. – Режим доступу : http://www.nbuv.gov.ua/portal/natural/Vsntu/2010/polit/112-SevNTU/112-42.pdf.

10. Колотуха О.Ю. Політика Франції щодо розбудови системи європейської безпеки за президентства Ніколя Саркозі [Електронний ресурс] / О.Ю.Колотуха. – Режим доступу : http://www.nbuv.gov.ua/portal/Soc_Gum/Gileya/2012_58_dod/Gileya58d/ P17_doc.pdf.

11. Transforming Defense National Security in the 21-st Century : Report of the National Defense Panel [Електронний ресурс]. – Режим доступу:
http://www.dod.gov/pubs/foi/administration_and_Management/other/902.pdf.

12. Най Джозеф С. Главная сила Америки – ее информационные возможности [Електронний ресурс] / Най С.Джозеф, Уильям А.Оуэнс. – Режим доступу : http://www.bigpi.biysk.ru/aaa/BCE/information/gjcom6.htm.

13. A Strong Britain in an Age of Uncertainty: The National Security Strategy [Електронний ресурс]. – Режим доступу : http://www.cabinetoffice.gov.uk/sites/default/files/resources/national-security-strategy.pdf.

14. Government ICT Strategy [Електронний ресурс]. – Режим доступу : http://www.cabinetoffice.gov.uk/media/317444/ict_strategy4.pdf.

15. Defense et Securite nationale: le Livre Blanc [Електронний ресурс]. – Режим доступу : http://www.diplomatie.gouv.fr/fr/IMG/pdf/0000.pdf.

16. Стратегия национальной безопасности Российской Федерации до 2020 года, утвержденная Указом Президента Российской Федерации от 12 мая 2009 г. № 537 [Електронний ресурс]. – Режим доступу : http://www.scrf.gov.ru/documents/99.html.

*Солодка О.М.,*
*кандидат юридичних наук,*
*старший науковий співробітник,*
*Національна академія Служби безпеки України*

# ІНФОРМАЦІЙНИЙ СУВЕРЕНІТЕТ УКРАЇНИ

У сучасному світі створюється єдина глобальна комунікаційна система. У цьому процесі беруть участь держави, міжнародні інформаційні агенції, транснаціональні медійні корпорації, неурядові правозахисні організації тощо. Формується світовий медійний ринок, місце, "де виробляється й застосовуються формальні та неформальні правила, що визначають характер загальноприйнятих наративів, простір, де сперечаються ідеології та формуються альянси, що визначають урешті-решт долю урядів та націй, арена, на якій образи, породжені ЗМІ, стають знаменником сили" [1].

Отже, на сьогодні інформаційний простір активно формується й держава прагне встановити контроль лімітування кордонів і позначити власну територію в глобалізованому середовищі.

Одна з головних причин глобалізації – розвиток виробничих сил і засобів інформації, їх інтернаціоналізація. Цьому сприяє швидкість поширення інформації та можливість прямого спілкування людей, які перебувають у будь-якому місці на планеті; технічна свобода виходу в широкий ефір; багаторазове зростання аудиторії; доступність інформації та її повнота з будь-яких питань у міжнародних масштабах; доступність комп'ютерних технологій і копіювальної техніки. Усі ці зміни так чи інакше приводять до змін сфер життя, зокрема політичної.

Суверенітет у політичній науці – найважливіша ознака держави у вигляді її повної самостійності, тобто верховенства внутрішньої політики та незалежності в зовнішній.

В усі часи суверенітет держав обмежувався багатьма факторами. У сучасних умовах виникає необхідність переосмислення та переоцінки поняття "суверенітет". При цьому все більше простежується тенденція відмови від частини національного суверенітету на користь наднаціональних і світових спільнот, міжнародних організацій.

Отже, виходячи з викладеного, інформаційна безпека України є складовою її національної безпеки, а національна безпека, як і її складові, базується на такому явищі, як суверенітет.

У статті 3 Закону України "Про основи національної безпеки" інформаційне середовище визнано об'єктом національної безпеки, а

забезпечення інформаційного суверенітету України – одним з основних напрямів державної політики з питань національної безпеки в інформаційній сфері [2].

Так, у ст. 1 Закону України "Про національну програму інформатизації" ідеться, що "інформаційний суверенітет держави – здатність держави контролювати й регулювати потоки інформації з-поза її меж з метою додержання законів України, прав і свобод громадян, гарантування національної безпеки" [3]. У ст. 23 Закону України "Про науково-технічну інформацію" визначено, що основою інформаційного суверенітету є національні інформаційні ресурси [4]. Поняття "національні інформаційні ресурси" охоплює усі сфери людської діяльності, в результаті якої виникає інформація, яка в процесі інформаційної діяльності перетворюється на інформаційний ресурс [5, с. 2, 3].

Чинне законодавство не визначає правовий статус інформаційного простору України – передумову формування інформаційного суспільства, входження України у світове інформаційне співтовариство, один із головних чинників збереження інформаційного суверенітету, зміцнення державності та забезпечення національної безпеки.

Іноземний досвід і вітчизняні наукові дослідження свідчать про те, що сформулювати юридично обґрунтовані поняття "інформаційний простір України", "інформаційний суверенітет України" можна, враховуючи сукупність елементів інформаційного простору держави та напрями державної інформаційної політики, що передбачено поняттям "національний інформаційний простір", і виходячи виключно із суверенного права України на самостійне й незалежне вирішення цього питання.

## ЛІТЕРАТУРА

1. Монро Прайс. Средства массовой информации и суверенитет / Монро Прайс // Отечественные записки. – 2003. – № 4.

2. Закон України "Про основи національної безпеки" від 19.06.2003 р. № 964 // Відомості Верховної Ради України. – № 39. – Ст. 351.

3. Закон України "Про національну програму інформатизації" [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80.

4. Закон України "Про науково-технічну інформацію" від 02.09.1997 року № 2658-XII ВР // Відомості Верховної Ради України. – 1997. – № 48. – Ст. 650.

5. Приймак Ю.Ю. Національні інформаційні ресурси – джерело державних інформаційних продуктів та послуг [Електронний ресурс] / Ю.Ю.Приймак. – Режим доступу до статті : http://archive.nbuv.gov.ua/e-journals/dutp/2009_2 /doc_pdf/Priymak.pdf.

*Строгий В.І.,*
*кандидат юридичних наук,*
*старший науковий співробітник,*
*Національна академія Служби безпеки України*

## ІНФОРМАЦІЙНА БЕЗПЕКА: ТЕОРІЯ, ПРАКТИКА, СИСТЕМА ЗАХИСТУ

Сучасна епоха ознаменувалась становленням інформаційного суспільства. У період глобальної інформатизації виникає потреба у використанні органами державної влади, місцевого самоврядування, громадськими організаціями та об'єднаннями інформаційних ресурсів і розроблення системи їх захисту з метою подальшого ефективного розвитку держави й забезпечення інтересів громадян.

У сучасних умовах інформація стає стратегічним продуктом. Здатність суспільства та його інститутів збирати, накопичувати й використовувати інформацію, забезпечувати свободу інформаційного обміну є важливою передумовою соціального та технологічного прогресу, чинником національної безпеки, однією з основ успішної внутрішньої й зовнішньої політики.

Водночас склалися такі передумови, які вимагають прискореного розвитку інформаційного суспільства в Україні. Насамперед, це пов'язано із соціально-економічною нерівністю, яка виникає між розвинутими країнами і країнами, що розвиваються, внаслідок суттєвої різниці в темпах зростання обсягів та номенклатури товарів і послуг, які виробляються й надаються за допомогою інформаційно-комунікаційних технологій. Така нерівність негативно впливає на конкурентоспроможність країн і життєвий рівень людей. У зв'язку з цим усе більш істотне місце починають займати питання забезпечення інформаційної безпеки держави.

У загальному плані інформаційна безпека – це стан захищеності інформаційного простору, який забезпечує формування та розвиток цього простору в інтересах особи, суспільства й держави. Згідно з

документами Всесвітнього саміту з питань інформаційного суспільства забезпечення інформаційної інфраструктури, організацій і громадян (e-Safety) є також одним з основних напрямів розбудови інформаційного суспільства. При цьому інформаційна безпека в сучасному світі, коли саме та чи інша інформація впливає на прийняття державою тактичних і стратегічних рішень, уважається основою національної безпеки.

У Стратегії національної безпеки України "Україна у світі, що змінюється", затвердженій Указом Президента України від 8 червня 2012 року № 389/2012, визначається, що життєво важливі національні інтереси України реалізуються в складному внутрішньому та зовнішньому середовищі, яке характеризується низкою викликів і загроз, а забезпечення сприятливих зовнішніх умов для розвитку та безпеки держави передбачає, зокрема, забезпечення інформаційної безпеки при інтеграції до структур глобального інформаційного суспільства.

Питання забезпечення інформаційної безпеки як частини безпекового середовища країни наразі набувають особливої актуальності.

У статті 17 Конституції України визначено, що захист суверенітету й територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу. Це конституційне положення підкріплюється Стратегією національної безпеки України "Україна у світі, що змінюється", в якій забезпечення інформаційної безпеки визнане складовою державної політики національної безпеки та полягає, зокрема, у стимулюванні виробництва сучасних засобів і систем захисту інформаційних ресурсів, створенні національної системи кібербезпеки.

Від обсягу, швидкості та якості оброблення інформації значною мірою залежить ефективність управлінських рішень; зростає значення методів управління з використанням інформаційних технологій соціальними й економічними процесами, фінансовими і товарними потоками, аналізу та прогнозування розвитку внутрішнього й зовнішніх ринків. Застосування інформаційних технологій визначає структуру і якість озброєнь, рівень їх достатності, ефективність дій збройних сил. Спроможність ідентифікувати науково-технічні та екологічні проблеми, здійснювати моніторинг їх розвитку і прогнозування наслідків безпосередньо залежить від ефективності використовуваної інформаційної інфраструктури.

Отже, інформаційна безпека є невід'ємною складовою кожної зі сфер національної безпеки, а також важливою самостійною сферою

забезпечення національної безпеки. Саме тому розвиток України як суверенної, демократичної, правової та економічно стабільної держави можливий тільки за умови забезпечення належного рівня її інформаційної безпеки.

*Табаков В.З.,*
*кандидат технічних наук, доцент,*
*Інститут підготовки кадрів*
*державної служби зайнятості України*

## ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В СИСТЕМЕ ЗАКОНОДАТЕЛЬСТВА УКРАИНЫ

Внимание к проблеме надежности и безопасности интернета и телекоммуникаций в современном обществе постоянно растет. Задача построения действенной общеевропейской системы защиты от кибертерроризма находится в центре внимания стран Европейского Союза. В отчете Европейского агенства по сетевой и информационной безопасности (ENISA) о наиболее значимых инцидентах в Европейском Союзе за август 2012 года рассмотрены примеры пяти инцидентов нарушения информационной безопасности и произведен анализ действенности статей законодательства Европейского Союза, направленных на защиту от этих нарушений.

Вот эти пять примеров: 1. Появление на форумах хакеров в июне 2012 года 6 млн 500 тыс. паролей пользователей социальной сети, имеющей бизнес направленность. 2. Нарушение электроснабжения телекоммуникационных сетей Норвегии, Швеции и Финляндии в декабре 2011 года штормом Дагмар, в результате чего миллионы пользователей около двух недель оставались без телефонной связи и интернета. 3. Сбой центра обработки смарт-данных в Великобритании в октябре 2011 года. 4. Нарушение летом 2011 года безопасности голландского центра сертификации PKI. 5. Перенаправление в апреле 2010 года на крупных сайтах электронной коммерции, таких как www.amazon.de, www.dell.com, а также доменных областях mil, gov и других, 15% мирового интернет-трафика через китайские серверы в течение 20 минут.

Значительные сбои и нарушения данных получают широкое освещение в средствах массовой информации, что свидетельствует о значимости информационной безопасности для общества. Однако многие нарушения остаются незамеченными и, если и обнаружива-

ются, то о них не сообщается ни органам власти, ни широкой общественности. Не существует общей точки зрения относительно кибернетических инцидентов, их причин и последствий для пользователей. Непрозрачность и отсутствие информации об инцидентах приводит к тому, что политикам трудно понять их общественную значимость, причины и возможные взаимосвязи. Такое положение дел осложняет обоснованность принятия решений о выделении средств для технологического противодействия кибернетическим инцидентам и решение задачи противодействия киберинцидентам в правовом поле. И, наконец, оставляет клиентов в неведении относительно частоты и степени влияния киберинцидентов. В обществе растет угроза кибертерроризма, а государственные структуры не в состоянии ни адекватно оценить его общественную опасность, ни вообще хоть как-то противодействовать кибертерроризму. Мало того, заинтересованность государственных структур в обработке все большего количества данных, в том числе и персонального характера, переводит вопросы защиты от кибертерроризма в плоскость противостояния интересов государственных структур и личных интересов граждан. Это в частности касается и практики защиты персональных данных в системе законодательства Украины.

Адекватное законодательное регулирование общественных отношений в сфере противостояния кибертерроризму для государственных структур в Украине становится все более значимым в связи с принятием Украиной на современном этапе активных мер по адаптации национального законодательства к законодательству Европейского Союза. Что касается инцидентов, связанных с нарушением информационной безопасности первого типа, то в настоящее время директива ЕС, имплементированная в национальное законодательство, обязывает провайдеров сообщать об инцидентах национальной власти. В отчете ENICA приведен краткий анализ статей законодательства ЕС в области кибербезопасности, показана схема действий и информационных потоков, направленных на реализацию мер по борьбе с кибертерроризмом.

Рамочная директива Реформы телекоммуникаций “Безопасность и неприкосновенность”, принятая в 2009 году, дополнена статьей 13а, касающейся безопасности и неприкосновенности общественных электронных коммуникационных сетей и услуг. В частности в ней говорится: провайдеры сетей связи общего пользования и услуг обязаны принять меры, чтобы гарантировать безопасность и целостность своих сетей; провайдеры обязаны сообщать в компете-

нтные национальные органы о существенных нарушениях безопасности; национальные власти обязаны информировать ENISA и власти за рубежом, когда это необходимо, например, в случае инцидентов, связанных с транснациональным воздействием; национальные власти обязаны предоставлять ENISA и ЕС ежегодные информационные отчеты об инцидентах.

В мае 2012 года ENISA получил первый набор ежегодных докладов от государств-членов касаемо инцидентов, проишедших в 2011 году. ENISA получил 51 отчет об инцидентах, порог общественной опасности которых превысил согласованный уровень. В докладах описаны услуги, оказанные пострадавшим, количество пользователей, пострадавших, продолжительность, причины, меры и выводы. Несмотря на то, что это был первый набор отчетов об инцидентах, эти отчеты уже предоставили ценную информацию о типах угроз, имеющих место в Европейском секторе электронных коммуникаций. Информация из отчетов об инцидентах используется для выработки общеевропейской стратегии кибербезопасности и при организации пан-европейских учений Cyber Security.

Статья 4 директивы электронной конфиденциальности реформы телекоммуникаций “Безопасность обработки” также была изменена в части, касающейся защиты данных и конфиденциальности, связанных с предоставлением услуг государственными электронными коммуникационными сетями. Поставщикам услуг вменяется в обязанность: принять соответствующие технические и организационные меры для обеспечения безопасности услуг; уведомлять о нарушениях конфиденциальности персональных данных компетентные национальные органы; уведомлять об утечке данных абонентов или частных лиц, когда нарушения конфиденциальности их персональных данных могут отрицательно повлиять на их личную жизнь; производить регистрацию нарушений безопасности персональных данных, в том числе фактов, связанных с нарушениями, последствия которых ликвидированы и меры по исправлению которых приняты.

На рис. 1 представлена содержащаяся в отчете ENISA общая модель взаимодействия акторов в сфере кибербезопасности в соответствии с законодательством ЕС. На схеме показаны провайдер, национальные органы власти, зарубежные представительства национальных органов, ЕС, ENISA, общественность и жертва.

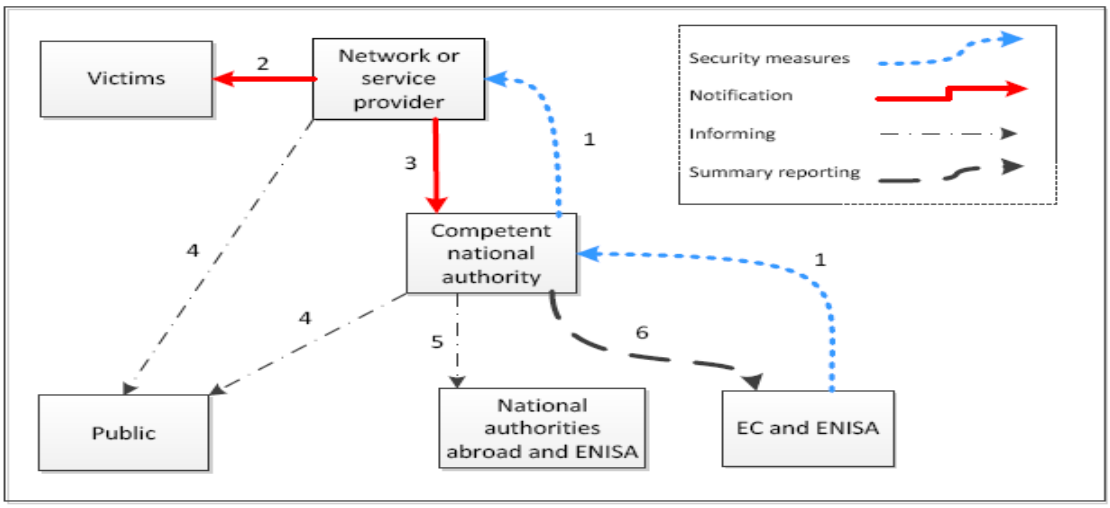



Рис. 1 Общий вид действий и информационных потоков

Стрелками показаны: меры обеспечения безопасности (1), оповещение (2, 3), информирование (4, 5), отчетность (6).

## ЛИТЕРАТУРА

1. Cyber Incident Reporting in the EU: An overview of security articles in EU legislation./ ENISA, August 2012. – 14 p.

*Тихомиров О.О.,*
*кандидат юридичних наук,*
*Навчально-науковий інститут інформаційної безпеки*
*Національної академії Служби безпеки України*

## КІБЕРЗЛОЧИН: ТЕОРЕТИКО-ПРАВОВІ ПРОБЛЕМИ

Актуальність протидії кіберзлочинності сьогодні не викликає сумнівів, а з подальшим інформаційним розвитком України вона буде дедалі посилюватись. Масштаби кіберзлочинності як транснаціонального явища зумовлюють численні проблеми практичного й наукового характеру, вирішення яких може забезпечити нівелювання негативного впливу та мінімізацію темпів і форм його розвитку.

Важливість протидії кіберзлочинності вже визнана світовою спільнотою у відповідних правових актах міжнародного рівня, що вивело її проблеми за межі кримінологічної та криміналістичної площини, в яких коріниться їх походження та причини актуалізації. “Кіберзлочин”, ставши предметом міжнародного і національного

правового регулювання, увібрав у себе зокрема проблеми, пов'язані з правовою імплементацією, удосконаленням і гармонізацією національного законодавства та зумовив необхідність його теоретико-правового осмислення.

Однією з проблем, на якій доцільно акцентувати увагу, є проблема понятійно-термінологічна. Термін "кіберзлочин", яким зараз у наукових колах прийнято позначати специфічні види злочинів, віднесених до так званої "кібернетичної сфери", набув на пострадянському просторі достатньо широкого вжитку не маючи сформованого загальновизнаного юридичного наповнення. Залишається невирішеним питання установлення співвідношення "кіберзлочину" з такими поняттями, як "комп'ютерний злочин", "злочин у сфері комп'ютерної інформації", "злочин у сфері використання комп'ютерів", "злочин у сфері використання інформаційних технологій", або із законодавчим в Україні поняттям "злочин у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку"; концептуального визначення місця "кіберзлочину" в системі протиправних діянь, передбачених національним законодавством: як окремого виду цих діянь, як специфічної форми їх скоєння, як того й іншого.

Все це ставить під великий сумнів доцільність і можливість нормативного визначення кіберзлочину і впровадження його як окремого виду злочинів кримінальним правом. Шляхом вирішення цієї проблеми є ґрунтовне загально-теоретичне осмислення тієї змістовної частини поняття "кіберзлочин", яку надає приставка "кібер-", враховуючи аксіологічні, етимологічні, семантичні її особливості, а також історію виникнення і розвитку самого явища кіберзлочинності. Означена проблема належить до низки проблем формування понятійно-термінологічного апарату сфери кібернетичної безпеки, які мають вирішуватись комплексно [1].

Іншим проявом понятійно-термінологічної проблеми є запозиченість поняття "кіберзлочинність" з певним закладеним в нього змістом з міжнародних правових актів, зокрема з Конвенції про кіберзлочинність [2], які створені державами з різними типами правових системи та різним уявлення про поняття "злочин". Надане ними розуміння кіберзлочинності є достатньо узагальненим і абстрагованим від правової системи конкретної держави і не може в повній мірі відповідати її особливостям, що додатково породжує проблеми нормативно-правової імплементації.

Так, для правової системи України характерним є поділ протиправних діянь на дві групи: злочини (найбільш суспільно небезпечні правопорушення, за які передбачена кримінальна відповідальність) і

проступки (всі інші правопорушення, за які передбачена юридична відповідальність інших видів, зокрема адміністративна, цивільна, дисциплінарна). Причому не вважаються злочинами діяння, які не мають високого ступеню суспільної небезпеки (не наносять значної суспільної шкоди) навіть якщо вони за всіма іншими ознаками відповідають злочину. Враховуючи високий рівень латентності кіберзлочинності, який зумовлює прихованість реальних обсягів її негативних наслідків, можливості застосування такого критерію як обсяг суспільної шкоди або ступінь суспільної небезпеки в якості визначального при кваліфікації правопорушень в кібернетичній сфері є достатньо обмеженими. Крім того питання виокремлення "кіберпроступку" як виду правопорушень майже не розглядається [3], що залишає поза межами державно-правового реагування значну кількість діянь, які поодинці не наносять значної суспільної шкоди і, відповідно, не можуть кваліфікуватися як "злочини", але у своїй масі створюють значну суспільну небезпеку. Серед них можуть бути і кіберзлочини у латентній формі, які також залишаться без належного реагування.

Остання проблема може додатково посилитись новелами Кримінального процесуального кодексу України, що започатковує впровадження нового для правової системи України виду правопорушень – кримінального проступку, який у майбутньому буде мати окрему регламентацію матеріальним кримінальним правом.

Теоретико-правовою проблемою іншого характеру є проблема ефективності правових засобів протидії кіберзлочинності та адекватності їх застосування, яка лежить в площині загальної проблеми правового розвитку України.

Згідно положенням теорії права правовий вплив може здійснюватись на двох рівнях:

– на свідомість індивідів, який передбачає широке використання методу переконання в процесі правової освіти та виховання з метою формування внутрішніх мотивів та стимулів правомірної поведінки індивідів;

– на поведінку індивідів, що здійснюється за допомогою застосування (або можливості застосування) методів державного примусу (такий вплив здійснюється спеціально-юридичними засобами, серед яких: юридична відповідальність, правосуддя, засоби виявлення, припинення, профілактики правопорушень тощо).

Можливості застосування методів правового впливу на свідомість індивідів в Україні сьогодні є достатньо обмеженими, по-перше, низьким рівнем правової та інформаційної культури громадян, що не дозволяє сподіватись на внутрішню мотивацію до належної (правомірної) поведінки та належний захист своїх конститу-

ційних прав, по-друге, транснаціональним характером кіберзлочинності, яка може виходити за юрисдикційні межі окремої держави. Очевидно, що за таких умов реальний потенціал дієвості має лише влив на поведінку індивідів. Це надає сьогодні особливого значення правоохоронній складовій протидії кіберзлочинності, тобто системі дієвих охоронних правових норм, передусім кримінальних, створених за єдиними міжнародними стандартами, а також ефективній діяльності правоохоронних та судових органів держави і відповідних міжнародних організацій щодо застосування цих норм.

Вирішення означених проблем може стати кроком на шляху адекватного правового сприйняття поняття "кіберзлочин", визначення необхідності та ступеня його нормативно-правового впровадження і, як наслідок, гармонізації національної правової бази стосовно діяльності, спрямованої на протидію кіберзлочинності.

## ЛІТЕРАТУРА

1. Мельник С.В. До проблеми формування понятійно-термінологічного апарату кібербезпеки // Збірник наукових праць Військового інституту Київського національного університету ім. Тараса Шевченка, Вип. 30 [Електронний ресурс] / С.В.Мельник, О.О.Тихомиров, О.С.Лєсков. – Режим доступу : http://www.nbuv.gov.ua/portal/natural/Znpviknu/2011_30/Zbirnik_30_28.pdf.

2. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 07.09.2005 №2824-IV // Відомості Верховної Ради України. – 2006. – № 5–6. – Ст. 71.

3. Тихомиров Д.О. До проблеми розмежування кіберзлочину і кіберпроступку / Д.О.Тихомиров // Актуальні проблеми управління інформаційною безпекою держави : зб. матеріалів наук.-практ. конф., м. Київ, 22 березня 2011 р. – К. : Вид-во НА СБ України, 2011. – Ч. 2. – С. 75–77.

*Ткачук Т.Ю.,*
*кандидат юридичних наук,*
*Національна академія Служби безпеки України*

## АКТУАЛЬНІ НАПРЯМИ ВЗАЄМОДІЇ ОРГАНІВ ВИКОНАВЧОЇ ВЛАДИ У СФЕРІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Дослідження практики реформування органів виконавчої влади в інформаційній сфері в нашій країні свідчать, що, як і в інших сферах, перевага тут надається, по суті, переходу від галузевої структу-

ри до функціональної. Вважається, що це сприятиме вдосконаленню взаємодії чинної системи взаємовідносин органів виконавчої влади, зокрема щодо підвищення ефективності національної інформаційної безпеки.

Формально система органів виконавчої влади у сфері національної інформаційної безпеки, в якій задіяні всі гілки влади та громадські структури, гарантує підтримку національної безпеки в державі. Проте на практиці дуже часто спостерігається відсутність чіткої та повної взаємодії.

Наразі діяльність органів виконавчої влади у сфері інформаційної безпеки України істотно ускладнена. Починаючи з 1997 р., органи виконавчої влади, що забезпечують інформаційну безпеку України, перебувають у стадії перманентної реорганізації. Тривалі структурні зміни, кадрові призначення, затвердження положень про діяльність ключових органів влади, опанування керівниками нової сфери відповідальності дозволяють дійти висновку про часткову втрату впливу на процеси в інформаційній сфері.

Позаяк, у функціонуванні окремих структур системи органів виконавчої влади у сфері національної інформаційної безпеки часто спостерігається дублювання функцій, що пояснюється різними причинами. З одного боку, це позитивний чинник (звичайно, за певних обставин). Дублювання функцій є умовою здорової конкуренції функціонально подібних структур, особливо це важливо у сфері національної інформаційної безпеки.

Але нерідко дублювання діяльності окремих органів виконавчої влади призводить до безладу та невиправданих бюджетних витрат. Це є істотним чинником, що має спонукати органи виконавчої влади до проведення постійного моніторингу функціонування структур системи та до пошуку способів оптимізації співробітництва, щоб підвищити ефективність діяльності різних структур. Проте часто спрацьовує не державний інтерес, а політичний або соціальний. Наприклад, оргструктура (яка набула статусу “п’ятого колеса до воза”) зберігається тільки через те, що не визначено, як працевлаштувати тих, хто там працює. Особливо це стосується різних координаційних і консультативних органів у системі державного управління, які створені як “постійно діючі” й мають штатних працівників. Часто такі органи формуються за ситуаційним принципом, для розв’язування нагальної проблеми, яка виникла в державі. Та після її розв’язання орган продовжує “функціонувати”.

У період інформатизації в органах виконавчої влади, які беруть участь у забезпеченні національної інформаційної безпеки, поряд із завданнями підтримки традиційних за змістом проблем національ-

ної безпеки загалом, з'являються нові, раніше не властиві (скажімо, організація системи національної інформаційної безпеки у сфері використання електронних телекомунікаційних систем, зокрема діяльності, спрямованої на протидію комп'ютерній злочинності). Така діяльність, з одного боку, є необхідною складовою традиційного процесу національної інформаційної безпеки, а з іншого – одним із нових напрямів правоохоронної діяльності, яку мають проводити відповідні державні органи в межах їх функціональної компетенції. Цю діяльність можна також віднести до внутрішньої, властивої не тільки системі правоохоронних органів. Водночас вона має загальносоціальний характер, оскільки впливає на управління інформатизацією суспільства в цілому.

Поява таких специфічних функцій, раніше не властивих органам виконавчої влади, спричиняє цілу низку проблем комплексного характеру, що можуть бути розв'язані шляхом кардинального реформування, а отже, удосконалення діяльності органів виконавчої влади. Тобто йдеться про прогнозовану на тривалий проміжок часу функцію, що потребує постійної структури для реалізації.

Відмітимо, що комп'ютерна злочинність є складовою національної інформаційної безпеки, а згідно з чинним законодавством організація та підтримка національної безпеки належить до компетенції СБУ.

Створення нової організаційної структури з метою організації взаємодії або координації діяльності наявних правоохоронних та інших органів виконавчої влади, діяльність яких пов'язана з інформатизацією відомств і протидією негативним явищам (загрозам) у цій сфері, на нашу думку, є недоцільним. Нові органи потребують додаткового бюджетного фінансування, нерідко дублюють функції раніше створених. Головне, саме сфера національної інформаційної безпеки подвійно скоординована РНБО та КМУ. Отже, додаткова координація навряд чи потрібна.

Вважаємо, що це організаційно-правове питання необхідно розв'язувати на основі чіткого розмежування функцій і завдань органів виконавчої влади, задіяних у забезпеченні національної інформаційної безпеки, особливо з функціями та завданнями СБУ щодо реалізації цього нового напряму діяльності в системі національної інформаційної безпеки. Існує думка, що потрібно створити відповідний спеціальний підрозділ у структурі Ради національної безпеки і оборони України. Це зумовлено змістом окремих рішень, ініційованих РНБО та реалізованих у низці указів Президента України. Тобто фактично згаданий орган продемонстрував свою політичну обізнаність щодо актуальності проблеми на рівні державного управління,

отже, свою компетентність. Є підстава визначити для нього нову підфункцію, що є складовою провідної координуючої функції РНБО. Конституційним органом державної влади має бути розроблена чітка політика, що передбачає колегіальне вироблення й документальне закріплення позиції щодо основних напрямів адміністративної діяльності, пов'язаної з процесами інформатизації, у тому числі у сфері національної інформаційної безпеки, зокрема з питань профілактики та протидії правопорушенням із використанням комп'ютерних технологій.

Необхідність удосконалення процесу взаємодії органів виконавчої влади у сфері інформаційної безпеки зумовлена також бурхливим розвитком соціальних відносин, зокрема електронних інформаційних відносин, що створюються на основі електронно-обчислювальної (комп'ютерної) техніки та технологій. Великі надії покладаються на впровадження досягнень науково-технічного прогресу саме в цій сфері.

Уважаємо, що з метою вдосконалення механізму взаємодії органів виконавчої влади в інформаційній сфері доцільно включити в Указ Президента України від 8 липня 2009 року № 514/2009 "Про Доктрину інформаційної безпеки України" [1] спеціальний розділ "Стан інформаційної безпеки України", в якому чітко визначити актуальні проблеми державної політики забезпечення інформаційної безпеки та зосередити увагу на необхідності їх вирішення.

## ЛІТЕРАТУРА

1. Про Доктрину інформаційної безпеки України : Указ Президента України від 8 липня 2009 року № 514/2009 [Електронний ресурс]. – Режим доступу : http://www.president.gov.ua/documents/9570.html.

*Трубін І.О.,*
*заступник завідувача лабораторії,*
*Науково-дослідний інститут фінансового права*

## ІНФОРМАЦІЙНА БЕЗПЕКА: ДИСКУСІЙНІ ПИТАННЯ

У сучасних умовах формування заходів, що пов'язані із забезпеченням інформаційної безпеки на рівні державної політики, перебуває в тісному взаємозв'язку з процесом наукового пізнання. Саме його досягнення стають своєрідним фундаментом підготовки концепцій та формулювання основних напрямів діяльності держави у відповідній сфері.

За останні роки вченим удалось досягти в цій царині значних успіхів. Зокрема, у вітчизняній науці нові знання функціонують у вигляді системи, що визначає поняття інформаційної безпеки, принципи, методи та заходи захисту інформації, стан та рівень правового забезпечення відповідних відносин тощо.

Проте, незважаючи на вказані наукові досягнення, є питання, що викликають різнобічне трактування. Серед них можна виділити, по-перше, неоднозначність трактування низки понять; по-друге, неоднозначність у поглядах вчених щодо класифікації загроз інформаційній безпеці.

В цій доповіді ми спробуємо узагальнити окремі досягнення сучасної науки, що за своєю сутністю можуть вплинути на формування державної політики інформаційної безпеки та розвиток науки в цілому, а також мають дискусійний характер.

Щодо першого мається на увазі відмінність у підходах до визначення понять: конфіденційність, цілісність та доступність.

Так, зарубіжні вчені Р.Крутц і Р.Вайнс визначають конфіденційність, цілісність та доступність основними принципами інформаційної безпеки [1, с. 8]. Ці самі поняття І.Евод трактує як завдання [5, с. 300–301].

У вітчизняному праві визначено, що поняття конфіденційності, цілісності та доступності виступають властивостями інформації. Цієї позиції дотримуються зокрема такі вчені, як Б.Кузьменко та О.Чайковська [6, с. 11]. Крім того, це підкріплюється положеннями чинного законодавства. Так, відповідно до пункту 2 Положення про технічний захист інформації в України конфіденційність, цілісність та доступність є властивостями інформації. Додатково А.Берко, В.Висоцька, І.Рішняк визначають конфіденційність, цілісність та доступність як вимоги [2, с. 20].

У цілому не можна стверджувати, що згадані вчені, за формальними ознаками, які випливають з розкриття понять конфіденційності, цілісності та доступності, висловлюють хибні твердження, оскільки залежно від ситуації застосування доречною може бути їх роль і як властивостей, і як вимог, і як завдань. Зазначене свідчить про дискусійність та необхідність додаткового наукового осмислення з метою узагальнення й систематизації наявних визначень.

Щодо другого питання, то його дискусійність підтверджується значною кількістю публікацій, у яких вчені розкривають власні погляди на класифікацію загроз інформаційній безпеці. Варто зупинити на основних із них.

Так, Б.Кузьменко та О.Чайковська пропонують класифікацію загроз, яка ґрунтується на визначенні властивостей інформації: а)

загрози порушення конфіденційності інформації; б) загрози порушення цілісності інформації; в) загрози порушення доступності інформації [7, с. 6–7].

Схожі міркування висловлює А.Логінов у власному дисертаційному дослідженні. Зокрема вчений визначає такі загрози, як: розкриття інформаційних ресурсів; порушення цілісності інформаційних ресурсів; збій у роботі обладнання [9].

Натомість С.Гуцу [3] та О.Литвиненко [8] сходяться на тому, що до основних загроз інформаційній безпеці належать: загрози впливу неякісної інформації на особистість, суспільство, державу; загрози несанкціонованого й неправомірного впливу сторонніх осіб на інформацію й інформаційні ресурси; загрози інформаційним правам і свободам особистості.

Л.Євдоченко, формуючи власний підхід до класифікації інформаційних загроз та з метою вироблення рекомендацій щодо організації державою дієвих форм і методів забезпечення інформаційної безпеки, визначає і класифікує загрози за кількома критеріями: способом впливу на об'єкти інформаційної безпеки (інформаційні, фізичні й програмно-математичні, організаційно-правові); джерелами надходження (внутрішні та зовнішні); характером вияву (політичні, економічні, організаційно-технічні) [4, с. 8].

І на останок, А.Погребняк відмічає, що загрози можуть бути як випадковими, так і навмисними, й наводить їх широкий перелік [11, с. 46–47, 50].

У підсумку варто зазначити, що наукове пізнання – процес невпинний. Тому, формуючи власну думку щодо згаданих питань, можна опинитись у ситуації, коли не врахованими залишаться більш актуальні сучасні погляди колег. Наразі вказані в доповіді питання можуть стати предметом наукової дискусії або одним із напрямів наукового дослідження. На теоретичному рівні вироблення єдиного підходу до визначення основних понять інформаційної безпеки, критеріїв класифікації загроз може розглядатись як один із способів упорядкування понятійно-категоріального апарату такої науки, як інформаційне право.

## ЛІТЕРАТУРА

1. Ronald L. Krutz. The CISSP Prep Guide–Mastering the Ten Domains of Computer Security // Ronald L. Krutz. Russell Dean Vines. – 2001. – John Wiley & Sons, Inc. – 501 p.

2. Берко А.Ю. Методи та засоби оцінювання ризиків безпеки інформації в системах електронної комерції / А.Ю.Берко, В.А.Висоцька, І.В.Рішняк // Вісник Національного університету "Львівська політехніка". – 2008. – № 610. – С. 20–33.

3. Гуцу С.Ф. Правові основи інформаційної діяльності [Електронний ресурс] / С.Ф.Гуцу. – Режим доступу : http://studrada.com.ua.

4. Євдоченко Л.О. Удосконалення системи державного забезпечення інформаційної безпеки України в умовах глобалізації: автореф. дис. … канд. наук з держ. упр. : 25.00.01 / Л.О.Євдоченко. – Л., 2011. – 24 с.

5. Илайес Эвод. Электронная коммерция. Практическое руководство / Илайес Эвод ; пер. с англ. – СПб. : ООО "ДиаСофтЮП", 2002. – 608 с.

6. Кузьменко Б.В. Захист інформації : навч. посіб. / Б.В.Кузьменко, О.А.Чайковська. – К., 2009. – Ч. 1. – 83 с.

7. Кузьменко Б.В. Захист інформації : навч. посіб. / Б.В.Кузьменко, О.А.Чайковська. – К. : Видавничий відділ КНУКіМ, 2009. – Ч. 2. – 69 с.

8. Литвиненко О. Проблема інформаційної безпеки в контексті міграційних процесів [Електронний ресурс] / О.Литвиненко. – Режим доступу : http://www.nbuv.gov.ua/portal/soc_gum/Ukralm/2012_7/lytvynenko.pdf.

9. Логінов А.В. Адміністративно-правове забезпечення інформаційної безпеки органів виконавчої влади : дис. … кандидата юридичних наук : спец. 12.00.07 – теорія управління; адміністративне право і процес; фінансове право; інформаційне право / А.В.Логінов ; Національна академія внутрішніх справ України. – К., 2005.

10. Макарова М.В. Електронна комерція : [посібник для студентів вищ. навч. закладів] / М.В.Макарова. – К. : Видавничий центр "Академия", 2002. – 272 с.

11. Погребняк А.В. Технології комп'ютерної безпеки : моногр. / Погребняк А.В. – Рівне : МЕГУ, 2011. – 117 с.

*Турченко Ю.В.,*
*Військовий інститут*
*Київського національного університету*
*ім. Тараса Шевченка*

## ІНФОРМАЦІЙНА СКЛАДОВА МІНІСТЕРСТВА ОБОРОНИ УКРАЇНИ: ЦІЛІ ТА ЗАВДАННЯ

Процеси інформатизації військової сфери потребують більш детального аналізу з боку військових та політологів. Міністерство оборони України (МОУ) є суб'єктом інформаційної політики. Інфо-

рмаційна складова Міністерства оборони полягає в реалізації державної політики у сфері безпеки та оборони в межах конституційних повноважень Міністерства оборони та визначених законами України функцій Збройних Сил України. Проаналізуємо *цілі та завдання інформаційної складової Міністерства оборони України.*

Інформаційна складова Міністерства оборони становить сукупність цілей та завдань, які відображають його інтереси в інформаційній сфері, стратегічних напрямів їх досягнення й системи заходів їх реалізації.

Короткостроковою метою інформаційної складової МОУ є оптимізація організаційно-штатної структури інформаційно-медійних підрозділів Міністерства оборони та Збройних Сил України, забезпечення ефективності діяльності військових ЗМІ.

Середньострокова мета – створення ефективного механізму системної реалізації діяльності структур Міністерства оборони в інформаційному полі для досягнення завдань державної безпеки в інформаційному полі України. У цьому вимірі діяльність інформаційної складової Міністерства оборони планується у формах:

- забезпечення стабільного позитивного подання державницьких інформаційних повідомлень в інформаційному полі України, центральних і регіональних ЗМІ; формування значного рівня впливовості медійних засобів та повідомлень Міністерства оборони і Збройних Сил, забезпечення стійкого позитивного інтересу всіх прошарків суспільства до безпекової, патріотичної, оборонної, військової тематики у зв'язку з діяльністю Міністерства оборони та Збройних Сил тощо;

- створення ефективних механізмів інформування й інформаційного супроводження, формування партнерських інформаційних структур за кордонами України у впливових інформаційних джерелах загальноєвропейського та регіонального значення.

Довгостроковою стратегічною метою інформаційної складової Міністерства оборони є формування цілісного системного інституту інформаційного впливу та взаємодії безпекового й оборонного сектору держави з громадськістю, створення ефективного інформаційного інструментарію впливу в інформаційних полях регіонів, України в цілому та за кордоном, ефективної правової бази інформаційної діяльності в безпековому секторі держави.

*Виходячи з провідних цілей МОУ, основними завданнями інформаційної складової Міністерства оборони є:*

- створення умов для формування у Збройних Силах України розвинутого інформаційного середовища як елемента прозорого, демократичного цивільного контролю над військовими формуваннями, забезпечення розвитку інфраструктури та інтегрування військ-

кових засобів масової інформації в загальнодержавну систему ЗМІ, вільний доступ до інформації;

- оптимізація інформаційно-медійної структури Міністерства оборони;

- подальше використання та розвиток сучасних інформаційних та телекомунікаційних технологій;

- створення на базі медійних засобів Міністерства оборони та розширене застосування сучасних технологій формування інформаційного контенту й комунікативних технологій;

- ефективне формування і використання військових та загальнонаціональних інформаційних ресурсів, забезпечення швидкого й вільного доступу до них;

- забезпечення військовослужбовців, членів їх сімей, громадян України суспільно важливою інформацією, створення умов для розвитку незалежних військових засобів масової інформації.

Інформаційна складова Міністерства оборони України може бути ефективною тільки за умови її комплексного та системного характеру, функціонального розподілення діяльності на відкриту та закриту для суспільства, проведення її на загальнодержавному рівні для забезпечення цілей загальнодержавної інформаційної політики у сфері національної безпеки в інформаційному полі.

Враховуючи зазначене вище, одним із джерел формування інформаційного поля для забезпечення інтересів держави та громадянського суспільства є інформаційна складова Міністерства оборони України. Більше того, вона повинна стати визначальним чинником формування інформаційного середовища в Збройних Силах України, важливим фактором створення інформаційного поля громадянського суспільства та комунікації держави на міжнародному рівні.

*Фурашев В.М.,*
*кандидат технічних наук,*
*старший науковий співробітник, доцент,*
*Науково-дослідний інститут інформатики і права*
*Національної академії правових наук України*

## ІНДИКАТОРИ СУЧАСНИХ ВИКЛИКІВ І ЗАГРОЗ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

За аналогією з тим, що безпека – стан захищеності, коли кому-, чому-небудь ніщо не загрожує, *інформаційна безпека – стан захищеності людини, суспільства, коли відсутні негативний, у загаль-*

*неприйнятому (унормованому) розумінні, вплив інформації на людину, суспільство та негативні наслідки застосування сучасних інформаційних технологій.*

Повної, не кажучи вже про абсолютну, інформаційної безпеки не може бути внаслідок сутності інформації та методів і засобів її поширення. Можна говорити лише про рівень інформаційної безпеки, його співвідношення з бажаним.

Рівень інформаційної безпеки визначається на основі сукупності кількісних та якісних характеристик певних її індикаторів. Саме тому, Стратегія національної безпеки України [1] серед механізмів реалізації державної політики національної безпеки передбачає удосконалення системи управління національною безпекою шляхом, зокрема, *розроблення та впровадження загальнодержавної системи визначення й моніторингу порогових значень показників (індикаторів),* що характеризують рівень захищеності національних інтересів у різних сферах життєдіяльності та виникнення реальних загроз національній безпеці.

Основою для визначення індикаторів, що характеризують рівень інформаційної безпеки, повинна бути, на нашу думку, саме інформація, а точніше – її властивості: повнота, вчасність, вірогідність, конфіденційність та цілісність, а також доступність і режим розповсюдження, наслідки застосування інформаційних технологій.

Виходячи з цього, *базисними індикаторами* рівня інформаційної безпеки слід уважати:

- повноту інформації *(властивості: віддзеркалення вичерпного характеру відповідності одержаних відомостей цілям збору; достатність для розуміння ситуації та прийняття рішення; характеристика, яка визначає кількість інформації, необхідної та достатньої для прийняття правильного рішення)*;
- вчасність інформації *(властивості: ознака того, що вона є саме тією, яка потрібна на цей момент; важливість, істотність у певний момент часу)*;
- вірогідність інформації *(віддзеркалення дійсності (істинного стану справ); достовірність (ступінь наближеності інформації до першоджерела або точність передання інформації)*;
- конфіденційність інформації *(властивість захищеності інформації від несанкціонованого доступу та спроб її розкриття користувачем, що не має відповідних повноважень)*;
- цілісність інформації *(показник того, що дані повні, не були змінені при виконанні будь-якої операції над ними, будь-то передавання, зберігання або подання)*;

- доступність інформації *(здатність забезпечення, за необхідності, своєчасного безперешкодного доступу до інформації, що цікавить)*;

- санкціонованість поширення інформації *(процес надання інформації споживачам у рамках обумовлених повноважень)*.

За результатом аналізу законодавчо окреслених на сьогодні шляхів запобігання реальним та потенційним загрозам у сфері інформаційної безпеки, які наводяться в законах України "Про основи національної безпеки" [2, ст. 8], "Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки" [3] та Доктрині інформаційної безпеки України [4], можна встановити на макрорівні індикатори, які визначають рівень національної інформаційної безпеки та які, на нашу думку, можна позначати як *реалізаційні індикатори*:

- наявність та достатність нормативно-правової й організаційно-розпорядчої бази у сфері забезпечення інформаційної безпеки;

- ефективність нормативно-правових та організаційно-розпорядчих передумов практичної реалізації запобігання й усунення наявних і можливих загроз у сфері інформаційної безпеки;

- достатність та ефективність економічної й програмно-технічної баз для запобігання та усунення реальних і можливих загроз в інформаційній сфері;

- спроможність протидіяти інформаційно-психологічним операціям.

Оскільки поняття "інформаційна безпека" внаслідок своєї сутності багатоаспектне, багатогранне, то й наведені реалізаційні індикатори, які не є вичерпними, також багатоаспектні, багатоскладові. Тому підкреслимо, що ці індикатори визначені *на макрорівні* й у подальшому потребують деталізації.

Від того, наскільки правильно визначені індикатори, зроблено необхідний (оптимальний) рівень їх деталізації з подальшим визначенням виміру, кількісного або якісного, кожного індикатора та їх сукупності, залежить рівень об`єктивності уявлення стану цієї складової процесу (в нашому випадку – інформаційної безпеки).

Окремо необхідно відзначити таку властивість інформаційної безпеки, як негативні наслідки застосування інформаційних технологій, які надають більше можливостей для здійснення маніпулювання суспільною свідомістю, використання персональних даних, поширення невластивих українській культурній традиції цінностей і способу життя, культу насильства, жорстокості, порнографії, зневажливого ставлення до людської й національної гідності тощо.

Саме застосування сучасних інформаційних технологій "породило" такі поняття, як "комп'ютерна злочинність" та

“комп’ютерний тероризм”, сутність яких спрямована передусім на спотворення або фальсифікацію наведених вище властивостей інформації з метою досягнення певних цілей.

Зауважимо, що, наприклад, такий злочин у сфері інформаційних технологій, як крадіжка номерів кредитних карток й інших банківських реквізитів (фішинг), потребує знання саме повної, достовірної та цілісної інформації. Злочинці в цій сфері намагаються отримати таку інформацію за будь-яку ціну.

На наше глибоке переконання, ключ до вирішення багатьох питань інформаційної безпеки полягає саме у спроможності виміряти, якісно або кількісно, такі її базисні індикатори – властивості інформації, як повнота, вчасність, вірогідність, цілісність.

## ЛІТЕРАТУРА

1. Про Стратегію національної безпеки України : Указ Президента України від 12.02.2007 року № 105/2007 // Офіційний вісник України. – 2007. – № 11. – Ст. 389.

2. Про основи національної безпеки України : Закон України від 19 червня 2003 року № 964-IV / Відомості Верховної Ради України. – 2003. – № 39. – Ст. 351.

3. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : Закон України від 09.01.2007 № 537-V // Відомості Верховної Ради України. – 2007. – № 12. – Ст. 102.

4. Про Доктрину інформаційної безпеки України : Указ Президента України від 08.07.2009 № 514/2009 // Офіційний вісник Президента України. – 2009. – № 20. – Ст. 677.

*Хлань В.Г.,*
*кандидат технічних наук,*
*старший науковий співробітник,*
*Національна академія Служби безпеки України*

## СТОСОВНО ОКРЕМИХ АСПЕКТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КОНТЕКСТІ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ СЛУЖБОЮ БЕЗПЕКИ УКРАЇНИ

Служба безпеки України відповідно до покладених на неї завдань здійснює інформаційно-аналітичне забезпечення (ІАЗ) органів державної влади та управління.

Під час прийняття державними інститутами ефективних управлінських рішень виникає потреба у врахуванні інтересів суб'єктів суспільних відносин: особи – її права на конфіденційність приватного життя; органу влади – щодо отримання повної й достовірної інформації для виконання покладених на нього функцій; суспільства – стосовно забезпечення конституційного права на інформацію про діяльність державних органів.

Значущість проблеми інформаційної безпеки випливає із сучасних тенденцій формування нового типу суспільства. Перехід до інформаційної ери, нові досягнення в маніпулюванні суспільною свідомістю зумовлюють виняткове значення дослідження цього аспекту як одного зі складових забезпечення державної безпеки.

Таким чином, створюється проблемна ситуація, яка полягає в суперечності між потребою органів державної влади в достовірній, своєчасній, актуальній і релевантній інформації та необхідністю додержання прав стосовно її отримання, накопичення, поширення й використання. Звідси виникає низка завдань, серед яких дотримання вимог щодо інформаційної безпеки на всіх етапах підготовки інформації до використання в управлінській діяльності, адже для України на сучасному етапі розвитку це питання стоїть на одному рівні із захистом суверенітету й територіальної цілісності, забезпеченням економічної безпеки.

У науковій літературі поняття інформаційно-аналітичної діяльності розглядається як особливий напрям інформаційної роботи, пов'язаний із пошуком, отриманням, опрацюванням, збереженням та поширенням інформації переважно у сфері управлінської, політичної та економічної діяльності. У той же час, для прийняття управлінських рішень важливе не стільки своєчасне ознайомлення з первинною інформацією, скільки завчасне виявлення проблемних ситуацій і прогнозування розвитку подій.

Потреба в отриманні зазначеної інформації зумовлена переходом владних структур до прогностичних форм діяльності. Останнє передбачає використання багатоваріантних моделей розвитку подій, що потребує не тільки констатації фактів (для доведення тієї чи іншої тези), а й системного підходу до розв'язання проблеми в цілому. Так, актуальності набуває достовірність інформації та можливість забезпечення її достатнього рівня за допомогою відповідних заходів з інформаційної безпеки.

Беручи до уваги той факт, що все у світі так чи інакше пов'язане з опрацюванням інформації, а будь-які дії окремих людей або колективів відображаються в інформаційних повідомленнях, під час досліджень інформаційної безпеки доцільно виділити одну з її

складових – енергоінформаційну. У такому випадку, об'єктами безпеки будуть виступати свідомість, підсвідомість особи, основними причинами небезпеки – несанкціоновані енергоінформаційні впливи, а найбільш суттєвими загрозами – неусвідомлювані кримінальні дії, зомбування і т.д.

Під час виконання своїх службових обов'язків працівники інформаційно-аналітичних підрозділів обробляють значні обсяги різнопланової інформації, яка за своєю природою має неформалізований характер. Так, у процесі аналітико-синтетичного оброблення оперативних даних на перший план висувається питання щодо додержання вимог інформаційної безпеки, а також захисту інформації від впливу так званої інформаційної зброї. Зазначена зброя використовується в інформаційній війні, яка в широкому сенсі не є алегоричним поняттям. Це суспільно-політичне явищ, яке повністю підпадає під традиційні визначення війни.

Сьогодні інформаційну війну розглядають як найбільш ефективний і "цивілізований" (гуманний) шлях колонізації однієї країни іншою. Неминучість інформаційної війни зумовлена економічною доцільністю, а висока ймовірність залучення до неї України – її геополітичним становищем та наявністю політичних, економічних й інших інтересів щодо нашої держави з боку розвинених країн, забезпечення яких значною мірою реалізується на інформаційному рівні. За таких умов значно зростає відносна вага спеціальних сил і засобів. Акцент переноситься зі знищення сил противника на знищення інфраструктури, насамперед економічної, дезінтеграцію ворожого суспільства, його примусу змінити свої орієнтири розвитку, адаптуватися до нових вимог. Відбуватиметься це завдяки проведенню інформаційних операцій, які розглядаються як інструмент впливу на систему соціально-політичної комунікації держави.

З огляду на викладене, перспективним убачається концептуальне розроблення та вдосконалення теоретико-методологічних засад інформаційної безпеки в контексті інформаційно-аналітичного забезпечення органів державної влади підрозділами Служби безпеки України.

На методологічному рівні предметна сфера забезпечення інформаційної безпеки повинна мати єдиний системоутворюючий фактор, скажімо, знання динамічних та статистичних аспектів інформаційних процесів, що відбуваються в соціо- та соціо-технічних системах. Кожен із цих аспектів має в основі власну функціональну модель і побудований з урахуванням відповідних рівнів ієрархії. Унаслідок цього система інформаційної безпеки набуває складної структури, відбувається її поділ на підсистеми та окремі складові,

різні за типами. Тому основу подальшого наукового дослідження має становити теорія складних систем. Її використання дозволить визначити загальні закономірності виникнення інформаційних загроз незалежно від їхнього функціонального змісту, а в подальшому обмежити їх руйнівні наслідки.

*Череватий В.В.,*
*Національна академія Служби безпеки України*

## ХАРАКТЕР ЗАГРОЗ КОНСТИТУЦІЙНОМУ ЛАДУ УКРАЇНИ В ІНФОРМАЦІЙНІЙ СФЕРІ

Оскільки сучасний процес інтенсивного розвитку суспільства нерозривно пов'язаний із такими явищами, як інтеграція та глобалізація, боротьба різновекторних національних інтересів через інформаційний простір, що загрожує розмиванням суспільних цінностей і національної ідентичності, то інформаційна складова набуває дедалі більшої значущості, стає одним із найважливіших елементів забезпечення як національної безпеки в цілому, так і конституційного ладу зокрема [3; 214].

Конституційний лад – це логічна побудова, яка відображає об'єктивовані в нормах конституційного права устрій держави і суспільства, а також місце людини в системі відносин: держава – суспільство – особа, – тому забезпечення його належного функціонування є одним із найголовніших завдань держави [4; 12]. Це забезпечення набуває актуальності з урахуванням низки чинників, які не завжди позитивно впливають на розвиток суспільного та державного ладу, – зовнішніх та внутрішніх загроз функціонуванню конституційного ладу.

Зовнішні і внутрішні загрози конституційному ладу визначаються через реальні та потенційні загрози національній безпеці України в цілому та її складовим зокрема (державна, економічна, військова тощо). У сфері інформаційної безпеки як головні загрози конституційному ладу можна виділити:

- поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України;
- зовнішні та внутрішні негативні інформаційні впливи на індивідуальну й суспільну свідомість через засоби масової інформації та мережу Інтернету;

- негативні інформаційні впливи, спрямовані на підрив конституційного ладу та використання засобів масової інформації й мережі Інтернету для пропаганди сепаратизму за етнічною, мовною, релігійною й іншими ознаками;

- несанкціонований доступ до інформаційних ресурсів органів державної влади, розголошення інформації, яка становить державну та іншу передбачену законодавством таємницю, а також конфіденційної інформації, що є власністю держави;

- недостатня розвиненість інститутів громадянського суспільства, послаблення суспільно-політичної, міжетнічної та міжконфесійної єдності суспільства, недосконалість партійно-політичної системи, непрозорість політичної та громадської діяльності, що створює передумови для обмеження свободи слова, маніпулювання суспільною свідомістю;

- поширення у засобах масової інформації невластивих українській культурній традиції цінностей і способу життя, культу насильства, жорстокості, порнографії, зневажливого ставлення до людської й національної гідності [2; 19–20].

Саме для безпечного функціонування національного і світового інформаційного простору на рівні держави проводиться комплексна протидія зазначеним загрозам на основі пошуку і прийняття управлінських рішень, ефективність яких залежить від урахування характеру загроз конституційному ладу в інформаційній сфері.

Характер загроз конституційному ладу України в інформаційній сфері неможливо визначити без їх аналізу, який передусім передбачає виявлення джерел, класифікацію, з'ясування ступеня і параметрів для прогнозування та ідентифікації загроз. Джерела загроз – це умови й фактори, які потенційно містять деструктивні, шкідливі якості, а за окремих умов і реально виявлять небезпечні національним інтересам наміри, у нашому випадку в інформаційній сфері. За своїм виникненням та розвитком вони можуть мати природне, техногенне чи соціальне (тобто як внутрішнє, так і зовнішнє) походження.

Джерелами природного походження є небезпечні геологічні, метеорологічні морські та прісноводні явища, що спричиняють ерозію ґрунтів чи надр; природні пожежі; масове ураження сільськогосподарських рослин і тварин хворобами чи шкідниками; зміна стану водних ресурсів та біосфери тощо (серед таких для України найбільш актуальною є проблема повені у Закарпатті). Джерелами техногенного походження можуть бути транспортні аварії-катастрофи, пожежі, неспровоковані вибухи чи їх загроза, аварії з викидом (загрозою викиду) небезпечних хімічних, радіоактивних, біологічних

речовин, раптове руйнування споруд та будівель, аварії на інженерних мережах і спорудах життєзабезпечення, гідродинамічні аварії на греблях, дамбах тощо.

До джерел соціального (антропогенного) походження відносять вчинення людиною різноманітних дій щодо дестабілізації системи безпеки або спрямування її діяльності у вигідному для суб'єкта впливу руслі [1; 78]. За змістом дій їх можна поділити на:

- ненавмисні - викликані помилковими чи ненавмисними діями людини (помилковий запуск ракети, збиття у повітрі цивільного літака, що не відповідав на запити військ протиповітряної оборони тощо);

- навмисні - ті, що стали результатом навмисних дій людей (акт тероризму, провокація війни, широкомасштабні інформаційні війни, геноцид та ін.).

Класифікувати загрози конституційному ладу України в інформаційній сфері з урахуванням параметрів, ступеня прояву можна за певними критеріями.

З огляду на якісні параметри загроз:

- за наявності у визначений період негативного впливу вони можуть бути реальними або потенційними;

- за спрямуванням впливу – на яку сферу чи сукупність сфер суспільно-політичного життя вони впливають, реалізацію яких національних інтересів унеможливлюють (політичні, економічні, соціальні, військові тощо);

- за розмахом та масштабами наслідків – глобальні, регіональні, національні, локальні, поодинокі;

- за розташуванням джерел загрози – внутрішні чи зовнішні;

- за характеристикою загроз стосовно суб'єктів їх дії – організовані, заплановані, стихійні, спонтанні тощо;

- за впливом на конституційний лад – безпосередні (стосовно конституційного ладу в цілому) чи опосередковані (через його структурні складові);

- за відтворенням у суспільній свідомості – явні, відомі, неявні, невідомі;

- за характером експертного виявлення – виявлені, проаналізовані, передбачені; невиявлені, непроаналізовані, непередбачені.

З огляду на кількісні параметри загроз:

- за інтенсивністю дії – слабкої, середньої та сильної інтенсивності;

- за тривалістю впливу – миттєві, короткострокові й довготривалі.

Така класифікація прийнятна для визначення загроз не лише конституційному ладу України в інформаційній сфері, а й національній безпеці з її складовими (державна, політична, економічна, соціальна, військова безпека тощо) та національним інтересам загалом.

За означених умов, дослідження і вирішення цієї проблеми має невідкладний характер та становить особливий інтерес для сучасної науки й практики, вказує на необхідність усебічного системного підходу при її вивченні, базисом якого повинні стати ґрунтовні наукові здобутки соціального, політичного, економічного, екологічного та іншого характеру, що будуть термінологічними та методологічними засадами організації діяльності всіх складових як інформаційної, так і національної безпеки загалом.

## ЛІТЕРАТУРА

1. Аналіз соціальних систем / М.І.Мельник (кер. автор. колективу), П.М.Копка та ін. – К., 2007.

2. Доктрина інформаційної безпеки України // Офіційний вісник Президента України. Інформаційний бюлетень № 20 (105). – К. : ДП НВЦ "Євроатлантикінформ", 2009.

3. Пилипчук В.Г. Формування теоретико-правових основ забезпечення державної безпеки України (кінець ХХ – початок ХХІ століття) : моногр. / В.Г.Пилипчук. – К. : НКЦ СБ України, 2008.

4. Прієшкіна О.В. Конституційний лад України: актуальні питання становлення, інституціоналізації та розвитку : моногр. / О.В.Прієшкіна. – О. : Фенікс, 2008.

*Чернухін І.О.,*
*Служба безпеки України*

## ПРАВОВІ АСПЕКТИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ВІД КІБЕРНЕТИЧНИХ ЗАГРОЗ

Протягом останніх років *окреслилась стійка тенденція збільшення кількості проявів комп'ютерних атак* на важливі об'єкти національних інфраструктур іноземних країн, що призводило до завдання шкоди державам через спотворення важливої для них інформації, блокування виробничих процесів на об'єктах промисловості, житлово-комунального господарства, транспорту, енергетики. У жовтні 2010 року комп'ютерний вірус StuxNet, виявлений в інформаційній системі технологічного управління заводу із збагачення урану в Ісламській Республіці Іран, призвів до виходу з ладу більше половини обладнання підприємства. 2011 року відбулися кібератаки на систему водозабезпечення інфраструктурних об'єктів штату Іллінойс (США), 2012-го – мережу управління електростанцією в м. Бендер-

Аббас (Іран) та мережі нафтодобувної кампанії Aramco (Саудівська Аравія). Посягання на об'єкти не лише політичної, а й економічної, соціально-політичної сфер іноземних країн за допомогою інформаційних технологій зумовило актуалізацію проблеми протидії кібернетичній злочинності на державному рівні. США та країни Європейського Союзу (ЄС) увели в законодавство таку дефініцію, як *критична інфраструктура*.

У вітчизняному законодавстві це поняття не регламентовано. Водночас, за суттю воно включає, насамперед, об'єкти життєзабезпечення та підвищеної небезпеки, об'єкти, уразливі в терористичному та диверсійному плані. Хоча рівень упровадження нових інформаційних технологій у вітчизняне виробництво нижчий, ніж у розвинутих країнах, потреба модернізації інформаційно-телекомунікаційних систем технологічного управління на об'єктах, що побудовані *за старими технологіями з використанням ручного або апаратного (унеможливлює зміну програми) управління,* упровадження новітніх систем програмного управління без застосування та перевірки систем захисту інформації робить уразливими ці об'єкти в кібертерористичному аспекті.

На сьогодні основними недоліками вітчизняного законодавства, що зумовлюють низьку ефективність захисту критичної інфраструктури від кіберзагроз, залишаються такі:

– *законодавчо не визначено механізм віднесення даних*, що циркулюють у системах управління технологічними процесами на об'єктах критичної інфраструктури*, до інформації*, захист якої є обов'язковим. Натомість зазначене виступає необхідною умовою створення комплексної системи захисту інформації (КСЗІ). Хоча законодавством України регламентовано потребу в захисті ядерних установок (Закон України "Про використання ядерної енергії та радіаційну безпеку"), об'єктів централізованого питного водопостачання (Закон України "Про питну воду та питне водопостачання"), забезпеченні безпеки на трубопровідному транспорті (Закон України "Про трубопровідний транспорт"), безпеки руху (Закон України "Про залізничний транспорт"), норма права, що конкретизує обов'язкову побудову систем управління технологічними процесами на об'єктах критичної інфраструктури відповідно до встановлених вимог захисту інформації, відсутня;

– *відсутність вимог із заборони підключення* інформаційних систем управління технологічними процесами на об'єктах критичної інфраструктури *до глобальних мереж.* Відповідно до Порядку підключення до глобальних мереж передачі даних (затв. постановою Кабінету Міністрів України від 12 квітня 2002 року № 522) за-

бороняється підключати до глобальних мереж інформаційні системи, на яких обробляється інформація з обмеженим доступом, що є об'єктом державної власності й охороняється згідно із законодавством. Відповідно до законодавства України віднесення відомостей до інформації з обмеженим доступом (службова інформація, державна таємниця) базується на критерії рівня змістового навантаження відомостей (інформація щодо організації, особи, заходів, засобів та ін.). Водночас інформація, що циркулює в інформаційно-телекомунікаційних системах управління технологічними процесами на об'єктах критичної інфраструктури, не має змістового навантаження (технологічна інформація-сигнал, команда та ін.);

– *брак державного впливу на рівень захисту інформації* в інформаційних системах об'єктів критичної інфраструктури приватної форми власності. Згідно зі статтею 9 Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" відповідальність за забезпечення захисту інформації в системі покладається на власника системи. Тобто, у разі перебування об'єкта критичної інфраструктури в приватній формі власності, вимоги щодо захисту її інформаційно-телекомунікаційної мережі визначатиме комерційна структура. При цьому законодавством не регламентовано обов'язковість проведення державної експертизи КСЗІ в такій мережі.

Потребує додаткової законодавчої регламентації питання створення, взаємоз'єднання й експлуатації інформаційно-телекомунікаційних систем управління об'єктами критичної інфраструктури, що мають єдиний технологічний цикл на території декількох держав (наприклад газо-, нафто-, аміакопроводи).

Враховуючи зазначене, з метою мінімізації кібернетичних загроз критичній інфраструктурі вбачається доцільним:

– законодавчо віднести інформацію, що циркулює в інформаційних (автоматизованих) системах управління технологічними процесами на об'єктах життєзабезпечення та підвищеної небезпеки незалежно від форми власності, до *інформації, вимога щодо захисту якої є обов'язковою* (шляхом внесення змін до профільних для галузі економіки чи сфер життєзабезпечення законів України або до Закону України "Про інформацію");

– внести зміни до постанови Кабінету Міністрів України від 12 квітня 2002 року № 522 у частині заборони підключення інформаційних систем управління технологічними процесами об'єктів життєзабезпечення та підвищеної небезпеки до інтернету;

– законодавчо регламентувати питання створення, взаємоз'єднання та експлуатації інформаційно-телекомунікаційних систем управління об'єктами критичної інфраструктури, що мають єдиний технологічний цикл на території України й інших держав;

– надавати пріоритет використанню вітчизняного програмного забезпечення в системах управління технологічними процесами на об’єктах критичної інфраструктури державної форми власності.

## ЛІТЕРАТУРА

1. Закон України “Про основи національної безпеки України” від 19 червня 2003 р. № 964-IV [Електронний ресурс] // Офіційний сайт Верховної Ради України. – Режим доступу : http.//rada.gov.ua.

2. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” від 5 липня 1994 р. № 88/94-ВР [Електронний ресурс] // Офіційний сайт Верховної Ради України. – Режим доступу : http.//rada.gov.ua.

3. USA PRESIDENTIAL DECISION DIRECTIVE/NSC-63, Subject: Critical Infrastructure Protection, May 22, 1998. [Електронний ресурс]. – Режим доступу: http://www.fas.org/irp/offdocs/pdd/pdd-63.htm

4. Нідільніченко В. Розвиток інформаційних технологій і національна безпека України / В. Нідільніченко // Національна безпека: український вимір. – 2009. – № 3(22).

5. COMMUNICATION FROM THE COMMISSION on a European Programme for Critical Infrastructure Protection, Brussels, 12.12.2006, COM(2006) 786 final. [Електронний ресурс]. – Режим доступу : http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33260_en.htm.

6. Закон України “Про інформацію” від 2 жовтня 1992 р. № 2657-XII [Електронний ресурс] // Офіційний сайт Верховної Ради України. – Режим доступу : http.//rada.gov.ua.

*Чеховська М.М.,*
*кандидат економічних наук, доцент,*
*Національна академія Служби безпеки України*

## АВТОМАТИЗОВАНІ СИСТЕМИ СУДІВ ЯК ОБ’ЄКТ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Застосування в діяльності судів, органів прокуратури та слідчих органів автоматизованих систем і баз даних зумовлено дією таких нормативно-правових актів, як Кримінальний процесуальний кодекс України, Закон України “Про захист інформації в інформаційно-телекомунікаційних системах”, Положення про порядок ведення Єдиного реєстру досудових розслідувань, Положення про автоматизовану систему документообігу суду та ін.

Однак необхідно наголосити, що деякі норми Кримінального процесуального кодексу України містять передумови для створення загроз національній безпеці держави, зокрема у сфері інформаційної безпеки, та потребують упровадження відповідної системи заходів із її захисту. Скажімо, статтею 35 "Автоматизована система документообігу суду" передбачається функціонування відповідної автоматизованої системи, призначеної для надання фізичним та юридичним особам інформації про стан розгляду матеріалів кримінального провадження; централізованого зберігання текстів вироків, ухвал та інших процесуальних документів; підготовки статистичних даних; видачі вироків, ухвал суду та виконавчих документів на підставі наявних у системі даних; передачі матеріалів до електронного архіву [1].

Крім того, статтею 214 "Початок досудового розслідування" Кодексу передбачається ведення Єдиного реєстру досудових розслідувань, адже досудове розслідування уважається таким, що розпочалося, лише з моменту внесення відповідних відомостей у зазначений реєстр.

Як бачимо, при цьому формуються відповідні бази даних, несанкціоноване втручання в роботу яких може призвести до негативних наслідків як для об'єктів національної безпеки, так і для суб'єктів її забезпечення. Тобто виникає потенційна загроза національній безпеці України, у тому числі стабільності в суспільстві, безпосередньо в інформаційній сфері у випадку розголошення інформації, яка становить державну або іншу, передбачену законодавством, таємницю, а також конфіденційну інформацію. Отримані відомості також можуть слугувати інструментом у намаганні маніпулювати суспільною свідомістю.

Яскравою ілюстрацією технологічної недосконалості, необхідності захисту інформації в автоматизованій системі, спірних аспектів у редагуванні інформації є порушення у 2011 році проти голови Глухівського міського районного суду Сумської області трьох кримінальних справ за ч. 1 ст. 376-1, ч. 2 ст. 368 і ч. 1 ст. 364 Кримінального кодексу України (зловживання службовим становищем, отримання хабара, незаконне втручання в роботу автоматизованої системи документообігу суду, прийняття суддею завідомо неправосудного рішення) [2]. Так уперше в історії України правоохоронцям удалося зафіксувати й довести факт втручання в комп'ютерну програму "Документообіг загальних судів", адже суддя чинила тиск на підлеглих і змушувала їх вносити неправдиві відомості до зазначеної програми. В результаті до судді потрапляли справи, в яких вона була зацікавлена і за які, власне, отримувала хабарі. Іншими словами, при всій задекларованій розробниками надійності, програма до-

кументообігу може бути уразливою як ізсередини, так і ззовні – при одночасній роботі в програмі та інтернеті.

В той же час необхідно зазначити, що вказані вище автоматизована система документообігу суду та Єдиний реєстр досудових розслідувань є кроком на шляху до розвитку національної інформаційної інфраструктури й ресурсів, а також елементом реалізації конституційних прав громадян на доступ до інформації.

З огляду на зазначене виникає необхідність упровадження технічних засобів захисту інформаційних систем від несанкціонованого втручання в їх роботу, а також розроблення низки правових норм, які б передбачали відповідальність за вказані дії.

## ЛІТЕРАТУРА

1. Кримінальний процесуальний кодекс України [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/4651-17.

2. Александрова А. Суддю покарали за хабар і втручання в програму документообігу. Чи може це повторитися? / А.Александрова [Електронний ресурс]. – Режим доступу : http://zib.com.ua/ua/10850-suddyu_pokarali_za_habar_i_vtruchannya_v_programu_dokumentoo.html.

*Шеломенцев В.П.,*
*кандидат юридичних наук, заслужений юрист України,*
*Міністерство внутрішніх справ України*

## ФОРМУВАННЯ ЗАКОНОДАВЧИХ ОСНОВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

7 березня цього року у Верховній Раді України було зареєстровано проект Закону про внесення змін до Закону України “Про основи національної безпеки України” щодо кібернетичної безпеки України, внесений Кабінетом Міністрів України [1]. Як убачається, це відбулося в аспекті вирішення питань розроблення засад забезпечення кібербезпеки держави, поставлених ще в липні 2012 року учасниками парламентських слухань на тему “Про стан та перспективи розвитку Воєнної організації та сектору безпеки України” [2].

Залежність об’єктів критичної інфраструктури України від використання кібернетичних систем робить їх уразливими стосовно протиправного впливу з використанням ресурсів кібернетичного

простору та підвищує ризик виникнення надзвичайних ситуацій, створює реальні загрози життєдіяльності людини, суспільства, держави, подальшому соціально-економічному розвитку та національній безпеці України.

У зазначеному законопроекті вперше з моменту ратифікації Конвенції Ради Європи про кіберзлочинність на законодавчому рівні здійснено спробу визначити такі поняття, як "кібернетичний простір "(кіберпростір) та кібернетична безпека" (кібербезпека).

Формування законодавчих основ забезпечення кібербезпеки держави шляхом внесення змін до Закону України "Про основи національної безпеки України" безпосередньо вказує на те місце, яке автори законопроекту відводять кібербезпеці в системі національної безпеки. Так, відповідно до законопроекту пропонується розглядати кібернетичну безпеку як складову інформаційної безпеки, поряд із свободою слова та захистом інформації. Загрози кібернетичного характеру національним інтересам і національній безпеці України, окрім інформаційної сфери, визначені у воєнній, державній сферах безпеки та безпеки державного кордону України.

Водночас, слід відмітити, що у тексті законопроекту відсутні терміни "кіберзлочинність" та "кібертероризм" (замість них використовуються "комп'ютерна злочинність" та "комп'ютерний тероризм"). Зазначене суперечить підходам, викладеним у нових редакціях Стратегії національної безпеки України та Воєнної доктрини України. Так, серед основних чинників, що загрожують глобальній міжнародній стабільності та негативно позначаються на безпековому середовищі України, новою редакцією Стратегії національної безпеки України визначено саме поширення кіберзлочинності [3]. А в новій редакції Воєнної доктрини України поширення тероризму (у тому числі кібертероризму) розглядається як тенденція, що впливає на воєнно-політичну обстановку у світі [4].

У новій редакції Стратегії відмічається нездатність України протистояти новітнім викликам національній безпеці, пов'язаним із застосуванням інформаційних технологій в умовах глобалізації, насамперед кіберзагрозам.

Проте у законопроекті, наводячи перелік кіберзагроз, автори не розкрили роль кібернетичних атак, які є основним способом реалізації такого виду загроз. А відповідно до Стратегічного оборонного бюлетеня України саме кібернетичні атаки, поряд із високоточною зброєю, диверсіями, радіоелектронними перешкодами становлять загрозу живучості систем управління, військ (сил) і важливих об'єктів [5].

Хоча запобігти кібернетичним атакам технічно не убачається можливим, незалежно від складності систем захисту своєчасне ви-

явлення та швидке адекватне реагування на кібернетичні атаки дозволяє значно мінімізувати наслідки таких атак.

Крім того, у зазначеному законопроекті серед основних напрямів державної політики з питань національної безпеки не передбачається створення національної системи кібербезпеки, хоча це прямо визначено положеннями нової редакції Стратегії національної безпеки України. Не передбачається також упровадження принципово нової системи організації та проведення заходів інформаційної боротьби, яка включатиме відповідні органи управління, сили та засоби, що створюються в Міністерстві оборони України, Збройних Силах України, інших складових сектору безпеки й оборони України, що визначено новою редакцією Воєнної доктрини України.

Актуальність розбудови дієвої системи кібернетичної безпеки України зумовлена тим, що в сучасних умовах глобалізації значно зростають уразливості інформаційно-телекомунікаційних систем, що функціонують в інтересах управління державою, забезпечують потреби оборони та безпеки держави, кредитно-банківської та інших сфер економіки, систем управління об'єктами критичної інфраструктури.

Отже, проект Закону про внесення змін до Закону України "Про основи національної безпеки України" щодо кібернетичної безпеки України проміжний на шляху удосконалення Доктрини інформаційної безпеки України та розроблення законопроекту про кібернетичну безпеку України. Уразливими для реалізації цих кіберзагроз є об'єкти, функціонування інформаційно-телекомунікаційних систем яких пов'язане з використанням ресурсів кіберпростору. Тобто об'єкти, завдання шкоди яким можливе шляхом деструктивного кібернетичного впливу (кібернетичної атаки).

При цьому логікою розроблення законопроекту "Про кібернетичну безпеку України" повинно передбачатися першочергове визначення об'єктів критичної національної інфраструктури, що потребують нагального захисту від кібернетичних атак.

Як убачається, не всі об'єкти такої інфраструктури є уразливими для кібернетичних впливів (тобто діяльність не всіх об'єктів критично залежить від нормального функціонування інформаційно-телекомунікаційних систем). Водночас, кожній такій системі, що використовується на окремому об'єкті критичної національної інфраструктури, властиві конкретні уразливості, а отже, й відповідні кіберзагрози.

Тобто, лише визначивши об'єкти критичної національної інфраструктури та встановивши основні зовнішні й внутрішні загрози кібернетичного характеру, можна приступити до формування системи безпеки, ефективність якої буде зумовлена підбором найбільш

ефективних заходів захисту від різних видів кібернетичних загроз; суб'єктів, здатних забезпечити необхідний рівень кіберзахисту.

## ЛІТЕРАТУРА

1. Офіційний сайт Верховної Ради України. – http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=45998.

2. Про Рекомендації парламентських слухань на тему: "Про стан та перспективи розвитку Воєнної організації та сектору безпеки України" : Постанова Верховної Ради України від 5 липня 2012 року № 5086-VI // Голос України. – 2012. – № 133. – 24 лип.

3. Про рішення Ради національної безпеки і оборони України від 8 червня 2012 року "Про нову редакцію Стратегії національної безпеки України" : Указ Президента України від 8 червня 2012 року № 389/2012 // Офіційний вісник Президента України. – 2012. – № 20. – С. 19. – Ст. 470. — 19 червн.

4. Про рішення Ради національної безпеки і оборони України від 8 червня 2012 року "Про нову редакцію Воєнної доктрини України" : Указ Президента України від 8 червня 2012 року № 390/2012 // Офіційний вісник Президента України. – 2012. – № 20. – С. 31. – Ст. 471. – 19 червн.

5. Про рішення Ради національної безпеки і оборони України від 29 грудня 2012 року "Про Стратегічний оборонний бюлетень України" : Указ Президента України від 29 грудня 2012 року № 771/2012 // Офіційний вісник Президента України. – 2013. – № 3. – С. 3. – Ст. 75. – 5 лют.

*Шепета О.В.,*
*кандидат юридичних наук,*
*Національна академія Служби безпеки України*

## ДЕРЖАВНА ПОЛІТИКА ЩОДО ЗАХИСТУ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Реалізація державної політики щодо захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах полягає у: 1) підготовці пропозицій до визначення загальної стратегії та пріоритетних напрямів діяльності у сфері захисту державних інформаційних ресурсів в ІТС; 2) виконанні обов'язків уповноваженого органу у сфері захисту інформації в

інформаційно-телекомунікаційних системах; 3) розробленні порядку та вимог до захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, а також погодження проектів нормативно-правових актів із цих питань; 4) розробленні критеріїв та порядку оцінювання стану захищеності державних інформаційних ресурсів в інформаційно-телекомунікаційних системах тощо.

Реалізація державної політики забезпечується шляхом виконання низки заходів відповідно до визначених завдань, а саме:

- методичного керівництва та координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форми власності з питань, пов'язаних із запобіганням учиненню порушень безпеки інформації в інформаційно-телекомунікаційних системах, виявленням та усуненням наслідків інших несанкціонованих дій щодо державних інформаційних ресурсів в інформаційно-телекомунікаційних системах;
- накопичення й аналізу даних про вчинення та/або спроби вчинення несанкціонованих дій щодо державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, а також про їх наслідки:
- організації та здійснення оцінювання стану захищеності державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, надання відповідних рекомендацій.

Із метою забезпечення єдиного підходу до захисту державних інформаційних ресурсів, на виконання постанови Кабінету Міністрів України від 24.02.2003 № 208 "Про заходи щодо створення електронної інформаційної системи "Електронний Уряд" [СН] у рамках Національної системи конфіденційного зв'язку у м. Києві, створюється окрема підсистема для телекомунікаційного забезпечення функціонування Єдиного веб-порталу органів виконавчої влади.

На сьогодні підключення органів державної влади до мережі Інтернету здійснюється через захищений вузол інтернет-доступу Держспецзв'язку. Подальше підключення органів державної влади до Інтернету має здійснюватись виключно через захищений вузол інтернет-доступу НСКЗ.

На виконання завдань Національної програми інформатизації [СІ] у межах здійснення проекту "Забезпечення антивірусного захисту державних інформаційних ресурсів" створено Центр

антивірусного захисту інформації (ЦАЗІ). Одним із основних завдань ЦАЗІ є впровадження єдиної технологічної політики щодо антивірусного захисту інформації в ІТС органів державної влади, а також централізованого забезпечення їх антивірусними *програмними* продуктами, сертифікованими у встановленому законодавством України порядку.

Також із використанням ресурсів ЦАЗІ проводяться державні *експертизи* антивірусних програмних засобів із метою визначення можливості їх застосування в Україні та експрес-експертизи антивірусних оновлень до них.

Із метою проведення оцінки стану захищеності державних інформаційних ресурсів в інформаційно-телекомунікаційних системах відповідно до затвердженого постановою Кабінету Міністрів України від 03.08.2005 № 688 Положення утворено Реєстр інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління. Забезпечення функціонування цього Реєстру покладено на Департамент безпеки інформаційно-телекомунікаційних систем Держспецзв'язку.

Реалізація вимог Положення створює передумови для запровадження єдиної системи обліку відомостей про ІТС органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління; проведення аналізу стану захисту державних електронних інформаційних ресурсів в ІТС; надання методичної допомоги і координування *діяльності* міністерств та інших центральних органів виконавчої влади, пов'язаної із захистом державних електронних інформаційних ресурсів в ІТС.

Таким чином, для вжиття запобіжних заходів та розвитку методології запобігання порушенню цілісності, доступності й конфіденційності державних інформаційних ресурсів слід здійснювати заходи, спрямовані на підготовку до ліквідації наслідків несанкціонованих дій, що порушили безперебійне функціонування інформаційно-телекомунікаційних систем органів державної влади; поширювати інформацію щодо наявних та ймовірних загроз, інструментів і засобів забезпечення безпеки інформації.

*Шилін М.О.,*
*доктор юридичних наук, доцент,*
*Національна академія Служби безпеки України*

# ЩОДО ПРАВОВИХ СУПЕРЕЧНОСТЕЙ У ЗАКОНАХ УКРАЇНИ “ПРО ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ” ТА “ПРО ІНФОРМАЦІЮ”

Захист персональних даних в Україні унормований Законом України “Про захист персональних даних” від 1 червня 2010 року № 2297-VI, який набув чинності з 1 січня 2011 року. У 2012 році (23 лютого і 20 листопада) до нього були внесені суттєві зміни відповідно законами України № 4452-VI та № 5491-VI.

Згідно зі ст. 1 цей Закон регулює відносини, пов’язані із захистом і обробленням персональних даних, і спрямований на захист основоположних прав та свобод людини і громадянина, зокрема права на невтручання в особисте життя у зв’язку з обробленням персональних даних. Дія його поширюється на діяльність з обробленя персональних даних, яка проводиться повністю або частково із застосуванням автоматизованих засобів, а також персональних даних, що містяться у картотеці чи призначені до внесення до картотеки, із застосуванням неавтоматизованих засобів [1]. А за ст. 2 цього ж Закону обробка персональних даних – будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення, розповсюдження, реалізація, передача), знеособлення, знищення даних, у тому числі з використанням інформаційних (автоматизованих) систем.

Відразу впадає в очі певна суперечність. Якщо тлумачити статтю 1, виходячи з дослівної її редакції, то Закон “Про захист персональних даних” регулює тільки правовідносини, які виникають у випадку оброблення персональних даних, яка здійснюється повністю або частково із застосуванням автоматизованих засобів, а також персональних даних, що містяться у картотеці чи призначені для внесення до картотеки, із застосуванням неавтоматизованих засобів. А обробка персональних даних відповідно до редакції статті 2 – це певні дії з даними, у тому числі з використанням інформаційних (автоматизованих) систем, але ці дані не обов’язково містяться в картотеці чи будуть занесені до неї, тобто обробка персональних даних не пов’язується тільки з формуванням та експлуатацією певних банків даних – інформаційних систем, як автоматизованих так і неавтоматизованих (картотечних).

У статті 1 Закону також наголошується, що дія цього нормативно-правового акта не поширюється на діяльність з оброблення персональних даних, яка проводиться творчим чи літературним працівником, у тому числі журналістом, у професійних цілях, за умови забезпечення балансу між правом на невтручання в особисте життя та правом на самовираження. З цього приводу виникає декілька питань. Які критерії забезпечення творчим і літературним працівником, у тому числі журналістом, балансу між правом на невтручання в особисте життя та правом на самовираження? В Законі вони не визначені. Чому виняток щодо непоширення дії положень Закону "Про захист персональних даних" про обробку персональних даних у професійних цілях зроблено лише для творчого й літературного працівника, у тому числі журналіста? Адже це не повною мірою кореспондується із ч. 6 статті 6, де зазначається, що не допускається обробка даних про фізичну особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини, а також статтею 25 Закону, яка визначає (встановлює) випадки обмеження дії певних його статей, зокрема в інтересах національної безпеки. Виходячи з їх змісту, відповідні суб'єкти, зокрема оперативні співробітники Служби безпеки України при виконання контррозвідувальних завдань у межах своєї компетенції, можуть здійснювати обробку персональних даних.

Відповідно до статті 5 Закону України "Про інформацію" [2] 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. Разом із тим, стаття 5 Закону України "Про захист персональних даних" наголошує, що персональні дані, крім знеособлених, за режимом доступу є інформацією з обмеженим доступом. А за ст. 21 Закону України "Про інформацію" інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація (ч. 1).

Конфіденційна інформація – інформація про фізичну особу, а також доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом (ч. 2 ст. 21). Окрім того, відповідно до ч. 2 статті 11 Закону України "Про інформацію" 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 захисту прав людини.

З цього випливає, що не кожна особа має право вільного доступу до інформації з обмеженим доступом і не тільки тієї, яка знаходиться у розпорядженні органу державної влади, а й іншого розпорядника чи володільця, зокрема фізичної особи. Навіть до інформації, яка стосується персонально особи, вона не завжди може мати вільний доступ, про що зокрема наголошується в ч. 3 статті 11 зазначеного Закону: "кожному забезпечується вільний доступ до інформації, яка стосується його особисто, крім випадків, передбачених законом". Тому стаття 5 Закону України "Про інформацію" є декларативною і певним чином суперечить іншим нормативним положенням чинного законодавства.

Певним чином суперечні в названих законах і положення щодо віднесення інформації про фізичну особу до інформації з обмеженим доступом та визнання її конфіденційною. Так, у статті 5 Закону України "Про захист персональних даних" наголошується, що персональні дані, крім знеособлених персональних даних, за режимом доступу є інформацією з обмеженим доступом, а у статті 21 Закону України "Про інформацію", як уже зазначалося, що конфіденційною інформацією є інформація про фізичну особу, а також доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. З одного боку, за цією правовою нормою вся інформація про фізичну особу є інформацією з обмеженим доступом і конфіденційною. З іншого, конфіденційною є й інформація, доступ до якої особа обмежує. З цього випливає, що особа може й не обмежувати доступ до своїх персональних даних, тобто допускає, що вони можуть поширюватися без її відома.

Якими в цьому випадку є ці персональні дані – конфіденційними чи ні? Як бачимо, однозначної відповіді законодавці на це питання, на жаль, не дають. Окрім того, віднесення усієї інформації про фізичну особу до категорії конфіденційної, як слушно зауважують в одній із своїх публікацій Є.Д.Скулиш і А.І.Марущак, … "значно знижує інформаційно-правове значення відповідної інформації, що зрештою відобразиться на режимі доступу до такої інформації й може зумовити труднощі у правозастосуванні при неправомірному розголошенні чи поширенні такої інформації. Подібна позиція законодавця ставить під сумнів існування таких видів інформації з обмеженим доступом, як лікарська таємниця, таємниця усиновлення, банківська таємниця, до обсягу яких потрапляють персональні дані. При цьому варто звернути увагу й на той факт, що фізична особа може, але не зобов'язана встановлювати режим обмеженого доступу до інформації, яка їй належить або її стосується. Тому не зовсім коректним слід визнати віднесення інформації про фізичну особу автоматично до конфіденційної" [3, с. 9].

Водночас у статті 11 Закону України “Про інформацію” є припис (ч. 2), що 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. Виникає справедливе запитання, яким чином на практиці можна забезпечити виконання вимоги Закону про непоширення без згоди особи серед її колег по роботі третьою особою, наприклад, інформації про дату її народження чи сімейний стан?

Загалом аналіз законів України “Про захист персональних даних” та “Про інформацію” свідчить про наявність у них інших суттєвих недоліків, на що звертали увагу науковці Національної академії СБ України [3, с. 7–12].

У зв’язку з цим можна стверджувати, що зазначені вище нормативно-правові акти потребують удосконалення. Саме на вирішенні цієї проблеми, з урахуванням її важливості, і повинна бути зосереджена увага вітчизняних науковців-правників, які займаються дослідженнями питань правового забезпечення інформаційної безпеки України.

## ЛІТЕРАТУРА

1. Закон України “Про захист персональних даних” // Відомості Верховної Ради України. – 2010. – № 34. – Ст. 481.

2. Закон України “Про інформацію” // Відомості Верховної Ради України (ВВР). – 1992. – № 48. – Ст. 650 (у редакції Закону № 2938-VI (2938-17) ВВР, 2011, № 32, ст. 313).

3. Скулиш Є.Д. Новели інформаційного законодавства України: проблеми теорії і практики / Є.Д.Скулиш, А.І.Марущак // Інформаційна безпека людини, суспільства, держави. – 2011. – № 1(5). – С. 7–12.

*Юрченко О.М.,*
*доктор юридичних наук, доцент,*
*Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю при РНБО України*

## ДЕСТРУКТИВНИЙ ІНФОРМАЦІЙНИЙ ВПЛИВ НЕУРЯДОВИХ ОРГАНІЗАЦІЙ НА ДЕМОКРАТИЧНІ ПРОЦЕСИ В УКРАЇНІ

Тенденції останнього десятиріччя переконливо свідчать, що у світі сформувалось та інтенсивно розвивається нове середовище протиборства інтересів у різних сферах – інформаційний простір.

Характерно, що ця конкурентна боротьба торкається політичної, соціальної, культурної та інших сфер діяльності держав, інтересів транснаціональних компаній, а також міжнародних організацій. Можливості інформаційного простору активно використовуються організованими злочинними угрупованнями. Все частіше він стає засобом впливу на свідомість окремих громадян та їх співтовариства.

Розширення можливостей суспільства для отримання й поширення інформації, віртуального спілкування в соціальних мережах створює сприятливі умови для використання новітніх інформаційних технологій у вирішенні будь-яких нагальних питань. Це загострює одну з найбільш актуальних проблем сучасності – необхідність створення і впровадження ефективних механізмів протидії використанню інформаційного простору з деструктивною метою. Адже відсутність чи недостатня дієвість таких механізмів спричиняє реальні та потенційні загрози національній безпеці України.

Передусім мова йде про активне втручання деяких іноземних держав у внутрішнє життя України шляхом нав'язування суспільству своєї ідеології та цінностей. Здебільшого такий вплив здійснюється через міжнародні неурядові організації (МНО).

Станом на 1 січня 2013 року в Україні зареєстровано 91 317 громадських організацій (міжнародні – 821, всеукраїнські – 2924, місцеві організації – 59 935, їхні осередки – 27 637) [1], що сприймається як свідчення поглиблення демократичних процесів у нашій державі.

Слід зазначити, що більшість МНО невідома широкому загалу. Проте їхня діяльність, хоча, здебільшого, і залишається поза увагою ЗМІ, украй необхідна для суспільства. Вона передусім зосереджена на вирішенні багатьох його нагальних проблем через благодійництво, допомогу в захисті інтересів широких верств населення, культурної спадщини країни тощо. Така гуманітарна діяльність позитивно впливає на розвиток і зміцнення громадянського суспільства.

Але існують і такі міжнародні неурядові організації, які, прикриваючись лозунгами про демократію, захист прав та свобод людини, присвоюють роль арбітра в питаннях державного будівництва, ідеології, вибору шляхів економічного й соціального розвитку країни. При цьому їхні оцінки і судження здебільшого поширюються як істина в останній інстанції та не допускають альтернативи.

Таким чином, використовуючи статус громадської організації, МНО фактично ведуть активну політичну роботу, спрямовану на розпалювання в суспільстві протестних настроїв, формування недо-

віри до чинної влади, посилюють свій вплив на прийняття політичних рішень.

Саме тому будь-які спроби влади спрямувати їхню діяльність у бік політичної толерантності та невтручання у внутрішні справи країни або забезпечити державний контроль за точною реалізацією задекларованих ними завдань відразу ж стають предметом жорсткої критики іноземних держав, на утриманні яких перебувають ці МНО. При цьому здійснюється масоване поширення інформації про різке зниження в країні "індексу демократії" та усіляких рейтингів, суттєво зростає кількість публікацій негативного характеру як у вітчизняних, так і зарубіжних ЗМІ щодо "відродження в країні авторитарного режиму й диктатури".

Необхідно також наголосити, що МНО тісно пов'язані із внутрішніми опозиційними силами в країні й фактично стали не лише їхніми "спонсорами", але й "сценаристами" їхньої деструктивної діяльності. Інформаційні операції під їхнім проводом нерідко зводять нанівець зусилля офіційних державних структур, спрямовані на поліпшення соціально-політичної та економічної ситуації в державі. У результаті це суттєво впливає на свідомість громадян, поглиблює суспільну апатію і зневіру стосовно можливості позитивних зрушень у країні.

Серед найбільш активних МНО, через які реалізуються різного роду сценарії тиску на владу, можна виділити такі, як "Репортери без кордонів" (Франція), "Агентство з міжнародного розвитку" (США), Міжнародний фонд "Відродження" (фінансується Дж. Соросом) та інші [2, с. 57].

Сьогодні в експертному середовищі все частіше оприлюднюється точка зору, що МНО та сучасна інтернет-спільнота країни, яка формується під їхнім впливом, повністю опозиційні до чинної влади. Їхнє упереджено-критичне ставлення до розвитку демократичних процесів в Україні, вищого керівництва держави та діяльності державних інституцій дає підстави для сумніву, що в осяжному майбутньому вони змінять свою позицію. А це свідчить про те, що МНО і надалі будуть намагатись впливати на внутрішню й зовнішню політику та суспільно значущі процеси в Україні, орієнтуючись на інтереси своїх іноземних фінансових донорів. Особливе загострення такого протистояння очікується в період підготовки до виборів Президента України у 2015 році.

З огляду на зазначене потрібно вжити ефективних заходів щодо законодавчого регулювання діяльності МНО на території України,

визначення їх відповідальності за втручання у внутрішні справи держави та діяльність в її інформаційному просторі, яка створює загрози суверенітету й національним інтересам.

Необхідно запровадити відповідні санкції щодо МНО, які здійснюють політичну діяльність на території нашої країни або намагаються маніпулювати свідомістю суспільства в інтересах іншої держави.

## ЛІТЕРАТУРА

1. Оприлюднення експрес-випусків Держстату в 2013 році користувачами [Електронний ресурс]. – Режим доступу : http://ukrstat.org/uk/express/expres_u.html.

2. Поляруш О.О. Украина: эволюция “революций” / О.О.Поляруш, О.М.Юрченко. – К. : Саммит-книга, 2013. – 219 с.

# АКТУАЛЬНІ ПИТАННЯ ЗАХИСТУ ІНФОРМАЦІЇ: ТЕХНІЧНІ ТА ТЕХНОЛОГІЧНІ АСПЕКТИ

*Ваганій Н.В.,*
*ІСТЕ СБ України*

*Клівак В.А.,*
*кандидат технічних наук*
*ІСТЕ СБ України*

## ПІДВИЩЕННЯ СКРИТНОСТІ ТА ЗАВАДОСТІЙКОСТІ СИСТЕМ РАДІОЗВ'ЯЗКУ ШЛЯХОМ ЗАСТОСУВАННЯ ДКЧС КОСТАСА

Одне з питань захисту інформації, яка передається по радіоканалу, – підвищення скритності та завадостійкості систем радіозв'язку [1, с. 47].

Можливими шляхами розв'язання зазначеної проблеми є використання нових видів складних сигналів, які підвищують завадостійкість та скритність, розроблення й удосконалення нових методик формування та оброблення зазначених сигналів, створення нових видів систем радіозв'язку на основі цих сигналів і методик.

Пошук складних сигналів, що забезпечують задані властивості систем радіозв'язку, досі триває. Американський учений Дж. П.Костас запропонував як зондуючий вид когерентний дискретно-кодований за частотою сигнал (ДКЧС) із функцією невизначеності в координатах "дальність – доплерівська частота", яка наближається до δ-функції (ДКЧС Костаса) [2, с. 5]. Перспективність таких сигналів підтвердили у своїх роботах і розвинули відповідну аналітичну теорію та математичний апарат відомі західні учені С.В.Голомб і Х.Тейлор [3, с. 44–63; 4, с. 600–604], які розглядали цей вид сигналів як перспективний для використання в радіолокації.

Однак ДКЧС Костаса, попри очікуване підвищення структурної та енергетичної скритності, а також завадостійкості, в аспекті використання в системах радіозв'язку не досліджувались.

Оцінимо ефективність застосування дискретно-кодованих за частотою сигналів на основі масивів Костаса у системах радіозв'язку. Для цього проаналізуємо системи радіозв'язку з простими сигналами (ЧМ), ЛЧМ-сигналами та з використанням дискретно-кодованих за частотою сигналів на основі масивів Костаса.

Для оцінювання завадостійкості зазначених радіосистем використаємо залежності відношення сигнал/завада від імовірності правильного прийому, енергетичної скритності – спектральні щільності потужності сигналів, структурної скритності – кількість вимірів, необхідну для розкриття структури сигналу.

Графіки показників енергетичної скритності для зазначених вище систем радіозв'язку наведено на рис. 1. Відповідні показники структурної скритності (кількість вимірів, необхідна для розкриття структури сигналу) для оцінюваних систем радіозв'язку ілюструє рис. 2. Графіки залежності відношення сигнал/завада від імовірності правильного прийому для відповідних систем зв'язку наведено на рис. 3.

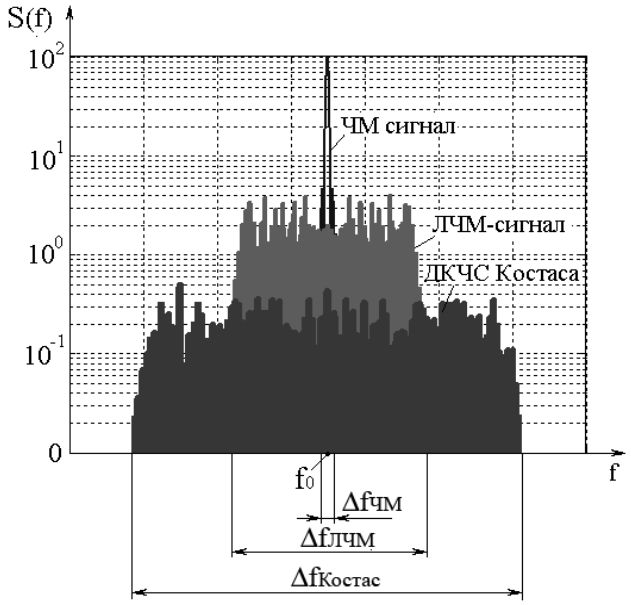



Рис. 1. Графіки показників енергетичної скритності для різних систем радіозв'язку

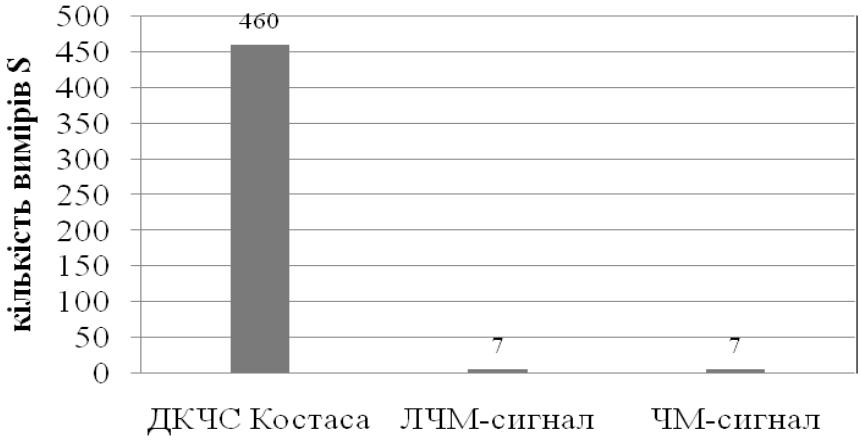



Рис. 2. Показники структурної скритності для різних систем радіозв'язку

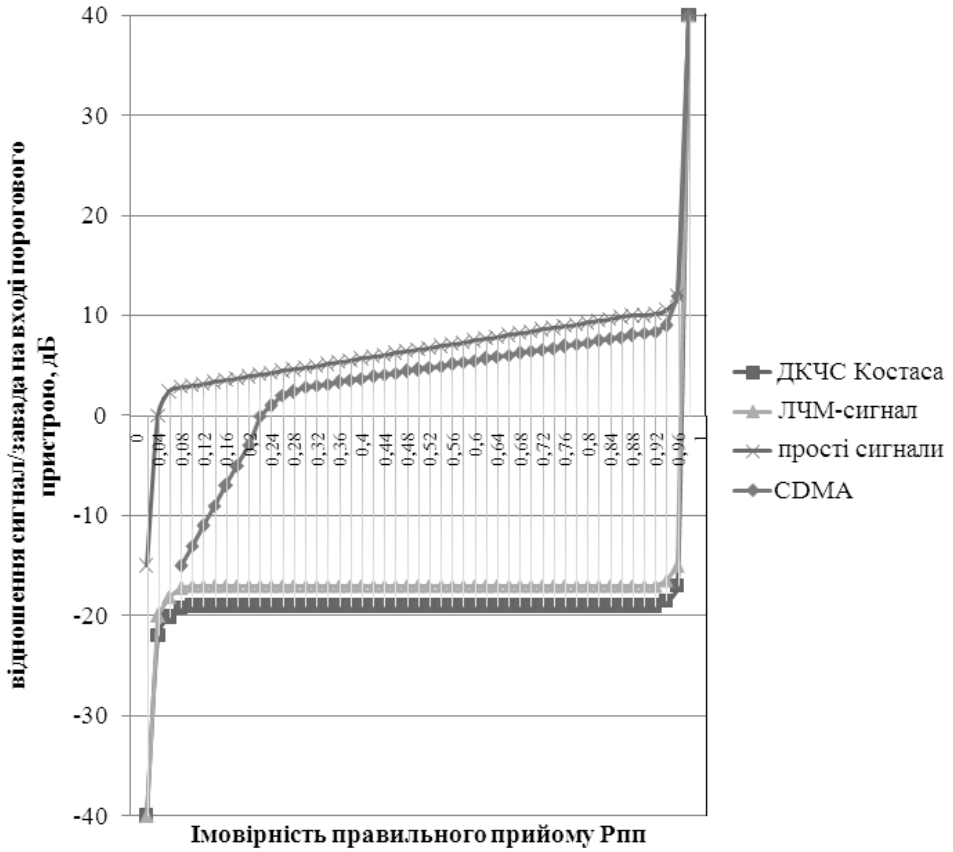



Рис. 3. Графіки залежності відношення сигнал/завада від імовірності правильного прийому

У результаті досліджень були виявлені такі властивості систем радіозв'язку із застосуванням дискретно-кодованих за частотою сигналів на основі масивів Костаса.

1. Є можливість підвищення рівня енергетичної скритності порівняно з системою радіозв'язку з простими сигналами на 23 дБ, порівняно із системою радіозв'язку з ЛЧМ-сигналом на 13,4 дБ.

2. Системи радіозв'язку з ДКЧС Костаса можуть забезпечити підвищення структурної скритності порівняно із системами з простими сигналами та ЛЧМ-сигналами до 18 дБ.

3. За завадостійкістю системи радіозв'язку з ДКЧС Костаса перевершують системи з простим сигналом на 29 дБ, системи з ЛЧМ-сигналом до 2 дБ, системи зв'язку стандарту cdmaOne до 26 дБ відповідно.

Таким чином, можна зробити висновок, що дискретно-кодовані за частотою сигнали на основі масивів Костаса можуть бути використані не лише в радіолокаційних системах як зондуючі сигнали, як їх пропонували застосовувати раніше, а і для підвищення завадостійкості та скритності передачі інформації по радіоканалу.

## ЛІТЕРАТУРА

1. Кокоток О.В. Некоторые аспекты безопасности систем радиосвязи / О.В.Кокотов, С.А.Серых, М.В.Соловьева // Зв'язок. – 2003. – № 1.– С. 47–49.

2. Костас Дж.П. Свойства сигналов с почти идеальной функцией неопределенности в координатах "дальность – допплеровская частота" / Дж.П. Костас // ТИИЭР. – 1984. – Т. 72. – № 8. – С. 5–18.

3. Голомб С.У. Конструкции и свойства массивов Костаса / С.У.Голомб, Х.Тейлор // ТИИЭР. – 1984. – Т. 72. – № 9. – С. 44–63.

4. Golomb S.W., Taylor H. Two-dimensional synchronization patterns for minimum ambiguity // IEEE Trans. Inform. Theory. – 1984. – Vol. IT-28. – No. 4. – P. 600–604.



*Віщун В.В.,*
*Національний університет оборони України*


## ЗД-МОНІТОРИНГ ПРОЦЕСІВ ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ ДЕРЖАВНИХ УСТАНОВ (ОРГАНІЗАЦІЙ) ПРИ ЗДІЙСНЕННІ КІБЕРАТАК

Упродовж останніх 50 років інформаційні системи із цінних та масивних перетворились на буденні й дрібні [1], а стрімке та глибоке проникнення їх в усі сфери життєдіяльності суспільства привело до виникнення прямої залежності безпечного існування людини від безпечного функціонування таких систем.

Функціонування інформаційних систем залежить від надійності програмного забезпечення кожного їх елемента. Як показує практика, наявне програмне забезпечення досить надійне, але є загрози їх нормальному функціонуванню, зокрема кібератаки [2].

Кібератака – активні дії в інформаційному середовищі спеціальних програмних продуктів або користувачів, які приводять до порушення конфіденційності, цілісності, спостереженості, доступності інформації та нормального функціонування інформаційних систем [3].

Для боротьби з кібератаками розробляються спеціалізоване програмне забезпечення (модулі доступу до робочих станцій, антивіруси, мережеві екрани тощо) та політика безпеки. Особливістю функціонування інформаційних систем є автоматизація процесів обміну, управління, доступу та ін. Така особливість не дозволяє користувачам робочих станцій, а також відповідальним адміністраторам мати повну картину процесів, що відбуваються в мережі, в режимі реального часу.

Надійне функціонування інформаційних систем та безпечну роботу підтримують адміністратори мереж. Адекватне реагування на зміни функціонування мереж при проведенні кібератак вимагає від адміністратора урахування численних факторів (від аналізу журналів маршрутизаторів до контролю доступу кожного користувача до ресурсів мережі). Тому створення умов для більш ефективного контролю функціонування мережі адміністраторами гарантує безпечне функціонування інформаційної системи при здійсненні кібератак загалом.

Забезпечення ефективного та безпечного функціонування інформаційних систем залежить від досвіду кожного адміністратора, програмного забезпечення, яке він використовує, програмного забезпечення, встановленого на робочих станціях, та безпосередньо апаратної частини (комп'ютери, мережеве обладнання). Власникам мереж державних установ (організацій) необхідний кінцевий результат, тобто гарантоване функціонування системи, а яким чином він буде досягнутий, залежить від тієї особи, на яку ці обов'язки покладені.

Для вирішення цієї проблеми необхідно якнайбільше спростити та формалізувати роботу адміністратора при обслуговуванні інформаційних систем. В умовах впливу кібератак на функціонування інформаційних систем у режимі реального часу моніторинг функціонування таких систем необхідно здійснювати теж у реальному часі.

Нині створені різні програмні продукти, які забезпечують моніторинг функціонування мереж. Вони надають змогу отримувати повідомлення про помилки або збої, що виникають. Утім, забезпечуючи можливість негайного повідомлення адміністратора про виникнення кризових ситуацій, вони тільки констатують факт порушення функціонування або безпеки.

Пропонуємо підвищити ефективність функціонування інформаційних систем органів військового управління в умовах кібератак за рахунок розширення можливості здійснення моніторингу процесів адміністраторами мереж, у 3Д-вимірі, в режимі реального часу. Для цього необхідно створити програмний продукт із можливістю подання вичерпної візуальної інформації про стан функціонування інформаційної системи для сектору, що контролюється.

Так, пропонується здійснити переформування параметрів, які потрібно контролювати адміністратору, для подання у візуалізації контрольованого сектору мережі, із кольоровим поданням процесів, що відбуваються, в режимі реального часу. Це дозволить адміністратору, увага якого залежить від психофізіологічних станів, стежити за функціонуванням інформаційної системи більш ефективно.

Прототипом для програмного продукту моніторингу мережевих процесів обрано модель 3Д-інтернету (моніторінгу), яка розроблялась у рамках японського проекту Daedalus [5]. Мережний трафік візуалізується в реальному часі у тривимірному інтерфейсі програми. Центральне коло – це інтернет, а сині кільця по периметру – корпоративні мережі. Оператор бачить усі типи трафіку, які виникають у системі, й може перемикати кілька режимів перегляду. Daedalus – це система раннього реагування з інтерфейсом для перегляду даних із 190 тис. японських IP-адрес, які відстежуються в рамках мережі спостереження Darknet Observation Network, створеної інженерами Національного інституту інформаційних і комунікаційних технологій Японії (NICT). Кожне кільце становить корпоративну мережу, де синій фрагмент відбиває активні IP-адреси, а чорні ділянки – неактивні IP-адреси. Поруч із відповідними IP-адресами візуалізуються жовті піктограми, що сповіщають про проведення кібератаки (наприклад, обмін пакетами між активними та неактивними IP-адресами вказує на поширення вірусу). Із натисканням на піктограму виводиться докладна інформація.

Для організації моніторингу інформаційних систем державних установ (організацій) параметри мережі, що контролюється, необхідно доповнити такими даними для візуалізації:

- часовими характеристиками активного існування IP-адрес та їх зв’язків;
- дозволеними шляхами інформаційних потоків;
- грифами секретності робочих станцій та пакетів даних;
- піковими навантаженнями на елементи системи;
- типами пакетів, що передаються;
- кордонами сегментів мереж.

Урахування таких даних дозволить отримати більш ефективну процедуру моніторингу функціонування інформаційних систем органів військового управління. Візуалізація процесів, які відбуваються в мережі, виведе аналіз процесу проведення кібератаки з площини “порушник – робоча станція” в площину “порушник – адміністратор моніторингу – робоча станція”.

## ЛІТЕРАТУРА

1. Історія обчислювальної техніки [Електронний ресурс]. – Режим доступу : – http://uk.m. wikipedia.org/article/31.htm.

2. Шабанов И. Программные закладки в бизнес-приложениях [Електронний ресурс]. – Режим доступу – http://www.bezopasnik.org/article/31.htm.

3. Информационная безопасность государства в военной сфере : науч.-метод. издание / Н.Н.Биченок, Т.М.Дзюба, А.А.Рось и др. – К. : НУОУ, 2012. – 264 с.

4. Антюхов В.И. Безопасность информационных систем и защита информации [Електронний ресурс] / В.И.Антюхов, А.Ю.Иванов. – Режим доступу. – http://gendocs.ru/ v11039.

5. Japan`s NICT develops futuristic `Deadalus` cyber-attack alert system [Електронний ресурс]. – Режим доступу : http://www.nict.go.jp/press/2012/06/06-1.html&usg=ALkJrhj C5Z79WU2TUtPne9XB0Z-ekHvHS.

*Войтюк О.С.,*
*кандидат юридичних наук,*
*Національна академія Служби безпеки України*

## ПРОБЛЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ У ВІЙСЬКОВІЙ СФЕРІ УКРАЇНИ

За умов глобальної інтеграції та жорсткої міжнародної конкуренції головною ареною зіткнень і боротьби різновекторних національних інтересів держав стає інформаційний простір. Сучасні інформаційні технології дають змогу державам реалізувати власні інтереси без застосування військової сили, послабити або завдати значної шкоди безпеці конкурентної держави, яка не має дієвої системи захисту від негативних інформаційних впливів. Збитки, що можуть бути завдані Україні в результаті несанкціонованого доступу до інформаційних ресурсів, мають прояви у військовій сфері – за рахунок падіння боєздатності військових формувань держави.

Відповідно до статті 17 Конституції України "…забезпечення інформаційної безпеки є однією з найважливіших функцій держави, справою всього Українського народу" [1]. Згідно із законодавством України інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації [3].

Динаміка розвитку інформаційних технологій у військовій сфері України висуває підвищені вимоги до вирішення питань інфор-

маційної безпеки. Сьогодні неможливо оцінювати бойовий потенціал військ і озброєння без урахування розвитку інформаційних систем та засобів.

Загрози інформаційній безпеці у військовій сфері України такі:

- неконструктивна політика іноземних держав щодо глобального інформаційного моніторингу, поширення інформації й нових інформаційних технологій;
- розвідувально-підривна діяльність спецслужб іноземних держав, спрямована проти військових формувань України;
- протиправна діяльність міжнародних терористичних й екстремістських організацій;
- злочинні діяння організованих кримінальних угруповань;
- протиправна діяльність окремих осіб, пов'язана з комп'ютерними злочинами;
- психологічні операції із використанням засобів масової інформації, інформаційні війни;
- порушення установлених форм збирання, оброблення і передавання інформації в органах військового управління, військових частинах й установах військових формувань України;
- навмисні дії та ненавмисні помилки персоналу інформаційних систем спеціального призначення у військових формуваннях;
- відмови технічних засобів і неполадки програмного забезпечення в інформаційних системах спеціального призначення у військах.

Інформаційними засобами реалізації наведених загроз є: порушення адресності та своєчасності інформаційного обміну, протизаконний збір та використання інформації; несанкціонований доступ до інформації й інформаційних ресурсів військових формувань України, неправомірні знищення, модифікація і незаконне копіювання даних з інформаційних систем; крадіжка інформації з бібліотек, архівів, банків та баз даних військових частин; порушення технологій оброблення інформації.

Найбільш уразливими об'єктами інформаційної безпеки у військовій сфері є: інформаційні ресурси органів військового управління, військових частин і установ військових формувань України, які містять інформацію щодо оперативних і стратегічних планів підготовки й ведення бойових дій, мобілізаційної готовності, тактико-технічних даних озброєння і військової техніки; інформаційні ресурси підприємств військово-промислового комплексу, що містять інформацію про їхній науково-технічний та виробничий потенціал, основні напрями розвитку озброєння, військової техніки, фундаментальні і прикладні науково-дослідні та досвідно-конструкторські роботи, які ведуться в інтересах оборони; системи зв'язку й автома-

тизовані системи управління військами та озброєнням, їх інформаційне забезпечення; морально-психологічний стан військ у частині, що залежить від інформаційно-пропагандиського впливу; інформаційна інфраструктура, зокрема центри оброблення, аналізу та зберігання інформації органів управління військових формувань України.

Основними напрямами подальшого удосконалення інформаційної безпеки у військовій сфері є: концептуальний, організаційний і технічний. Концептуальний передбачає структуризацію цілей забезпечення інформаційної безпеки у військовій сфері й відповідних практичних завдань. Організаційний, пов'язаний із необхідністю формування оптимальної структури та складу функціональних органів системи інформаційної безпеки у військовій сфері і координації їх ефективної взаємодії, удосконалення методів і засобів активної протидії технічній розвідці спецслужб іноземних держав. Технічний характеризується постійним удосконаленням засобів захисту інформаційних ресурсів від несанкціонованого доступу до них, розвитком захищених систем, зокрема систем зв'язку й управління військами й озброєнням, підвищенням надійності спеціального програмного забезпечення.

Одним із головних напрямів подальшого удосконалення інформаційної безпеки у військовій сфері виступає ефективний захист інформації щодо розробок, створення й тактико-технічних характеристик озброєння і військової техніки. Найбільш перспективним шляхом удосконалення структури управління інформаційною системою у військовій сфері України є використання нетрадиційних структур управління, орієнтованих на вирішення проблем. Для цього доцільно у військових формуваннях України створити єдиний центр інформаційної безпеки, який би координував діяльність усіх структур щодо забезпечення безпеки інформаційного ресурсу у військах. Як головний орган він повинен виконувати такі функції:

- координувати здійснення у військових формуваннях досліджень і робіт, що стосуються проблем інформаційної безпеки;
- брати участь у розробленні і забезпеченні виконання військовими формуваннями державних програм, спрямованих на захист державної таємниці;
- організовувати уведення у військових формуваннях обов'язкової атестації систем управління на вимоги безпеки інформації.

## ЛІТЕРАТУРА

1. Конституція України : прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 р. // Відомості Верховної Ради України. – 1996. – № 30. – Ст. 17.

2. Закон України “Про інформацію” від 2 жовтня 1992 року // Відомості Верховної Ради України – 1992. – № 48. – Ст. 651.

3. Закон України “Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки” // Відомості Верховної Ради України. – 2007. – № 12. – Ст. 102.

4. Закон України “Про основи національної безпеки України” // Відомості Верховної Ради України. – 2003. – № 39. – Ст. – 351.

5. Гавловський В. Організаційно-правові питання формування державної інформаційної політики в Україні / В.Гавловський, В.Гриценко, В.Цимбалюк // Збірник наукових праць Академії державної податкової служби України. – 2002. – № 3 (17). – С. 177–182.

6. Петрик В.М. Щодо визначення інформаційної безпеки та її різновидів / В.М.Петрик // Форми та методи забезпечення інформаційної безпеки держави : збірник матеріалів міжнародної науково-практичної конференції (м. Київ, 13 березня 2008 р.). – К. : Видавець Захаренко В.О., 2008. – С. 160–164.

7. Информационно-психологическая безопасность в эпоху глобализации : учеб. пособ. / [под. ред. В.В.Остроухова]. – К., 2008. – 544 с.

*Грицюк Ю.І.,*
*доктор технічних наук, професор,*
*Львівський ДУ БЖД*

*Хомін Д.М.,*
*Львівський ДУ БЖД*

## УПРОВАДЖЕННЯ БІОМЕТРИЧНИХ ТЕХНОЛОГІЙ У ДЕРЖАВНІЙ СЛУЖБІ НАДЗВИЧАЙНИХ СИТУАЦІЙ УКРАЇНИ

Зовсім недавно термін “біометрія” широко використовувався в основному коли йшлося про методи математичної статистики, які застосовувалися до будь-яких біологічних об’єктів. Зараз під біометричними технологіями найчастіше розуміють автоматизовані методи розпізнавання особи за біологічними або поведінковими ознаками [2; 3]. Біологічною ознакою може бути будь-який вроджений або повільно змінюваний параметр, індивідуальний для кожної людини. Державна служба надзвичайних ситуацій України (ДСНС України) – одна із державних установ, де тільки в останні роки по-

чали впроваджувати біометричні технології ідентифікації особи. Розглянемо деякі проблеми та перспективи їх упровадження в головних і територіальних управліннях.

Система біометричної ідентифікації особи може зчитати біологічні дані людини та визначити її як особу, зіставивши ці дані з біометричною інформацією в базі даних, отриманою внаслідок попереднього сканування цієї людини. Наразі практичне застосування отримала невелика кількість біометричних показників людини. Найвідомішими є "три великі біометрики", які дають змогу ідентифікувати особистість людини з високою достовірністю розпізнавання [2]: за відбитками пальців – 28,3 %; райдужною оболонкою ока – 26,7 %; зображенням обличчя – 20,8 %. Решта припадає на геометрію руки – 12,5 %, на верифікацію голосу – 9,2 % та підпису – 2,5 %.

Будь-яка система біометричної ідентифікації особи працює за таким узагальненим алгоритмом [3]:

1. Спеціальний сканер зчитує біометричний параметр людини.

2. Шляхом звернення до локальної або зовнішньої бази даних установлюється її особа, тобто отриманий біометричний параметр порівнюється з попередньо зареєстрованим біометричних шаблоном.

3. Приймається конкретне рішення, наприклад, подається команда на відкриття дверей або надається доступ до ПК чи мережі.

Основне призначення будь-якої системи біометричної ідентифікації особи в ДСНС України – позбавлення користувачів проблем, пов'язаних із втратою ключів і посвідчень особи, а також від потреби запам'ятовувати ідентифікаційний код, паролі. Унікальність біометричних параметрів кожної людини робить неможливим їх використання третіми особами [3]. Процес спілкування користувача з біометричним сканером відбувається легко і вимагає мінімальних часових витрат. Процес розпізнавання, завдяки інтуїтивності програмного й апаратного інтерфейсу, зрозумілий і доступний людям будь-якого віку і не знає мовних бар'єрів.

Головне в системі біометричної ідентифікації особи – забезпечення максимальної безпеки і точності ідентифікації. При цьому часто доводиться вибирати між безпекою, точністю і простотою використання. Наприклад, надточна система біометричної ідентифікації особи може бути складною у використанні й не подобатися користувачам через деякі неточності біометричних сканувань. Розчаровані користувачі намагатимуться знайти можливості обійти систему, знижуючи цим самим її ефективність і загальну безпеку [2].

Утім, жодна із систем ідентифікації особи, в т.ч. біометричних, не захищена від неправильного її використання [3]. Кожна біометрична технологія має свої сильні та слабкі сторони. Деякі з цих тех-

нологій є оптимальними для надання доступу до ПК або мережі, тоді як офісні системи можуть використовуватися в багатьох інших середовищах (як зовнішніх, так і внутрішніх).

Стосовно проблеми надійності зберігання біометричних даних. Якщо покупець віддає продавцеві свою кредитну картку або залишає свій відбиток пальця, то він сподівається, що цією інформацією не скористається хто-небудь ще. Проте внутрішня безпека будь-якого підрозділу ДСНС України може бути порушена, а персональні дані, які використовуються для ідентифікації особи, вкрадені [2].

Об'єктом крадіжки може стати навіть уся база біометричних даних, позаяк підрозділи, що застосовують біометричні системи, не застраховані від такої можливості. Якщо у вас вкрали кредитну картку або номер соціального страхування, то ви завжди зможете їх замінити, чого не можна сказати про відбитки пальців. Якщо зловмиснику вдасться замінити в базі даних зображення ваших відбитків пальців, то він зможе отримати доступ до ваших рахунків або конфіденційних документів. Він навіть може спробувати виготовити форму вашого пальця і використовувати її для обману дактилоскопічного сканера.

Утім, компанії – виробники сучасних біометричних систем розробили засоби для обмеження таких ризиків [1]. Розглянемо деякі з них.

Марк Кросбі (Mark Crosbie), головний архітектор із питань безпеки компанії Hewlett-packard, уважає, що багато людей бояться, що їхні відбитки пальців вкрадуть і вони будуть загублені назавжди [2]. Проте, на відміну від паролів, безпека біометричних даних не пов'язана із забезпеченням їх конфіденційності. Компанії, які використовують сучасні біометричні системи, зберігають замість зображень відбитків пальців оброблені форми, так звані шаблони, які є зменшеними цифровими зображеннями відбитків пальців. За допомогою криптографії ці шаблони можна захистити так, що якщо сьогодні їх вкрасти, то вже завтра вони будуть неактуальні. Ступінь захисту бази біометричних шаблонів відбитків пальців, райдужної оболонки ока чи зображення обличчя може бути таким, як і у баз даних номерів кредитних карток або номерів соціального страхування [1].

Наприклад, певний підрозділ ДСНС України бере відбитки пальців, коли працівник реєструється в її системі [3]. Потім зображення перетворюється на 40 унікальних точок на пальці, інформація зберігається в зашифрованій базі даних, а зображення відбитка пальця видаляється. Коли працівник сканує свій палець, біометрична система використовує для його ідентифікації тільки ці унікальні точки. Водночас, самі точки не можуть бути використані для відтворення відбитка пальця працівника.

Використання біометричної технології у поєднанні з паролями і PIN-кодами робить крадіжку особистих ідентифікаційних даних практично неможливою [2]. Проте абсолютно захищеної системи досі не існує. При неправильному використанні біометричні дані й номери кредитних карток однаково не захищені від крадіжки. Надаючи свої біометричні дані, користувачі мають знати ризики їх викрадення та переваги їх використання, оскільки ці системи набувають все більшого поширення не тільки в розвинутих країнах Сходу і Заходу. Скоро вони будуть практично всюди.

Що стосується загальних перспектив розповсюдження та розширення біометричних технологій у структурних підрозділах ДСНС України, то тут аналітики передбачають на найближчі роки зростання кількості охочих їх застосувати приблизно на 25-30 %. При цьому найдинамічніше розвиватимуться відділи ІТ, в основному за рахунок недорогих продуктів для ПК. Однак тут є одна проблема, яка помітно перешкоджатиме масовому поширенню біометричних технологій. Ідеться про захист приватних прав користувачів. Варто згадати хоча б паніку серед користувачів ПК, коли компанія Intel вирішила вбудувати у свої процесори ідентифікаційні номери. У нашому ж випадку відкриваються колосальні можливості для зловмисників щодо збирання персональної інформації про користувачів ПК, та ще й без їх відома!

Загалом проблема надійного зберігання біометричних даних у підрозділах ДСНС України, як і будь-якої конфіденційної інформації, за бажання повністю вирішується [2, 3]. Найскладніше – це переконати людей, що конфіденційність подібних відомостей повністю гарантована. Позаяк, аналітики уважають, що можуть виникнути й певні складнощі суто психологічного характеру: зняття відбитків пальців поки що викликає в багатьох людей певні асоціації з причетністю до кримінальних справ.

Утім, важко не погодитися з тим, що біометричні технології є набагато надійнішими і зручнішими за ті засоби захисту, які широко застосовувалися донедавна, й забезпечують чималі переваги, насамперед, для кінцевих користувачів. Тому багатьом доведеться поступово звикати до думки, що коли-небудь замість пропозиції поставити свій підпис на документі ми почуємо: “Прикладіть руку”. Як свого часу князі, царі та інші повелителі свої укази скріплювали печаткою, яка знаходилася на пальці руки.

## ЛІТЕРАТУРА

1. Березин А. Идентификация по радужной оболочке глаза, скорее всего, станет повсеместной нормой, 19 апреля 2012 года / А.Березин. [Электронный ресурс]. – Доступный с http://science.compulenta.ru/674396/.

2. Биометрические средства идентификации личности [Электронный ресурс]. – Доступный с http://xreferat.ru/33/6447-1-biometricheskie-sredstva-identifikacii-lichnosti.html.

3. Биометрия. Изображение лица. [Электронный ресурс]. – Доступный с http:// wiki. oszone.net/index.php/Биометрия._Изображение_лица.

*Гулак Г.Н.,*
*Національна академія Служби безпеки України*

## ПОНЯТІЙНИЙ АПАРАТ ТА МОДЕЛІ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Вивчення виданих у 2011-2012 рр. аналітичних оглядів провідних експертів із питань інформаційної безпеки [1; 2] свідчить про вступ світового суспільства до якісно нової фази протиборства в глобальному інформаційному просторі. Ця фаза характеризується:

– колосальними масштабами проведення атак за географією розповсюдження шкідливих кодів шпигунських програм, а також інтенсивністю фіктивних запитів у випадку проведення DDoS–атак на інформаційні ресурси;

– широким спектром об’єктів атак (здебільшого це автоматизовані системи урядових установ, збройних сил, правоохоронних органів та великих комерційних компаній);

– активними та скоординованими діями порушників, що застосовували кваліфіковано спроектовані засоби нападу.

За різними оцінками, щорічні світові втрати від вандалізму кіберзлочинців становлять від 290 до 750 мільярдів євро.

Необхідність відповіді на виклики сучасності потребує адекватних дій на урядовому рівні, зокрема прийняття необхідних законодавчих актів, розроблення стратегії реалізації організаційних та інженерно-технічних заходів щодо убезпечення не тільки інформаційно-комунікаційних технологій, а й усіх *інтелектуалізованих інфраструктур найважливіших галузей суспільного виробництва та життєдіяльності людини*.

Саме наповнення “інтелектом” звичайних сфер транспорту, промисловості, енергетики, охорони здоров’я та багатьох інших за допомогою потужних комп’ютерів і вбудованих мікроконтролерів робить їх не тільки більш ефективними, життєво важливими для кожної особи, народу і всього людства, але й більш уразливими до загроз антропогенного й техногенного характеру, природних катаклізмів.

За останнє десятиріччя у більшості провідних країн світу створені спеціальні урядові структури або ініційовані процеси формування органів, що покликані забезпечити безпеку національного інформаційного простору, критичних інфраструктур. Їх повноваження і зона відповідальності визначені з урахуванням історичних традицій, національних пріоритетів та законодавства.

Серед множини функцій цих органів слід відмітити найбільш важливу та загальну, а саме забезпечення безпеки кібернетичного простору, захист критично важливих для людини, суспільства і держави інфраструктур.

У документах Всесвітньої конференції міжнародного електрозв'язку WCIT-2012 (Дубай, ОАЕ, 3-14.12.12) відмічено, що відсутність узгодженого на міжнародному рівне визначення кібербезпеки стримує міжнародні та національні зусилля з захисту мереж і комп'ютерних систем, що фактично не мають кордонів.

Зауважимо, що вже на початку лютого цього року (7.02.2013) була презентована стратегія дій Євросоюзу у сфері кібербезпеки. Її ключовою ланкою є директива, що зобов'язує уряди країн ЄС створити профільні адміністративні органи та забезпечити їх фінансування.

У світлі розв'язання актуальних проблем, що стоять перед Україною в плані забезпечення національної безпеки, нагальним постає завдання визначення власних пріоритетів у цій сфері, що неможливо без науково обґрунтованого термінологічного апарату та побудови моделей атак і захисту власного кричного середовища.

Таким чином, слід відповісти на питання:

- що таке "кібернетичний простір", "кібернетична безпека" і "забезпечення безпеки кіберпростору";
- чим відрізняється "забезпечення безпеки кіберпростору" від "захисту інформації".

Відповідь на останнє запитання зумовила два основних підходи до вирішення проблем у цій сфері.

Підхід Російської Федерації фактично визнає існування такого феномену, як кібернетичний простір, але на законодавчому рівні цей термін не закріплений.

Засадничий керівний документ РФ у царині національної безпеки – Доктрина інформаційної безпеки [5] – уводить лише поняття "інформаційна безпека", яке включає два компоненти: "захищеність національного інформаційного простору від впливу зовні" та "захист інформаційних ресурсів в електронному вигляді".

Положення Доктрини в основному фокусуються на різних аспектах захисту інформації в такій категорії автоматизованих систем,

як інформаційні та телекомунікаційні. Виходячи з контексту, можна припускати, що при цьому мова переважно йде про захист "змістовної", документальної інформації.

Разом із тим, слід відзначити той факт, що в сучасному промисловому світі постійно збільшується кількість використовуваних систем типу "автоматизовані системи управління технологічними процесами" (АСУ ТП), зокрема у галузях, особливо небезпечних для життя людини, включаючи управління різного роду хімічними виробництвами, усіма видами транспорту (повітряний, наземний і морський), виробництвом і розподілом електроенергії тощо.

У той же час, у наукових колах, зокрема в рамках американо-російських наукових симпозіумів 90-х років минулого сторіччя, було відмічено виникнення такого феномену, як "кібернетичний простір" (Cyberspace) і його вплив на критичні галузі суспільного виробництва [3]. У пізніших роботах російських вчених між поняттями "інформаційна безпека" й "кібернетична безпека", висловлюючись мовою математичних операцій, фактично ставлять знак "суворе включення" на користь першого [4].

Відсутність у низці російських досліджень проблем "інформаційних воєн" чіткого розмежування понять "захист від інформації" і "захист інформації" призводить до змішування методів та засобів інформаційно-психологічного впливу на населення з методами і засобами інженерно-технічних атак на цифровий інформаційний простір [6], визнання факту існування "кібернетичного простору" без його конкретного тлумачення [7].

У цих умовах убачається логічним виділити соціально-політичні технології інформаційних війн у самостійну дисципліну [8]. Також доцільно окремо вивчати інженерно-технічні аспекти інформаційних війн [9].

При цьому інформаційну зброю слід класифікувати за характером її впливу на мережеві ресурси/ автоматизовані системи, окремо розглядаючи засоби нападу, призначені для створення каналів витоку інформації з обмеженим доступом (мета – шпигунство, інше порушення конфіденційності) або порушення штатного функціонування системи та/або руйнування технічних чи програмних засобів, а також цифрових інформаційних ресурсів (мета – диверсія, терор або порушення цілісності й доступності).

Що стосується підходу США, офіційне тлумачення терміна "кіберпростір" містила низка директив Білого дому [11]. Ці документи визначають кіберпростір як взаємозалежну мережу інфраструктур інформаційних технологій, включаючи інтернет, телекомунікаційні мережі, комп'ютерні системи, а також процесори й контролери, вбудовані в критичні галузі виробництва.

До об’єктів потенційних атак терористів віднесено сукупність об’єднаних життєво важливою інфраструктурою ключових ресурсів, керованих приватним сектором, державою або органами місцевого самоврядування. Слід звернути увагу, що в зазначених документах згадуються два взаємодоповнюючих механізми безпеки: “охорона критичних структур” і “забезпечення безпеки кіберпростору”.

Для реалізації федеральних завдань у сфері національної безпеки, запобігання атакам і реагування на протиправні дії в мережевому середовищі у листопаді 2002 року було створено Міністерство національної безпеки США (US Department Homeland Security); у січні 2013 на базі ФСБ Росії – державну систему виявлення, попередження і ліквідації наслідків комп’ютерних атак на інформаційні ресурси РФ [10].

Порівняльний аналіз підходів до забезпечення захищеності від комп’ютерних атак критичної інформаційної інфраструктури Росії й безпеки кіберпростору США дозволяє зробити висновок про їх збіг за низкою основних позицій і відмінності в деяких деталях. Головне в обох випадках – наявність потужного федерального центру щодо забезпечення розслідувань інцидентів та технічної підтримки попередження атак і ліквідації їх наслідків.

З урахуванням викладеного вище, можна охарактеризувати цифровий інформаційний (кібернетичний) простір як глобальну мережеву структуру, вузли комутації якої також є мережевими структурами, при цьому кожен вузол може мати кілька шляхів, що зв’язують його з усіма іншими вузлами.

Кожен вузол, за наявності з’єднувального шляху, може ініціювати звернення до іншого вузла структури для отримання дозволу на прийом (операція читання) або передачу (операція запису) даних.

Дозволи й заборони на проведення операцій (установлення логічного зв’язку) становлять частину стратегії забезпечення безпеки простору, оскільки нелегальна операція читання несе загрозу конфіденційності інформації, нелегальний запис – її цілісності; нелегальні запити, навіть не будучи реалізованими, можуть частково або повністю заблокувати той чи інший шлях доступу до певного вузла.

Глобалізація інформаційних технологій призводить до зменшення кількості і розмірів ізольованих кластерів. А це відповідає ситуації, коли з більшості вузлів мережевої структури можна установити логічний зв’язок практично з будь-яким її вузлом, якщо правила розмежування доступу не заблокують цей зв’язок.

Таким чином, можливо стверджувати, що кіберпростір не існував, поки вузли мережевої структури однозначно не ототожнилися з більшістю сфер життєдіяльності так, що порушення зв’язаності усієї

мережевої структури могло призвести до порушення істотних умов реалізації такої діяльності. Крім того, постійно зростаюча поєднаність мережевої структури створює передумови для реалізації загроз, які виходять з однієї її частини, щодо інших частин.

Як наслідок, цілком очевидний висновок про необхідність якнайшвидшого вирішення питання про створення в нашій державі єдиного центру з питань мережевої безпеки з основними завданнями:

- реагування на інциденти в галузі безпеки та кризового управління процесами відновлення критичних інфраструктур;
- розслідування інцидентів у галузі безпеки критичних інфраструктур;
- організації інформаційно-технічної взаємодії з власниками критичних інфраструктур у державному та комерційному секторі, розроблення методик виявлення атак і методичних рекомендацій щодо захисту, а також планів попередження/блокування атак на об'єкти критичної інформаційної структури економіки, транспорту, паливно-енергетичного комплексу та ін., включаючи використання повноважень правоохоронних органів.

## ЛІТЕРАТУРА

1. "Red October" Diplomatic Cyber Attacks Investigation [Сетевой ресурс, URL]. – Режим доступа : http://www.securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation;

2. Лукацкий А. Почему атакуют объекты ТЭК? [Сетевой ресурс, URL] / А.Лукацкий. – Режим доступа : http://www.securitylab.ru/blog/personal/Business_without_danger/29330.php.

3. Высокотехнологичный терроризм : материалы российско-американского семинара, Москва, 4-6 июня 2001 г. – М., 2001. – 320 с.

4. Смирнов А.И. Информационная глобализация и Россия: вызовы и возможности / А.И.Смирнов. – М. : Изд. дом "Парад", 2005. - 392 с.

5. Доктрина информационной безопасности РФ // Научные и методологические проблемы информационной безопасности (сборник статей) / [под ред. В.П.Шерстюка]. – М. : МЦНМО. – 2004. – С. 149–197.

6. Воронцова Л.В. История и современность информационного противоборства / Л.В.Воронцова, Д.Б.Фролов. – М. : Горячая линия – Телеком, 2006. –192 с.

7. Гриняев С.Н. Поле битвы – киберпространство: Теория, приемы, средства, методы и системы ведения информационной войны / С.Н.Гриняев. – Мн. : Харвест, 2004. - 448с.

8. Бухарин С.Н. Методы и технологии информационных войн / С.Н.Бухарин, В.В.Цыганов. – М. : Академический проект, 2007. – 382 с.

9. Васенин В.А. Информационная безопасность и компьютерный терроризм / В.А.Васенин // Научные и методологические проблемы информационной безопасности (сборник статей) / [под ред. В.П.Шерстюка]. – М. : МЦНМО, 2004. – С. 67–83.

10. Указ Президента РФ от 15 января 2013 г. № 31с "О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации" [Сетевой ресурс, URL]. – Режим доступа : http://text.document.kremlin.ru/SESSION/PILOT/main.htm.

11. Национальная стратегия обеспечения безопасности киберпространства США (неофициальный перевод) // Смирнова А.И. Информационная глобализация и Россия: вызовы и возможности / А.И.Смирнова. – М. : Изд. дом "Парад", 2005. – С. 363–370.

*Дрейс Ю.О.,*
*Житомирський військовий інститут ім. С.П.Корольова*
*Національного авіаційного університету*

## ВИЗНАЧЕННЯ ВЕЛИЧИНИ МОЖЛИВОЇ ШКОДИ У РАЗІ РОЗГОЛОШЕННЯ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ ЧИ ВТРАТИ ЇЇ МАТЕРІАЛЬНИХ НОСІЇВ

Сучасний інформаційний простір складається з відкритої інформації, яка вільно поширюється, обробляється і зберігається, та тієї, доступ до якої обмежено, – інформації з обмеженим доступом (ІзОД) [1]. Таке обмеження доступу здійснюється відповідно до закону [2], якщо вона містить конфіденційну, службову чи таємну інформацію при дотриманні сукупності вимог, коли розголошення такої інформації може завдати істотної шкоди інтересам національної безпеки або шкода від оприлюднення переважає суспільний інтерес в її отриманні тощо. Тобто, можна стверджувати, що якщо немає завдання шкоди, то відсутні підстави для обмеження у доступі.

Наразі питання визначення величини цієї шкоди постає досить гостро. Адже саме її розмір повинен визначати, до якого виду ІзОД слід віднести інформацію в разі її розголошення чи втрати матеріальних носіїв (МНІ), наприклад: до *конфіденційної* – якщо шкода завдається фізичній чи юридичній особі, крім суб'єктів владних пов-

новажень (наприклад, персональні дані [3]), і тому порядок її поширення визначений за їхнім бажанням відповідно до передбачених ними умов; до *службової* – якщо шкода завдається суб'єктам владних повноважень у певному напрямі діяльності установи або при здійсненні контрольних, наглядових функцій органами державної влади, в процесі прийняття рішень, оперативно-розшукової, контрозвідувальної діяльності, що передують публічному обговоренню; до *таємної* – якщо шкода завдається особі, суспільству й державі та інформація містить державну, професійну, банківську таємницю, таємницю досудового розслідування та іншу передбачену законом таємницю, наприклад, таємницю усиновлення, лікарську таємницю тощо. Із перерахованих видів таємниць досить добре врегульовано державну таємницю (ДТ) [4], адже це питання забезпечення національної безпеки [5].

Як відомо, розмежування основних видів ІзОД відбувається за ступенем та грифом обмеження доступу для МНІ, що демонструє своєрідну нечітку величину можливої шкоди, наприклад, для службової інформації – "для службового користування" (ДСК), а для таємної інформації, зокрема державної таємниці (за ступенем та грифом секретності) – "таємно" (Т), "цілком таємно" (ЦТ), "особливої важливості" (ОВ).

Питанням визначення величини можливої шкоди національній безпеці держави у разі розголошення ДТ чи втрати матеріальних носіїв секретної інформації (МНСІ) займається обмежене коло науковців України (Корченко О.Г., Архипов О.Є., Муратов О.Є., Ворожко В.П., Касперський І.П.).

Наразі в Україні є лише одна методика [6] щодо визначення підстав для віднесення відомостей до ДТ та ступеня їх секретності. Її принцип полягає в бальному розрахунку величини прогнозованої сукупної шкоди за критерієм: $1 \le W < 10$ – "Т"; $10 \le W < 100$ – "ЦТ"; $100 \le W$ – "ОВ". Методичні рекомендації [6] містять низку невирішених питань та недоліків, але саме вони стали основою для подальшого дослідження означеної проблеми [7-8].

Для прийняття рішення, наприклад, у судовому процесі, щодо визначення розміру збитку, завданого національній безпеці держави в разі розголошення ДТ чи втрати МНСІ необхідно за допомогою наявних засобів у сфері охорони ДТ (ОДТ) проводити аналіз і оцінювання розмірів можливої шкоди. Результат оцінювання величини шкоди має бути зрозумілим та вираженим у прийнятних показниках (грошах) для подальшого її відшкодування, тощо.

На основі проведеного дослідження *розроблено* базову модель інтегрованого представлення параметрів шкоди шляхом логіко-

лінгвістичного підходу та узагальнення ідентифікуючих і оціночних показників засобів у сфері ОДТ; метод [9]; методологію синтезу системи, систему аналізу й оцінювання величини можливої шкоди національній безпеці держави у разі розголошення ДТ чи втрати МНСІ та відповідне програмне забезпечення з можливістю автоматизованого формування звіту отриманих результатів.

Залишається актуальним питання визначення величини можливої шкоди в разі розголошення конфіденційної, наприклад персональних даних, чи службової інформації або втрати їх МНІ, де, наприклад, $0 < W < 1$ може бути критерієм для визначення ДСК.

## ЛІТЕРАТУРА


1. Про інформацію / Верховна Рада України; Закон від 02.10.1992 № 2657-XII (редакція від 09.05.2011) // [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/2657-12.

2. Про доступ до публічної інформації / Верховна Рада України; Закон від 13.01.2011 № 2939-VI (редакція від 19.11.2012) // [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/2939-17.

3. Про захист персональних даних / Верховна Рада України; Закон від 01.06.2010 № 2297-VI (редакція від 20.12.2012) // [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/2297-17.

4. Про державну таємницю / Верховна Рада України; Закон від 21.01.1994 № 3855-XII (редакція від 24.02.2011) // [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/3855-12/page.

5. Про основи національної безпеки України / Верховна Рада України; Закон від 19.06.2003 № 964-IV (редакція від 20.07.2010) // [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/964-15.

6. Методичні рекомендації державним експертам з питань таємниць щодо визначення підстав для віднесення відомостей до державної таємниці та ступеня її секретності / Державний комітет України з питань державних секретів та технічного захисту інформації : Наказ № 22 від 09.11.1998 р. – К., 1998. – Збірка № 8. – С. 4–14.

7. Архипов О.Є. Оцінювання ефективності системи охорони державної таємниці : моногр. / О.Є.Архипов, І.Т.Бородавко, В.П.Ворожко. – К. : Наук.-вид. відділ НА СБ України, 2007. – 63 с.

8. Архипов О.Є. Критерії визначення можливої шкоди національній безпеці України у разі розголошення інформації, що охороняється державою : моногр. / О.Є.Архипов, О.Є.Муратов. – К. : Наук.-вид. відділ НА СБ України, 2011. – 195 с.

9. Корченко О.Г. Метод аналізу та оцінки величини можливої шкоди національній безпеці держави у сфері охорони державної таємниці / О.Г.Корченко, С.В.Казмірчук, Ю.О.Дрейс // Захист інформації: науково-практичний журнал. – Вип. №3 (56). – К. : НАУ. – 2012. – С. 5–18.

*Засядько А.А.,*
*доктор технічних наук, доцент,*
*Університет банківської справи НБУ, ЧІБС, м. Черкаси*

*Клювак О.В.,*
*Університет банківської справи НБУ, ЛІБС, м. Львів*

## ПОСИЛЕННЯ БЕЗПЕКИ ЗДІЙСНЕННЯ ТРАНЗАКЦІЙ В ІНТЕРНЕТІВСЬКИХ ПЛАТІЖНИХ СИСТЕМАХ ВІРТУАЛЬНИМИ КАРТКАМИ

У схемі здійснення транзакцій в інтернетівських платіжних системах з погляду безпеки найбільш критичним кроком є передання клієнтом-покупцем реквізитів банківської картки, які дають можливість аутентифікувати іншою стороною (продавцем) держателя платіжного засобу. Для убезпечення від перехоплення даних, які передаються через інтернетівську платіжну систему, застосовують механізм хешування. Проте, навіть такі криптостійкі хеш-функції, як MD-5 та SHA-1, на сьогодні піддаються злому. Тому, алгоритми хешування потребують постійного вдосконалення, а при розробленні необхідно здійснювати перевірку на крипостійкість.

Серед українських учених, які у своїх працях висвітлювали проблеми в галузі забезпечення автентичності банківських даних, криптографічних засобів захисту в платіжних-системах банків та хешування даних для забезпечення автентичності в комп'ютерних системах і мережах, можна виокремити таких: С.П. Євсєєв, А.А. Кузнецов, Т.Ю. Самбурська та інші. Серед іноземних фахівців, які проводили дослідження в галузі криптографічного захисту даних, що передаються через комп'ютерні системи й мережі, зокрема хешування даних для забезпечення їх автентичності, можна назвати таких, як: Peter Kankowski, William Stallings, Man Young Rhee, Sugata Sanyal, Ayu Tiwari and Sudip Sanyal, V. Pasupathinathan, J. Pieprzyk, H. Wang and J.Y. Cho, Sungwoo Kang, Haeryong Park, Donghyeon Cheon, Kilsoo Chun, Jaeil Lee, Ахо Альфред В., Хопкрофт Джон, Ульман Джеффри Д., Семенов Ю. А. та інші.

Опишемо комбінаційну схему хешування даних, котрі передаються під час здійснення інтернет-транзакції, та перевіримо цю схему на криптостійкість за допомогою визначення імовірності виникнення колізії.

Комбінаційний тип хешування, який пропонується застосовувати до даних, які передаються держателем картки на сервер інтернетівської платіжної системи при здійсненні автентифікації, полягає в тому, що генератор хеш-коду на вході отримує два елементи даних: сам код, який має бути захешовано та передано, і код схеми хешування.

Крім коду платник отримує ще одну із схем комбінаційного хешування. Цю схему також знає приймаюча сторона, отож вона не передається при пересиланні захешованого коду при здійсненні транзакції. Хешування за такою схемою передбачає використання одночасно 9 хеш-функцій (RSHash, JSHash, PJWHash, ELFHash, BKDRHash, SDBMHash, DJBHash, DEKHash, APHash). При цьому кожна з них отримує на вході одне й те саме поле, в цьому випадку, код ОВК, представлений у текстовому вигляді. Результати усіх функцій конкатенуються в єдине 288 бітове поле (кожна функція генерує чотирибайтове число, отож при конкатенації результатів дев'яти функцій утворюється поле довжиною 36 байтів). Те, в якій послідовності викликаються згадані функції, визначається кодом схеми хешування (КСХ). КСХ становить текстову стрічку довжиною 9 байтів, кожен символ якої ідентифікує одну певну хеш-функцію.

Криптостійка хеш-функція повинна мати такі властивості:

1. результат повинен обчислюватись для аргументу будь-якої довжини;
2. імовірність виникнення колізії повинна бути низькою;
3. алгоритм обчислення результату повинен бути відносно простим;
4. хеш-функція повинна бути одного напряму [1–3].

Розглянемо цю комбінаційну схему хешування під ракурсом перших двох властивостей, бо, на нашу думку, основна вимога з перелічених – друга. Загалом оцінити ймовірність виникнення колізії у хеш-функціях найпростіше таким чином. Припустимо, що результуюче значення хеш-функції може мати максимальне значення N. Оскільки це число є цілим і додатнім, це означає, що може бути N-можливих значень результату цієї хеш-функції. Оскільки є імовірність того, що вибірка k чисел із N-можливих міститиме значення, які повторюються, то імовірність того, що не міститиме, є доповнювальною до 1. Тобто імовірність, що таких дублів не буде, виражається формулою:

$$P = 1 - e^{\frac{-k(k-1)}{2N}} = \frac{k(k-1)}{2N}$$

Оскільки в нашом увипадку k набуває досить великих значень, то формулу можна спростити без вагомої втрати точності: $P = \frac{k^2}{2N}$

Стандартна хеш-функція генерує на виході число довжиною 4 байта, тобто 32 біти. Тому результат хеш-функції може бути в межах від 0 до $2^{32}$, а це означає, що кількість можливих варіантів $N=2^{32}$.

Важливою характеристикою якості хеш-функції виступає величина вибірки, при якій імовірність виникнення колізії дорівнює 50 %. Розрахуємо цю величину для 9 хеш-функцій: RSHash, JSHash, PJWHash, ELFHash, BKDRHash, SDBMHash , DJBHash , EKHash, APHash. Для цього розв'яжемо рівняння: $05 = \frac{k^2}{2^{32}}$ => k=65536. Це число означає, що при використанні хеш-функції 65536 разів є імовірність 50 %, що серед них буде бодай одна колізія. Звісно, це число буде дуже зростати при збільшенні N і зменшуватися при зменшенні ймовірності колізії.

Для того, щоб отримати імовірність виникнення колізії 50 % вибірка для 288-бітної хеш-функції повинна бути більшою у 2.8901 ч $10^{38}$ разів. Очевидно, що це є надзвичайно велике число. З іншого боку, імовірність виникнення колізії для 32-бітного числа вичерпується на 9 порядку (1 зі 100 млн), тоді як для 288 бітного вона може доходити до 86 порядку.

Отже, ефективний механізм автентифікації в інтернетівських платіжних системах передбачає уникнення передачі реквізитів платіжного засобу шляхом уведення у схему транзакції "онлайн власного коду" клієнта, який є прив'язкою до карткового рахунку. При хешуванні даних і банку, і клієнту відомі й код, і хеш-функції, якими здійснюється формування хеш-коду, тому банк може перевірити присланий захешований код, зіставивши із тим, який був отриманий шляхом проведення таких самих дій з тим самим кодом на стороні банку. Оскільки хешування – операція незворотна, це убезпечує від розшифрування вихідного коду зловмисником, якби він навіть перехопив захешовані дані. З іншого боку, хешування становить згортку початкової інформації, тобто існує хоча і мізерна, але таки існує імовірність отримання однакового результату при різних вхідних даних. Вказану імовірність можна зменшити ще на кілька порядків при застосуванні схеми комбінаційного хешування.

## ЛІТЕРАТУРА

1. Исследование протоколов и механизмов защиты информации в компьютерных системах и сетях [ Текст ] / А.А.Кузнецов, С.П.Евсеев, Б.П.Томашевский, Ю.И.Жмурко // Збірник наукових

праць Харківського університету Повітряних Сил ім. І.Кожедуба. – 2007. – № 2(14). – С. 102–111.

2. Credit Card Encryption and Password Hashing Utility Component [Електронний ресурс]. – Режим доступу : http://www.caritas.org.au/Content/ NavigationMenu/Caritas_Documents/PDFs/asiUtil_CreditCardEncryption.pdf.

3. Аутентификация в Интернет [Електронний ресурс] / Ю.А.Семенов – Режим доступу : http://docs.luksian.com/networks/techs/intro/?f=./6/authent.shtml.

4. Peter Kankowski Hash functions: An empirical comparison [Електронний ресурс ] / Peter Kankowski. – Режим доступу : http://www.strchr.com/hash_functions.

*Іванова О.С.,*
*Навчально-науковий інститут інформаційної безпеки*
*Національної академії Служби безпеки України*

## ФОРМУВАННЯ ЛОГІЧНОГО МАТЕМАТИЧНОГО МИСЛЕННЯ ПРИ ВИКЛАДАННІ МАТЕМАТИЧНИХ ДИСЦИПЛІН ДЛЯ СТУДЕНТІВ ТА КУРСАНТІВ

Ми прекрасно знаємо, що освіта нації – запорука її майбутнього. Адже система освіти суттєво впливає на формування духовних, моральних, естетичних та культурних цінностей людини.

Навчальний процес повинен постійно вдосконалюватися, адже сучасний ринок праці потребує не лише цілеспрямованих фахівців, які мають високий рівень теоретичної та практичної підготовки, але й таких, що спроможні самостійно приймати рішення, є ініціативними та творчими фахівцями, можуть швидко адаптуватись до нових умов на світовому ринку праці та вносити нові ідеї й розробки, тобто бути джерелом розвитку тієї галузі науки та виробництва, у якій вони задіяні.

Саме математичні науки є унікальним засобом формування таких якостей сучасного фахівця, як професійна компетентність, творче мислення, навички до самостійної наукової роботи. Математичні методи та математичне моделювання широко використовується для розв’язання практичних завдань із різних галузей науки, техніки, економіки, виробництва. Зокрема методи теорії ймовірності широко використовуються в різноманітних галузях природничих та технічних наук: у теорії надійності, теорії масового обслуговування,

теоретичній фізиці, геодезії, астрономії, теорії стрільби, теорії помилок спостереження, теорії автоматичного управління, загальної теорії зв'язку і т. ін.

У зв'язку з цим постають проблеми пошуку та винайдення засобів ефективного розвитку математичного мислення студентів та курсантів. Адже саме належний рівень розвитку логічного математичного мислення відіграє велику роль у формуванні таких якостей. Насамперед необхідно звернути увагу в навчальному процесі, на нашу думку, не тільки на те, що засвоюється (зміст навчання) студентами та курсантами, але й на якість засвоєння матеріалу. Переважно однією з особливостей викладання математичних дисциплін є бажання викладачів дати їх матеріал у повному обсязі, при цьому не ставлячи перед собою завдання формування у студентів та курсантів математичного логічного мислення.

На нашу думку, при викладанні математичних дисциплін слід звертати увагу на:

*1. Умови подання студентам матеріалу.*

Важко не погодитись, що успішність у засвоєнні матеріалу залежить від того, чи це здійснюється індивідуально чи колективно, в авторитарних чи гуманістичних умовах, з опорою на увагу, сприйняття та пам'ять чи на весь особистісний потенціал людини, за допомогою репродуктивних чи активних методів навчання.

*2. Максимальне використання наочного матеріалу із застосуванням комп'ютерних технологій.*

Справді, на заняттях працює принцип: "краще один раз побачити, ніж багато разів почути". Робота з предметами навколишньої дійсності вирішує завдання розвитку наочно-дійового, наочно-образного, а потім і словесно-логічного, абстрактного мислення студентів. Таким чином здійснюється корекція таких процесів мислення, як аналіз, синтез, узагальнення, абстрагування, формуються умови для розвитку пам'яті, уваги тощо.

*3. Уведення нетрадиційних лабораторних робіт.*

До такого типу робіт можна віднести, наприклад, момент виконання роботи на природі, де можна приділити увагу екологічному вихованню та реалізувати принцип міжпредметних зв'язків. Можна також розбити групу на команди по дві – три особи, поставивши перед кожною із них якусь конкретну математичну задачу, та запропонувати самостійно її розв'язати й порівняти методи її розв'язання. Таким чином, кожен із студентів та курсантів, у рамках своєї команди, може стати й експериментатором, і тим, хто перевіряє, здійснює розрахунки, що не лише формує практичні навички, а й дає

можливість установити логічний зв'язок теорії та практики, виховує відповідальність, працелюбство й колективізм.

*4. Спеціальний підбір задач та вправ, а також надання можливості студентам і курсантам створювати самим ситуативні моменти нових задач.*

Процес розв'язування задач відіграє значну роль у формуванні уявлень студентів та курсантів. Важливо підібрати задачі та вправи таким чином, щоб реалізувати їх зв'язок із конкретними ситуаціями життя та їх майбутньої спеціальності. Таким чином студенти та курсанти вчитимуться вирішувати життєво-практичні завдання, що будуть постійно зустрічатись після закінчення навчального закладу.

Ще один момент – складання задач самими студентами та курсантами. При цьому, по-перше, виховується самостійність (оперування вивченими об'єктами і фактами математичних наук), по-друге, розвивається математичне конструювання (застосування методів математичного моделювання) і, по-третє, розвивається творча активність.

*5. Упровадження професійної спрямованості при викладанні математичних дисциплін.*

*6. Правильну організацію самостійної роботи та розроблення спеціального навчально-методичного матеріалу, що сприяє ефективнішій самостійній роботі студентів та курсантів.*

Організація самостійної роботи повинна активно впливати на характер навчального процесу, систематизувати роботу студентів та курсантів протягом усього навчального процесу. Вона повинна охоплювати матеріали лекцій та семінарів, вироблення навичок правильного конспектування, професійний та термінологічний практикум, письмовий контроль за проблемою, огляд літератури, виконання самостійних різнорівневих проблемних та практичних завдань.

Отже, вивчення математичних дисциплін вносить невичерпний виховний і розвиваючий потенціал, і прихований він не в готових алгоритмах, теоремах та формулах, а в самій методиці подачі матеріалу. Тільки доцільно підібрані педагогічні методи спроможні розбудити (та підтримувати) мислення студента на мобілізаційно-діяльному рівні. Звичайно, що складність подачі матеріалу слід дозувати так, щоб чинити належний опір зусиллям студента та курсанта, не створюючи при цьому у нього враження безнадійності. Вражаючий результат засвоєння матеріалу грітиме душу викладача, і студент, і курсант переживатимуть незрівнянне емоційне піднесення, що надовго закарбується в душі. Виникне інтерес до самостійного вирішення інших, більш складних проблем. Є багато свідчень видатних математиків про те, що на хвилі саме такого емоційного піднесення вирішувалась їхня майбутня творча доля.

## ЛІТЕРАТУРА

1. Давыдов В.В. Проблемы развивающего обучения: опыт теоретического и экспериментального психологического исследования / В.В. Давыдов. – М., 1986.
2. Демиденко В.К. Психологія вищої освіти : навч. посіб. / В.К. Демиденко. – Бердянськ, 2003.
3. Дьяченко М.И. Психология высшей школы / М.И. Дьяченко, Л.А. Кандыбович. – Минск, 2003.
4. Метельський Н.В. Пути совершенствования обучения математике: пробл. современной методики математики / Н.В. Метельський. – Мн. : Университетское, 1989. – 160 с.
5. Мороз О.Г. Педагогіка і психологія вищої школи / О.Г. Мороз, О.С. Падалка, В.І. Юрченко. – К., 2003.
6. Пономарев Я.А. Знание, мышление и умственное развитие / Я.А. Пономарев. – М., 1967.
7. Слєпкань З.І. Методика навчання математики : підруч. для студ. мат. спеціальностей пед. навч. закладів / З.І. Слєпкань. – К. : Зодіак-ЕКО, 2000. – 512 с.



*Кузнецов О.О.,*
*доктор технічних наук, професор,*
*Харківський національний університет радіоелектроніки*

*Рябуха Ю.М.,*
*кандидат технічних наук,*
*Харківський університет Повітряних Сил імені І.Кожедуба*

*Колованова Е.П.,*
*Харківський національний університет радіоелектроніки*


## ДОСЛІДЖЕННЯ СУЧАСНИХ РЕЖИМІВ БЛОКОВОГО СИМЕТРИЧНОГО ШИФРУВАННЯ

Під режимом шифрування зазвичай розуміється такий метод застосування блокового симетричного шифру, який дає змогу реалізувати перетворення послідовності блоків відкритих даних на послідовність блоків зашифрованих даних із отриманням певних, наперед визначених криптографічних властивостей. Отримуваний рівень безпеки при криптографічному перетворенні залежить не тільки від властивостей застосовуваного шифру, але й від способів його використання, тобто властивості криптографічного перетворення

безпосередньо залежать від режиму застосування блокового симетричного шифрування [1–4].

Проаналізувавши сучасні режими застосування блокових симетричних шифрів, зокрема режими, стандартизовані міжнародними організаціями зі стандартизації (ISO/IEC) і відповідними національними організаціями США та РФ, обґрунтуємо вибір режимів застосування блокового симетричного шифрування, що можуть бути застосовані як національний стандарт України.

Після ухвалення нового стандарту шифрування FIPS-197 Національним інститутом стандартів і технологій США (NIST) було оголошено про пошук і розгляд нових і більш ефективних режимів шифрування [4]. За результатами аналізу особливостей побудови різних режимів та ретельних досліджень і оцінки їх криптографічних властивостей в окремому стандарті NIST Special Publication 800-38 специфіковано десять режимів застосування блокового симетричного шифру AES (допускається також застосування шифру TDEA). Перші чотири режими відповідають, із деякими варіаціями, чотирьом режимам, які визначено в чинному в Україні та розробленому ще у СРСР державному стандарті ГОСТ 28147-89 [1], а саме, режимам простої заміни, гамування, гамування зі зворотним зв’язком по шифротексту та режиму вироблення імітовставки. Міжнародний стандарт ISO/IEC 10116 дає специфікацію п’яти режимів [2; 3], а саме, ECB, CTR, CFB, CBC, OFB.

Аналіз показує, що на відміну від держстандарту ГОСТ 28147-89 та стандарту ISO/IEC 10116, сучасні режими застосування блокового симетричного шифрування, які специфіковані у NIST Special Publication 800-38, значно розширені. Пов’язано це передусім із виникненням нових потреб при застосуванні механізмів криптографічного захисту інформації у різних галузях (додатках), зокрема у телекомунікаційних протоколах при забезпеченні цілісності та конфіденційності інформації, захисті інформації на носіях даних, забезпечення безпеки ключових даних тощо.

## ЛІТЕРАТУРА

1. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – М. : Изд-во стандартов, 1989. – 20 с.

2. ГОСТ Р ИСО/МЭК 10116-93. Информационная технология. Режимы работы для алгоритма n-разрядного блочного шифрования [Електронний ресурс]. – Режим доступу : http://docload.spb.ru/Pages_gost/19004.htm.

3. ISO/IEC 10116. Information technology – Security techniques –

Modes of operation for an n-bit block cipher [Електронний ресурс]. – Режим доступу : http://www.iso.org.

4. NIST Special Publication 800-38D. Block Cipher Modes [Електронний ресурс]. – Режим доступу : http://csrc.nist.gov.

*Куцій М.С.,*
*Національна академія Служби безпеки України*

*Гринь А.К.,*
*кандидат технічних наук, доцент,*
*Національна академія Служби безпеки України*

## ВИКОРИСТАННЯ СИНЕРГЕТИЧНОГО ПІДХОДУ В МОДЕЛЮВАННІ СИСТЕМ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ СЕРЕДНЬОГО БІЗНЕСУ

Інформаційно-комунікаційні (ІТ) технології виступають одним із найважливіших факторів, що впливають на формування суспільства двадцять першого століття. Розвиток і темпи впровадження новітніх ІТ-технологій, глобальної комунікаційної мережі зумовлюють нові можливості автоматизації різних сфер людської діяльності, включаючи так звані *е*-сервіси: “електронний банкінг”; “електронна комерція”; “електронна звітність”; “електронна освіта”; “електронний уряд”; “електронне голосування”; “електронна держава”.

Відповідно, розширюється спектр можливих реалізацій загроз безпеці інформації, а в повсякденний обіг достатньо широкого кола фахівців входять такі нові поняття, як “кіберпростір”, “критична кібернетична інфраструктура”, “кіберзлочинність”, “кібернетична безпека”, “стратегія кібернетичної безпеки”, “система кібернетичної безпеки” та інші. Безумовно, мова йде про категорії загальної теорії інформаційної безпеки, об’єктом яких є ІТ-технології, що мають відношення до інтересів особи, суспільства, держави та міжнародних відносин.

У зв’язку з цим актуальне не лише питання створення ефективної міжнародної та державної системи кібернетичної безпеки, а і їх складових, наприклад, системи кібернетичної безпеки суб’єктів середнього бізнесу.

Реалії сьогодення визначають як один із чинників формування адекватної системи протидії кібернетичним загрозам суб’єктів сере-

днього бізнесу стан готовності їх управлінської команди до переорієнтації мислення персоналу в напрямі трансформації й інтеграції основних і спеціальних функцій менеджменту підприємства. Мова йде про особливості управління персоналом при застосуванні процесного підходу до управління інформаційною безпекою [1] суб'єктів середнього бізнесу, включаючи аудит стану кібернетичної безпеки, управління комп'ютерними інцидентами, кризис-менеджмент, забезпечення неперервності бізнесу тощо.

З*вернімо увагу на фінансово-економічні характеристики процесного підходу до забезпечення інформаційної безпеки в рамках заходів управління ризиками кібернетичної безпеки (управління комп'ютерними інцидентами)*.

Слід зазначити, що поняття "синергія" [3] та "синергетичний ефект" [2] в сучасній економічній теорії асоціюються із діями щодо злиття взаємоузгоджених економічних стратегій з метою створення єдиної корисної економічної системи. При цьому теорія і практика економічної діяльності свідчить, що в разі досягнення синергетичного ефекту, сумарна віддача від інтеграції економічних стратегій значно вища, ніж сума відповідних показників їх окремого використання [4].

У загальному випадку синергетика – це міждисциплінарний напрям, що досліджує процеси самоорганізації складних систем, яким характерні такі властивості, як відкритість, несталість і нелінійна динаміка розвитку. Синергетичний підхід до управління економічними системами, на відміну від кібернетичного підходу, як визначальну умову передбачає забезпечення оптимальної поведінки складних систем, наявність нерівновагових станів і процесів самоорганізації.

Натомість з погляду кібернетики процес управління складними системами становить впливи системи управління на підсистеми, що управляються. При цьому метою зазначених впливів є досягнення оптимального функціонування об'єкта в цілому. Оптимальне управління настає за умови, що система знаходиться в сталому стані гомеостатичної рівноваги, і саме в цьому стані вона досягає максимуму своєї ефективності.

Звісно, що у загальному випадку кіберпростір та економічні системи – це відкриті системи, а процес їх управління несталий і має нелінійну динаміку. Водночас, цей загальний випадок відповідає специфіці суб'єктів середнього бізнесу.

Синергетичний підхід (синергетичні ефекти) в контексті побудови системи протидії кібернетичним загрозам становить інтерес, насамперед, із точки зору завдань організації (самоорганізації) ефе-

ктивної інформаційно-економічної діяльності, що зумовлює можливі економічні наслідки господарської діяльності в умовах успішного ведення потенційним противником кібернетичних атак, можливості управління цими економічними наслідками (економічними ризиками) тощо. Тобто мова йде про пріоритет адміністративно-економічних важелів господарської діяльності, направлених на зменшення можливих економічних наслідків реалізації загроз критичній кібернетичній інфраструктурі суб'єктів середнього бізнесу, порівняно з "нарощенням" системи захисту інформації. І цей пріоритет є одним із чинників реалізації загальноприйнятої стратегії підвищення ролі заходів попередження кібернетичних загроз порівняно із заходами виявлення та реагування, тобто безпосередньо *належить до заходів профілактики правопорушень у кіберпросторі* [4].

Специфіка суб'єктів середнього бізнесу в завданнях забезпечення кібернетичної безпеки полягає в тому, що саме для цієї категорії можливих об'єктів кіберзлочинності, питання економічної ефективності засобів і заходів захисту інформації з обмеженим доступом та відкритої інформації (критичної до загроз порушення цілісності, авторства та доступності) є найбільш вагомим. Зумовлено це тим, що для суб'єктів середнього бізнесу, завдання побудови ефективної системи захисту критичної кібернетичної інфраструктури достатньо проблематичне, оскільки утримання значного штату спеціалістів, які б охопили широке коло питань розроблення, виробництва, впровадження, експлуатації засобів і заходів захисту інформації, управління інформаційною безпекою зокрема, є економічно невигідним. Як наслідок, більшість суб'єктів середнього бізнесу, як правило, користуються загальнодоступними в мережі Інтернет (безкоштовними) засобами і послугами захисту інформації, ефективність яких з точки зору комплексного підходу до захисту інформації викликає певні сумніви.

Таким чином, *синергетичний підхід у моделюванні систем кібернетичної безпеки середнього бізнесу доцільно використовувати як складову процесів управління інформаційною безпекою*, насамперед, що стосується моделювання загроз/порушника, формування політик безпеки та визначення ефективності системи захисту критичної кібернетичної інфраструктури. Використання синергетики сприяє виникненню додаткового корисного ефекту заходів кризисменеджменту та забезпечення неперервності бізнесу, що *має на меті зменшення загроз кібернетичних атак шляхом зниження в потенційного порушника мотивації щодо їх здійснення*.

Запропонований підхід економічних заходів кібернетичної безпеки суб'єктів середнього бізнесу може бути узагальнений і на інші суб'єкти господарської діяльності.

## ЛІТЕРАТУРА

1. Міжнародні стандарти "Управління інформаційною безпекою" серії ISO/IEC 27000.

2. Кемпбелл Э. Стратегический синергизм / Э. Кемпбелл, Кетлин Саммерс Лачс. – СПб. : Питер, 2004. – 416 с.

3. Ансофф И. Стратегическое управление / Ансофф И. – М., 1989. – С. 152.

4. Securing the payment environment to protect card data and render it useless in the hands of criminals/ [Електронний ресурс]. – Режим доступу : http://corporate.visa.com/ index. shtml.

*Ланде Д.В.,*
*доктор технічних наук,*
*ІПРІ НАН України, НДІІП НАПрН України*

## ЛІНІЇ ТРЕНДІВ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ ТА ЇХ ВІДОБРАЖЕННЯ В ІНФОРМАЦІЙНОМУ ПРОСТОРІ

Інформаційні операції визначаються як акції, спрямовані на вплив на інформацію та інформаційні системи противника, захист власної інформації та інформаційних систем [1]. Прояви інформаційних операцій фіксуються в багатьох сферах – військовій, соціальній, економічній. Інформаційні операції на сьогодні безпосередньо пов'язані з впливом на людей, маніпулюванням. Серед потенційних загроз в інформаційній сфері в Законі України "Про основи національної безпеки України" від 19 червня 2003 року № 964-IV (стаття 7) окремо відзначаються ризики інформаційних впливів: "... прагнення маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації".

"Тренд" (від англ. trend), як відомо, – це тривала, довгочасна тенденція зміни економічних показників в економічному прогнозуванні. Ми будемо обговорювати тренди, які притаманні публікаціям

в мережевих інформаційних ресурсах, що супроводжують інформаційні операції. Обговорення базується на дослідженні взаємозв'язку реальних подій і публікацій щодо них у веб-мережі.

Сучасний інформаційний простір – це унікальна можливість отримання будь-якої інформації по обраному питанню, за умови наявності відповідного інструментарію, застосування якого дає змогу аналізувати взаємозв'язок можливих подій або подій, які вже відбуваються, з інформаційною активністю визначеного кола джерел інформації.

Для дослідження взаємозв'язку реальних подій і публікацій про них в інтернеті використовувалася система InfoStream, що забезпечує інтеграцію та моніторинг мережевих інформаційних ресурсів [2].

Кількість веб-публікацій у день по якій-небудь темі, а особливо зміни (динаміка) цієї величини, часом дозволяють навіть недосвідченим фахівцям у предметній сфері робити більш-менш точні висновки.

Тренди повідомлень [1], що відповідають діям інформаційної операції, наведено на рис. 1. Як відомо, у плані профілактики інформаційних операцій варто уважно стежити за динамікою публікацій про цільову компанію, якщо є можливість, з урахуванням тональності цих публікацій, користуватися доступними аналітичними засобами, наприклад, вейвлет-аналізом або поліноми Кунченка [2]. При цьому варто орієнтуватися на можливі моделі інформаційних атак, наприклад, якщо ця модель охоплює фази: "фон" – "затишок" – "артпідготовка" – "затишшя" – "атака", то вже за першими трьома компонентами можна з великою ймовірністю передбачити майбутні події.

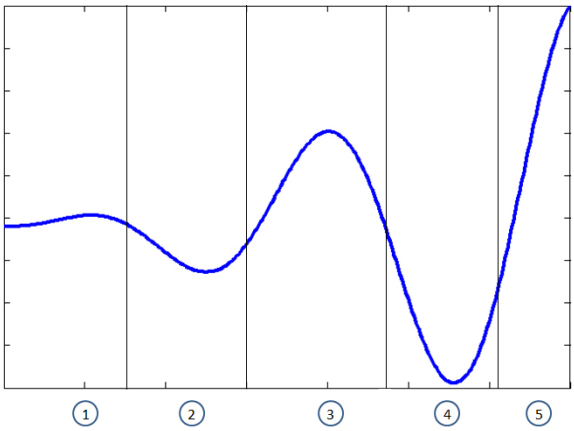



Рис. 1. Динаміка кількості тематичних повідомлень
під час проведення інформаційних операцій:
1 – фон; 2 – затишшя; 3 – "артпідготовка"; 4 – затишшя;
5 – атака/тригер зростання

Як відомо, інноваційна діяльність наразі також вимірюється через кількість публікацій щодо інновацій. Водночас упровадження інновацій інколи можна уважати інформаційними операціями. Уважніше розглянемо результати відповідних досліджень більш детально. На рис. 2 наведена обґрунтована діаграма кількості публікацій, що відповідає тренду інноваційної діяльності [4].

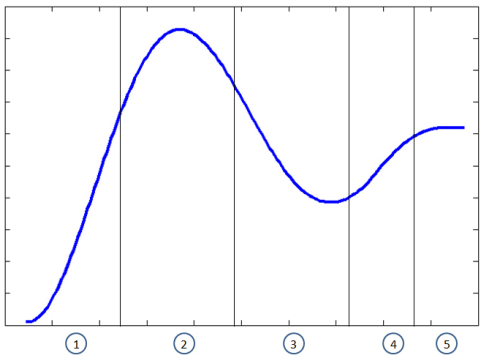



Рис. 2. Діаграма кількості публікацій, що відповідають тренду інноваційної діяльності:
1 – атака/тригер зростання; 2 – пік завищених очікувань;
3 – втрата ілюзій; 4 – суспільне усвідомлення;
5 – продуктивність/фон

Поєднуючи графіки, що відповідають початку інформаційної операції (рис. 3) та тренду інноваційної діяльності (рис. 4), можна отримати повний графік, що відповідає відображенню інформаційних операцій в інформаційному середовищі (рис. 5).

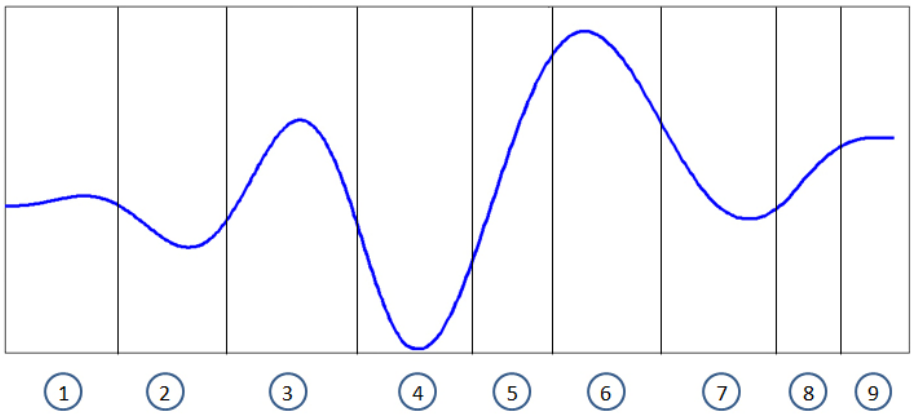



Рис. 3. Узагальнена діаграма кількості публікацій, що відповідають усім етапам життєвого циклу інформаційних операцій:
1 – фон; 2 – затишшя; 3 – “артпідготовка”; 4 – затишшя;
5 – атака/тригер зростання; 6 – пік завищених очікувань;
7 – втрата ілюзій; 8 – суспільне усвідомлення;
9 – продуктивність/фон

Запропоновані моделі цілком відповідають реальним даним, що отримуються із систем контент-моніторингу, що підтверджуються чисельними публікаціями автора [1]. Наведені залежності можуть бути використані як шаблони для виявлення інформаційних операцій, як шляхом аналізу ретроспективного фонду мережевих публікацій, так і для оперативного моніторингу появи деяких їх ознак у реальному часі.

Разом із тим, більш реалістичні моделі можуть бути отримані з урахуванням додаткового набору факторів, більшість яких не відтворюються в часі. Відзначимо, що відтворення результатів у часі є самою серйозною проблемою при моделюванні інформаційних процесів, зокрема, інформаційних операцій. На цей час лише ретроспективний аналіз вже реалізованих інформаційних операцій є відносно надійним способом верифікації результатів.

## ЛІТЕРАТУРА

1. Горбулін В.П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія / В.П.Горбулін, О.Г.Додонов, Д.В.Ланде. – К. : Інтертехнологія, 2009. – 164 с.

2. Григорьев А.Н. Мониторинг новостей из Интернет: технология, система, сервис : научно-методическое пособие / А.Н.Григорьев, Д.В.Ландэ и др. – К. : ООО “Старт-98”, 2007. – 40 с.

3. Поліноми Кунченка для розпізнавання образів / О.Р.Чертов // Вісник НТУУ “КПІ” Інформатика, управління та обчислювальна техніка. – 2009. – № 50. – С. 105–110.

4. Хорошевский В.Ф. Семантические технологии: ожидания и тренды / В.Ф.Хорошевский // Открытые семантические технологии проектирования интеллектуальных систем – Open Semantic Technologies for Intelligent Systems (OSTIS-2012) : материалы II Междунар. научн.-техн. конф. (Минск, 16–18 февраля 2012 г.). – Минск : БГУИР, 2012. – С. 143–158.

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

*Кащук В.І.,*
*Національна академія Служби безпеки України*

# АКТУАЛЬНІ НАПРЯМИ ПОПЕРЕДЖЕННЯ ПРАВОПОРУШЕНЬ У КІБЕРПРОСТОРІ ЯК СКЛАДОВА СТРАТЕГІЇ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ДЕРЖАВИ

Сучасний етап розвитку людства справедливо вважається епохою розбудови інформаційного суспільства на глобальному, національному, регіональному та інших рівнях. І одним із базових процесів його розбудови є інформатизація, а її рівень безпосередньо впливає як на розвиток різних сфер людської діяльності, так і на реалії щодо викликів і загроз інформаційній безпеці і насамперед у кіберпросторі, оскільки процес інформатизації формує кіберпростір.

Звісно, темпи інформатизації в Україні не такі як в країнах західної Європи та Сполучених штатах Америки, і це стосується, насамперед, кількості та масштабності вітчизняних об'єктів критичної інфраструктури в кіберпросторі, а що ж стосується присутності фізичних і юридичних осіб України у кіберпросторі, то мобільний зв'язок, відповідно, і мобільний Інтернет є вже практично у всіх населених пунктах країни, при цьому кількість абонентів постійно зростає.

Цей факт має певні плюси, бо ми на прикладі інших країн бачимо, що можна очікувати у найближчому майбутньому, а також маємо змогу аналізувати іноземний довід щодо побудови загальнодержавних систем забезпечення кібернетичної безпеки та конкретних заходів щодо її реалізації. Відповідно, є можливості для оцінювання ефективності вже реалізованих в інших країнах заходів кібернетичної безпеки, щоб визначитися з питанням – які ініціативи доцільно впроваджувати та розвивати, а від яких можливо доцільно і відмовитись.

На наш погляд, поняття кібернетичної безпеки є складовою частиною поняття інформаційної безпеки, оскільки суть загроз, методів, засобів і заходів однакова та обмежується лише кіберпростором. Однак кіберпростір, незалежно від існуючих підходів до його визначення, унікальне явище, що не має державних кордонів та об'єднує в собі такі складові, як: інформаційний простір, інформаційні ресурси, інформаційну інфраструктуру та інформаційні технології. Відповідно, кібернетична безпека, на відміну від інформаційної безпеки, не є лише невід'ємною складовою кожної зі сфер наці-

ональної безпеки та водночас самостійною сферою забезпечення національної безпеки (як зазначено у доктрині інформаційної безпеки України), а також додатково виступає самостійною сферою забезпечення міжнародної безпеки, безпеки громадян і бізнесу у кіберпросторі.

Таким чином, питання кібернетичної безпеки мають особливу специфіку у сфері інформаційної безпеки та потребують окремого законодавчого урегулювання, що і підтверджується більшістю випадків міжнародної практики.

Далі хотілося б звернути увагу на те, що в умовах, коли Кабінет Міністрів України схвалив законопроект "Про внесення змін до Закону України "Про основи національної безпеки України"щодо кібернетичної безпеки України", на наш погляд, доцільно розробити окремий законодавчий акт "Стратегія кібернетичної безпеки України". Цей документ повинен визначати цілі, основні принципи, підходи та заходи щодо діяльності загальнодержавної системи забезпечення кібернетичної безпеки України з метою забезпечення кібернетичного захисту в інтересах громадян, суспільства, держави та міжнародного правопорядку. При цьому Стратегія повинна визначати послідовність конкретних напрямів діяльності із попередження, виявлення та реагування на комп'ютерні інциденти, заходи протидії правопорушенням, які необхідно застосовувати для досягнення оптимального рівня захищеності кіберпростору.

На сьогодні є всі підстави вважати, що до найпоширеніших небезпек у кіберпросторі, які можуть мати транснаціональний характер, можна віднести правопорушення в кредитно-фінансовій сфері, телефонні шахрайства, шпіонаж, захоплення "комп'ютерного ресурсу" (у тому числі і створення бот-мереж), порушення авторського права та суміжних прав, поширення незаконного контенту, використання кіберпростору для розповсюдження наркотиків, торгівлі людьми та людськими органами і т. ін. Основним об'єктом яких є, як-правило, прості громадяни. Відповідно, завдання попередження зазначених правопорушень, на наш погляд, одне із найактуальніших для України.

У загальному випадку, під попередженням правопорушень можна розуміти сукупність стратегій і заходів, що використовуються для зниження ризику скоєння правопорушень, нейтралізації або зменшення їх наслідків. В свою чергу, до основних напрямів формування таких стратегій можна віднести такі позиції.

1. Зниження мотивації до скоєння правопорушень у кіберпросторі за рахунок підвищення рівня захисту інформаційних ресурсів та інформаційної інфраструктури (ІТ-технологій), шляхом створення умов для:

– розвитку ринку засобів і послуг із технічного та криптографічного захисту інформації, управління інформаційною безпекою

ІТ-технологій, доступності та зрозумілості цих засобів і послуг для широкого кола суб'єктів підприємницької діяльності та простих громадян;

– формування культури інформаційної безпеки у широких верст населення, охоплюючи технологічні, соціально-психологічні, економічні та правові питання.

2. Зниження мотивації до скоєння правопорушень у кіберпросторі за рахунок підвищення ефективності правоохоронної діяльності у сфері кібернетичної безпеки, шляхом створення умов для:

– розвитку технологічної складової національної та міжнародної системи виявлення, дослідження та реагування на комп'ютерні інциденти;

– підвищення ефективності діяльності правоохоронної системи у цій сфері.

Звісно, кожен із цих напрямів є також комплексною проблемою та потребує окремого обговорення.

## ЛІТЕРАТУРА

1. Актуальні проблеми управління інформаційною безпекою держави : зб. матер. наук.-практ. конф., 22 березня 2011 р. : у 2 ч. – К. : Наук.-вид. відділ НА СБ України, 2011. – Ч. 2. – 107 с.

2. Актуальні питання підготовки фахівців із розслідування кіберзлочинів : зб. матер. круглого столу, 25 листопада 2011 р., м. Київ. – К. : Наук.-вид. відділ НА СБ України, 2012. – 121 с.

*Мисюк Ю. П.,*
*кандидат технічних наук,*
*старший науковий співробітник,*
*Науково-дослідний інститут*
*Державної прикордонної служби України*

## ВИЗНАЧЕННЯ ПІДХОДІВ ЩОДО ЗАХИСТУ ІНФОРМАЦІЇ ПІД ЧАС ОРГАНІЗАЦІЇ СЛУЖБИ ПРИКОРДОННИХ НАРЯДІВ

Забезпечення недоторканності кордонів належить до пріоритетних національних інтересів. Запобігання спробам порушення державного кордону і територіальної цілісності виступає одним із найважливіших напрямів державної політики у сфері прикордонної безпеки [1]. В умовах ресурсних обмежень держави посилюються вимоги до інформації про майбутні дії наявних сил та засобів на

державному кордоні, яка за умовою її несанкціонованого витоку може бути використана правопорушниками для реалізації їх злочинних намірів.

Розглянемо існуючі підходи щодо захисту інформації під час організації служби прикордонних нарядів на державному кордоні.

Відповідно до Закону України "Про Державну прикордонну службу України" її головним завданням є забезпечення недоторканності державного кордону [1]. Згідно наданих повноважень органи та підрозділи прикордонного відомства зобов'язані припиняти будь-які спроби незаконного перетинання кордону; забезпечувати виконання зобов'язань, що виникають із міжнародних договорів; здійснювати спільні заходи із суб'єктами інтегрованого управління кордонами тощо.

Після прийняття Концепції інтегрованого управління кордонами значно посилились вимоги до інформаційної складової системи інтегрованого управління кордонами [2; 3]. Це зумовлено необхідністю збирання, добування та оброблення даних обстановки на державному кордоні для забезпечення служби прикордонних нарядів випереджувальною інформацією про можливий розвиток протиправної діяльності. Успіх реалізації зазначеної інформації повністю залежить від відсутності каналів її витоку.

З іншого боку, одним із завдань Кодексу України про адміністративні правопорушення є вжиття заходів, спрямованих на запобігання адміністративним правопорушенням, виявлення й усунення причин та умов, які сприяють їх вчиненню, виховання громадян у дусі високої свідомості і дисципліни, суворого додержання законів України [4], що передбачає проведення комплексу гласних профілактичних заходів з мешканцями прикордоння, промисловими та громадськими організаціями тощо.

Зазначені особливості зумовлюють два основних варіанти несення служби прикордонними нарядами: приховані дії для реалізації випереджувальної та оперативної інформації про можливу протиправну діяльність на державному кордоні та демонстративні дії з метою профілактики протиправної діяльності. Обидва способи висувають різні вимоги до захисту інформації про організацію служби прикордонних нарядів на державному кордоні.

Під час реалізації випереджувальної та оперативної інформації про можливу протиправну діяльність на державному кордоні необхідно усунути можливі канали витоку задуму використання наявних сил та засобів для припинення правопорушення. При цьому важливими елементами є захист інформації про організаційні, планувальні майбутні дії, заходи з координації зусиль суб'єктів інтегрованого

управління кордонами та переважне використання пасивних технічних засобів охорони державного кордону (тепловізійні установки, сигнальні міни, сенсори тощо) для унеможливлення дистанційного демаскування системи охорони державного кордону. Також важливим питанням можна вважати і організацію радіозв'язку з прикордонними нарядами.

У процесі проведення демонстративних дій із профілактики протиправної діяльності, демонстрації присутності на державному кордоні представників правоохоронних органів виникають завдання поширення інформації про майбутні та реальні дії наявних сил та засобів на державному кордоні. Зважаючи на окремі факти виявлення у затриманих правопорушників технічних засобів, які можуть бути використані для демаскування системи охорони державного кордону (прилади нічного бачення, радіочастотні сканери тощо), бажане максимальне використання активних технічних засобів охорони державного кордону (наприклад, радіолокаційні, прожекторні станції тощо). Їх використання дає змогу розширити район, на якому одночасно можна провести демонстраційні профілактичні заходи.

Зважаючи на зазначене, під час прийняття управлінських рішень, розроблення телекомунікаційних систем в інтересах охорони державного кордону доцільно враховувати зміст заходів, які планується провести на державному кордоні (реалізація випереджувальної та оперативної інформації або демонстративні дії). Також в системі інтегрованого управління кордонами необхідно вживати додаткові заходи щодо координації діяльності суб'єктів інтегрованого управління кордонами у сфері інформаційної безпеки.

Напрямом подальших розвідок може бути дослідження механізмів державного управління в системі інтегрованого управління кордонами щодо удосконалення інформаційної безпеки у прикордонній сфері.

## ЛІТЕРАТУРА

1. Про Державну прикордонну службу України : Закон України від 03.04.2003 № 661-IV [Електронний ресурс]. – Режим доступу : http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=661-15.

2. Литвин М.М. Інтегроване управління кордонами : підручник / М. М. Литвин. – Хмельницький : Вид-во НАДПСУ, 2012. – 416 с.

3. Хруст Д.В. Основні напрямки забезпечення подальшого впровадження в практику охорони державного кордону сучасних прикордонних технологій / Д. В. Хруст // Науковий вісник Державної прикордонної служби. – 2009. – № 49. – С. 51-53.

4. Кодекс України про адміністративні правопорушення [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/80731-10/page1.

*Муратов О.Є.,*
*кандидат технічних наук,*
*старший науковий співробітник,*
*Національна академія Служби безпеки України*

# ТЕОРЕТИКО-ІГРОВЕ БАЧЕННЯ ВИЗНАЧЕННЯ ЦІННОСТІ ІНФОРМАЦІЇ

Домінуючою методологією у вирішенні питання про цінність інформації нині можна вважати оцінку ризиків. У сукупності зі сценарним підходом вона стає достатньою для забезпечення прийняття практично будь-якого сучасного управлінського рішення. В той же час багато питань при цьому залишається у "тіні авторитету" експертів, які обґрунтовували рішення. Для підвищення рівня об'єктивності аргументації у процесі вибору альтернатив під час прийняття рішень доцільно здійснити перехід від суто експертних до експертно-аналітичних методів при вирішенні ключових завдань вказаного підходу [1]. З цією метою в статті представлено узагальнену модель набуття інформацією цінності для суб'єкта, який отримує цю інформацію, а також заявлена можливість її використання для оцінювання наслідків для суб'єкта від втрати інформацією конфіденційності (розповсюдження інформації), проте формального опису такого оцінювання представлено не було [2].

При розгляді моделі набуття інформацією цінності [2] було зроблено припущення про те, що цінність інформації для суб'єкта визначається через ступінь зумовлення нею його наступної активності, результат якої визначатиметься інформацією, накопиченою суб'єктом про середовище, та інформацією, накопиченою середовищем про суб'єкта. Найкращим результатом вважатиметься такий, при якому наступний стан системи суб'єкт-середовище збігатиметься зі станом, якого очікував суб'єкт. Так, зміну в результаті активності суб'єкта можна представити наступним чином:

$$\Delta R_s(\Delta I) = R_s(I_{e_0}) - R_s(I_{e_0} + \Delta I), \qquad (1)$$

де $R_s(I_{e_0})$ – результат активності суб'єкта за умови неотримання середовищем інформації $\Delta I$; $R_s(I_{e_0} + \Delta I)$ – результат активності суб'єкта за умови отримання середовищем інформації $\Delta I$; $I_{e_0}$ – інформація, отримана середовищем, без врахування інформації $\Delta I$.

Фактичний результат обчислення $\Delta R_s(\Delta I)$ за формулою (1) може бути спостереженим і оціненим на підставі цього спостереження тільки після зміни стану середовища, тобто у наступний момент часу, у майбутньому. Основний практичний інтерес полягає у можливості його оцінювання у теперішньому, без очікування наступного моменту часу.

У загальному випадку такий прогноз може бути точним за умови, що суб'єкт знає закони зміни стану середовища, йому відомі всі необхідні його параметри та їх значення. Однак це є дуже складним і зазвичай існує невизначеність стосовно цих даних, яка зумовлює похибку між прогнозованим результатом та результатом, фактично спостереженим у майбутньому.

Для подальшого з'ясування залежності між мірою невизначеності та величиною похибки можна скористатися теорією ігор [3, 4]. Положення цієї теорії нині застосовується під час розгляду питань інформаційної безпеки [5, 6].

Теорія ігор надає можливість враховувати вплив поінформованості учасників на результат гри. Така поінформованість подається як знання гравців про стратегії інших учасників та їх вибори, виконаних на всіх ходах, що передують теперішньому моменту гри.

Якщо припустити, що гра Г може бути реалізованою будь-якою партією з множини $\Omega$, що кількість учасників задано і дорівнює $n$, що їх стратегії є відомими та незмінними, що задана функція виграшу $F_k$ для кожного з учасників $k = 1,...,n$, то ймовірність виграшу учасника $k$ після отримання повідомлення $M_e$ учасником $e$ змінюватиметься таким чином:

$$\Delta P_k(M_k) = \frac{E_{2k}}{|\Omega_{2e}|} - \frac{E_{1k}}{|\Omega|} = P_{2k} - P_{1k}, \qquad (2)$$

де $\Omega_{2e}$ – множина, до якої зменшиться множина $\Omega$ внаслідок зміни поінформованості учасника $e$; $|\Omega_{2e}|$ и $|\Omega|$ – кількість всіх можливих партій в $\Omega_{2e}$ та $\Omega$ відповідно; $E_{1k}$ – кількість приємних результатів для учасника $k$ у всіх можливих партіях із $\Omega$ у випадку, коли повідомлення $M_e$ не отримано; $E_{2k}$ – кількість приємних результатів для учасника $k$ у всіх можливих партіях із $\Omega_{2e}$ у випадку, коли повідомлення $M_e$ отримано учасником $e$.

Як можна побачити, формула (2) реалізує відоме уявлення цінності інформації за О.Харкевичем, що визначається як зміна ймовірності досягнення цілі у випадках отримання та неотримання інформації [1].

Слід зазначити, що отримання будь-яких повідомлень про хід партії її учасниками встановлюється правилами гри. В реальності може статися обмін повідомленнями поміж гравцями, яких не передбачено правилами гри. Якщо один із гравців одержує інформацію, про можливість одержання якої іншим гравцям нічого не відомо (виходячи з правил гри), в такому разі необхідно говорити про те, що гравці грають за різними правилами гри.

Незважаючи на простоту формули (2) оцінювання цінності інформації за його використанням на практиці часто стає складним завданням у зв'язку з необхідністю визначення всіх елементів множини $\Omega$, розміри якого часто надзвичайно великі.

Наведена математична ігрова модель взаємодії середовища та суб'єкта не суперечить існуючим уявленням про цінність інформації в процесі прийняття рішення. Незважаючи на складність практичного застосування, така модель дає достатньо повне уявлення про розміри завданої шкоди поширенням інформації. Вона може стати теоретичною основою для наукового супроводження питань про доцільність приховування відомостей, проведення дезінформування чи PR-компаній. Теоретико-ігрове бачення взаємодії середовища та суб'єкта може бути використане у навчальному процесі із метою пояснення сутності зазначених явищ, а також як альтернатива домінуючому нині сценарному підходу моделювання розвитку подій для прийняття управлінських рішень.

## ЛІТЕРАТУРА

1. Архипов О.Є. Критерії визначення можливої шкоди національній безпеці України у разі розголошення інформації,що охороняється державою: моногр. / О.Є.Архипов, О.Є.Муратов. – К. : Наук.-вид. відділ Національної академії Служби безпеки України, 2011. – 195 с.

2. Муратов А.Е. К вопросу о механизме приобретения ценности субъективной информации в задачах обеспечения безопасности / А.Е.Муратов // Захист інформації. – № 4(53). – 2011. – С. 40-45.

3. Мулен Э. Теория игр с примерами из математической экономики / Э.Мулен ; пер. с франц. – М. : Мир, 1985. – 200 с.

4. Петросян Л.А. Теория игр : учеб. пособ. для ун-тов / Л.А.Петросян, Н.А.Зенкевич, Е.А.Семина. – М. : Высш. шк., Книжный дом "Университет", 1998. – 304 с.

5. Чхартишвили А.Г. Теоретико-игровые модели информационного управления / А.Г.Чхартишвили. – М. : ЗАО "ПМСОФТ", 2004. – 227 с.

6. Козюра В.Д. Выбор момента времени для проведения операции воздействия на информацию / В.Д.Козюра, И.В.Пискун, В.А.Хорошко // Інформаційна безпека людини, суспільства, держави. – 2011. – №2(6). – С. 76-82.

*Пермяков О.Ю.,*
*доктор технічних наук, професор,*
*Національний університет оборони України*

*Варламов І.Д.,*
*кандидат технічних наук,*
*Національний університет оборони України*

*Ляшенко І.О.,*
*кандидат військових наук,*
*Національний університет оборони України*

# МЕТОДОЛОГІЧНІ АСПЕКТИ ЗАХИСТУ ІНФОРМАЦІЇ В ЄДИНІЙ АВТОМАТИЗОВАНІЙ СИСТЕМІ УПРАВЛІННЯ СЕКТОРОМ БЕЗПЕКИ Й ОБОРОНИ УКРАЇНИ

На сучасному етапі розвитку України проводиться реформування сектора безпеки і оборони як цілісної системи [1]. Особливості сектора безпеки і оборони нашої держави, як інструменту протидії всьому спектру внутрішніх і зовнішніх загроз, визначають необхідність створення єдиної автоматизованої системи управління цим сектором.

Така система гарантовано буде об’єктом кібернападу з метою несанкціонованого експорту даних, їх зміни або дезорганізації функціонування. Крім того, необхідно зазначити, що розвиток міжнародного права щодо кіберпростору, ймовірно, не забезпечить об’єктам сектору безпеки і оборони захист від кібернападу.

Історично програмне забезпечення кібернападу прийнято називати мелвером [2], тому пропонується ввести термін мелвер-захист для чіткого виокремлення з широкого спектру аспектів інформаційної боротьби (інформаційно-психологічна війна, публічна дипломатія та ін.) саме захисту від небажаного впливу за допомогою програм. Хоча кожен вид інформаційної боротьби прямо чи опосередковано може впливати на сектор безпеки і оборони, однак саме програмний вплив може бути найсуттєвішим та призвести до катастрофічних наслідків. Таким чином, під мелвер-захистом будемо розуміти захист від небезпечних програм, які змушують окремі комп’ютери або комп’ютерні сеті робити небажані для власників та користувачів дії. Прикладами таких програм є логічні бомби, черваки, віруси, фішинги, сніфери пакетів, регістратори клавіатури та ін. Для характеристики захищеності від шкідливих програм доцільно ввести термін мелвер-безпека.

Аналіз доступних матеріалів політики та технології інформаційної боротьби показав, що захист єдиної автоматизованої системі управління сектором безпеки і оборони повинен бути всебічно узгодженим, розвинутим та у вищій мірі визначеним [3, 4].

Особливості єдиної автоматизованої системи управління сектором безпеки і оборони України визначають його як складний об'єкт захисту. Тому пропонується забезпечити функціонування Центрального органу захисту, якій має достатній досвід та заслуговує на довіру. Цей орган повинен реалізовувати низку організаційно-технічних заходів, зокрема: вирішення завдання контролю за виконанням правил захисту; надання експертних оцінок щодо рівня безпеки; проведення розслідування щодо шляхів потрапляння мелверів в єдине інформаційне поле системи управління; забезпечення процедури автентифікації відправника та отримувача інформації; проведення моніторингу комп'ютерних мереж у режимі реального часу.

На основі зазначеного вище автори вважають за необхідне наголосити на необхідність реалізації такого технічного аспекту, як проведення глибокого інспектування інформаційних пакетів на предмет виявлення шкідливих програм, не порушуючи при цьому принципу закритості інформації.

Технологія постійного сканування повинна бути реалізована для виявлення та попередження аномальної активності, вторгнення, крадіжок особистих ідентифікаторів та несанкціонованого експорту даних. В основі технології постійного сканування повинні бути відомі сигнатури шкідливих програм. Важливе значення має реалізація кількох способів автентифікації для надання доступу до систем. Безумовно, важливим є реалізація принципу суворої ізольованості, для цього необхідно використовувати канали, абсолютно не пов'язані з інтрамережами складових сектору безпеки і оборони та публічним Інтернетом.

У перспективі необхідно реалізовувати нові протоколи, які б давали змогу встановлювати, хто відсилає кожний пакет, надавати пакетам пріоритети та зашифровувати інформацію. Також необхідно реалізовувати нові способи автентифікації, удосконалені підходи до авторизації доступу, рівномірної шифровки трафіку та нерухомих даних.

Необхідно зазначити, що важливу роль у процесі захисту також відіграє організація оброблення інформації. Аналіз особливостей оброблення даних в єдиному інформаційному полі органу управління показав, що кількість інформаційних каналів, як правило, обмежена, а ступень ймовірності даних різна. В таких умовах пропонується використовувати синергетичні підходи до комплексного оброблення даних із кожного інформаційного каналу [5, 6].

Важливою особливістю синергетичного підходу в умовах підтримки єдиного інформаційного поля органу управління є використання дискримінаторів ступенів свободи. Що стосується редукторів ступенів свободи, то такий підхід може (скоріш за все буде) застосовуватися однак, як виняток. Крім того, включення механізмів дискримінаторів ступенів свободи дає змогу всім каналам отримання даних брати участь у формуванні рішення з вагами, які відповідають ступеню їх інформативності в поточній ситуації.

Таким чином, без реалізації зазначених вище організаційно-технічних заходів щодо захисту інформації в єдиній автоматизованій системі управління сектором безпеки і оборони України не можливо досягти успіху в протидії всьому спектру внутрішніх і зовнішніх загроз у сучасних умовах.

## ЛІТЕРАТУРА

1. Указ Президента України від 8 червня 2012 р. № 389 "Про рішення Ради національної безпеки і оборони України від 8 червня 2012 р. "Про нову редакцію Стратегії національної безпеки України" [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/389/2012.

2. Кларк Р.. Третья мировая война: какой она будет? / Р.Кларк, Р.Нейк. – СПб. : Питер, 2011. – 336 с.

3. Пермяков О.Ю. Інформаційні технології і сучасна збройна боротьба / О.Ю.Пермяков, А.І.Сбітнєв. – Луганськ : Знання, 2008. – 204 с.

4. Пермяков О.Ю. Напрями захисту єдиного інформаційного поля органів управління від мелвер-нападу / О.Ю.Пермяков, І.Д.Варламов // Матеріали постійно діючого наукового семінару кафедри застосування інформаційних технологій та інформаційної безпеки Інституту інформаційних технологій Національного університету оборони України, 15 листопада 2012 року. – К. : НУОУ, 2012. – С. 5-7.

5. Воронин А.Н. Многокритериальные решения: модели и методы : моногр. / А.Н.Воронин, Ю.К.Зиатдинов, М.В.Куклинский. – К. : НАУ, 2011. 348 с.

6. Пермяков О.Ю. Синергетичний підхід до підтримки єдиного інформаційного поля / О.Ю.Пермяков, В.А.Савченко, І.Д.Варламов // Матеріали постійно діючого наукового семінару кафедри застосування геоінформаційних технологій та космічних систем Інституту інформаційних технологій Національного університету оборони України 19 листопада 2012 року. – К. : НУОУ, 2012. – С. 27-35.

*Проскуровський Р.В.,*
*кандидат технічних наук,*
*Інститут спеціального зв'язку*
*та захисту інформації НТУУ "КПІ"*

*Бакута А.Ю.,*
*Інститут спеціального зв'язку*
*та захисту інформації НТУУ "КПІ"*

# МЕТОДИ ЗАХИСТУ ВІД DDoS-АТАК

Атака на відмову в обслуговуванні або розподілена атака на відмову в обслуговуванні (*DoS attack, DDoS attack, Distributed Denial-of-service attack*) – напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними для користувачів, для яких комп'ютерна система була призначена [1].

Одним із найпоширеніших методів нападу є насичення атакованого комп'ютера або мережевого устаткування великою кількістю зовнішніх запитів (часто спеціально сформульованих), через що атаковане устаткування не може відповісти користувачам, або відповідає настільки повільно, що стає фактично недоступним. Взагалі відмова сервісу здійснюється: примусом атакованого устаткування до зупинки роботи програмного забезпечення/устаткування або до витрат наявних ресурсів, унаслідок чого устаткування не може працювати; через зайнятість комунікаційних каналів між користувачами і атакованим устаткуванням, внаслідок чого якість сполучення не відповідає вимогам.

DoS-атаки поділяються на локальні та віддалені. До локальних належать різні експлойти: форк-бомби і програми, що відкривають по мільйону файлів або запускають якийсь циклічний алгоритм, який "з'їдає" пам'ять та процесорні ресурси. Для локальної DoS атаки необхідно мати, або якимось чином отримати доступ до атакованої машини на рівні, достатньому для захоплення ресурсів.

Розглянемо віддалені DoS-атаки. Вони поділяються на два види.

Віддалена експлуатація помилок у програмному забезпеченні (ПЗ) з метою довести його до неробочого стану.

Flood – посилка на адресу жертви величезної кількості безглуздих (рідше – осмислених) пакетів. Метою флуду може бути канал зв'язку або ресурси машини. У першому випадку потік пакетів займає весь пропускний канал і не дає машині, що атакується, можливості обробляти легальні запити. У другому – ресурси машини захоплюються за допомогою багаторазового і дуже частого звернення до

якого-небудь сервісу, що виконує складну, ресурсоємну операцію. Це може бути, наприклад, тривале звернення до одного з активних компонентів (скрипту) web-сервера. Сервер витрачає всі ресурси машини на оброблення запитів, що атакують, а користувачам доводиться чекати.

У традиційному виконанні (один атакувальний – одна жертва) нині залишається ефективним лише перший вид атак. Класичний флуд – даремний, оскільки за наявності сучасної ширини каналу серверів, рівня обчислювальних потужностей і поширеному використанні різних анти-DoS прийомів в ПЗ (наприклад, затримки при багаторазовому виконанні тих самих дій одним клієнтом), атакувальний перетворюється на "докучливого комара", не здатного завдати будь-якого збитку. Але якщо цих "комарів" наберуться сотні, тисячі або навіть сотні тисяч, вони легко "покладуть сервер на лопатки". Розподілена атака, так звана "відмова в обслуговуванні" (DDoS), зазвичай здійснювана за допомогою безлічі "зазомбованих" хостів, може відрізати від зовнішнього світу навіть найпотужніший сервер, і єдиним ефективним захистом при цьому є організація розподіленої системи серверів (кластера).

Назвемо два варіанти організації DDoS-атак:

– Ботнет – зараження певного числа комп'ютерів програмами, які в певний момент починають здійснювати запити до атакованого сервера.

– Флешмоб – домовленість великої кількості користувачів інтернету почати здійснювати певні типи запитів до атакованого сервера.

Методи боротьби: Небезпека більшості DDoS-атак – в їх абсолютній прозорості і "нормальності". Адже якщо помилка в ПЗ завжди може бути виправлена, то повна витрата ресурсів – явище майже буденне. З ними стикаються багато адміністраторів, коли ресурсів машини (ширини каналу) стає недостатньо, або web-сайт піддається слешдот-ефекту. І, якщо різати трафік і ресурси для всіх підряд, то можна врятуватися від DDoS, у той же час, втративши велику частину клієнтів [2].

Виходу з цієї ситуації фактично немає, проте наслідки DDoS-атак і їх ефективність можна істотно понизити за рахунок правильного налаштування маршрутизатора, брандмауера і постійного аналізу аномалій в мережевому трафіку.

Боротьба з flood-атаками: Флуд буває різним: ICMP-флуд, SYN-флуд, UDP-флуд і HTTP-флуд. Сучасні DoS-боти можуть використовувати всі ці види атак одночасно, тому слід заздалегідь подумати про належний захист від кожної з них [3].

Icmp-флуд: Дуже примітивний метод забивання смуги пропускання і створення навантажень на мережевий стек через монотонну

посилку запитів ICMP ECHO (пінг). Легко виявляється за допомогою аналізу потоків трафіку в обидві сторони: під час атаки типу Icmp-флуд вони практично ідентичні.

Виконання: *# ping -i 0 -s 10000 -l 100 -q ya.ru -i* задає інтервал надсилання пакетів. Інтервал менше 200 мс дозволений тільки суперкористувачу; *-s* задає розмір пакету. Стандартний 54, найбільший 65507 байт. *-l* задає кількість пакетів що відправляються без очікування на відповідь, *i -q* робить так, щоб утиліта вивела лише підсумки.

Захист: Одним із способів захисту оснований на відключенні відповідей на запити ICMP ECHO: *# sysctl net.ipv4.icmp_echo_ignore_all=1*. Або за допомогою брандмауера: *# iptables -A INPUT -p icmp -j DROP --icmp-type 8*.

SYN-флуд: Один із поширених способів не лише забити канал зв'язку, але і ввести мережевий стек операційної системи в такий стан, коли він вже не зможе приймати нові запити на під'єднання, оснований на спробі ініціалізації великого числа одночасних TCP-з'єднань через посилку SYN-пакету з неіснуючою зворотною адресою. Після кількох спроб відіслати у відповідь ACK-пакет на недоступну адресу більшість операційних систем ставлять невстановлене з'єднання в чергу. І лише після *n*-ої спроби закривають з'єднання. Оскільки потік ACK-пакетів дуже великий, незабаром черга виявляється заповненою, і ядро дає відмову на спроби відкрити нове з'єднання. Найрозумніші DoS-боти ще й аналізують систему перед початком атаки, щоб слати запити лише на відкриті життєво важливі порти.

UDP-флуд: Типовий метод завантаження смуги пропускання, оснований на нескінченній посилці *udp*-пакетів на порти різних *udp*-сервісів. Атаку усувають шляхом від'єднання таких сервісів і установки ліміту на кількість з'єднань в одиницю часу до *dns*-сервера на стороні шлюзу:

*# iptables -i INPUT -p udp --dport 53 -j DROP -m iplimit --iplimit-above 1*

HTTP-флуд: Один із найпоширеніших на сьогодні способів флуду, оснований на нескінченному посиланні *http*-повідомлень *GET* на 80-й порт з метою завантажити web-сервер настільки, щоб він виявився не в змозі обробляти всю решту запитів. Метою флуду стає не корінь *web*-сервер, а один із скриптів, що виконують ресурсоємні завдання або що працює з базою даних. У будь-якому разі, індикатором атаки, що почалася, слугуватиме аномально швидке зростання логів *web*-сервера.

Щоб не опинитися в безвихідній ситуації під час DDoS-атаки на системи, необхідно ретельно підготувати їх до такої ситуації: всі сервери, які мають прямий доступ в зовнішню мережу, мають бути

підготовлені до простої і швидкої віддаленої роботи. Великим плюсом буде наявність другого, адміністративного, мережевого інтерфейсу, через який можна отримати доступ до сервера при зайнятому основному каналі.

Програмне забезпечення, використовуване на сервері, завжди повинно знаходитися в актуальному стані. Це захистить від DoS-атак, експлуатуючих вразливості в сервісах. Всі слухаючі мережеві сервіси, призначені для адміністративного використання, мають бути захована брандмауером від всіх, хто не повинен мати до них доступу.

На підходах до сервера (найближчому маршрутизаторі) має бути встановлена система аналізу трафіку, яка дасть змогу своєчасно дізнатися про атаку, що починається, і вчасно виконати заходи з її запобігання.

Слід зазначити, що всі прийоми та методи, приведені вище, спрямовані на зниження ефективності DDoS-атак, що мають за мету максимально загрузити ресурси машини. Якщо в розпорядженні є справді широкий канал, який легко пропустить трафік невеликого ботнету, можна вважати, що від 90% атак сервер захищений. Інший спосіб захисту оснований на організації розподіленої обчислювальної мережі, що включає безліч дублюючих серверів, які під'єднані до різних магістральних каналів. Коли пропускна спроможність каналу закінчуються, все нові клієнти перенаправляються на інший сервер або ж поступово "розподіляються" по серверах за принципом round-robin. Це неймовірно дорога, але дуже усталена структура.

## ЛІТЕРАТУРА

1. Защита от хакеров корпоративных сетей ; пер. с англ. А.А.Петренко. – 2-е изд. – М. : Компания АйТи ; ДМК-Пресс, 2005. – 864 с. : ил.

2. Матеріали сайту // http://systemnews.com.ru/?mod=art&part=other&id=020.

3. Матеріали сайту // http://www.xakep.ru/post/49752/.

*Решетніков О.В.,*
*Національна академія Служби безпеки України*

## МЕТОДИКА ПІДГОТОВКИ ФАХІВЦІВ З ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Із метою якісної підготовки, на сучасному рівні, фахівців з технічного захисту інформації, насамперед, необхідно зосередити увагу на таких темах:

1. *Основні положення нормативно-правового регулювання технічного захисту інформації в Україні.*

1.1. Сучасний стан нормативно-правового регулювання технічного захисту інформації в Україні.

1.2. Нормативно-правові документи щодо організація протидії витоку інформації.

2. *Методи, засоби та заходи захисту мовної інформації на об'єктах інформаційної діяльності.*

2.1. Загальні питання щодо витоку мовної інформації.

2.2. Лазерні канали витоку мовної інформації та параметричні явища в елементах приладів.

2.3. Характеристика середовищ поширення мовної інформації.

2.4. Характеристика сигналів, створюваних у каналах зв'язку при наявності акустичних полів та наведень.

2.5. Проведення випробувань для вимірів характеристик акустичних сигналів.

2.6. Засоби вимірювань параметрів вібрацій.

2.7. Засоби акустичної розвідки.

2.8. Принципи функціонування та основні характеристики мікрофонів.

2.9. Направлені мікрофони та лазерні акустичні системи розвідки.

3. *Методи, засоби та заходи захисту інформації в інформаційно-телекомунікаційних системах.*

3.1 Технічні канали витоку інформації та спеціального силового впливу.

3.2. Класифікація технічних каналів витоку інформації.

3.3. Засоби радіотехнічної розвідки.

3.4. Скануючи приймачі.

3.5. Портативні засоби знімання інформації з провідних ліній.

3.6. Цифрові аналізатори спектру, радіотестери, радіочастотоміри.

3.7. Методи та засоби захисту інформації по каналу побічних електромагнітних випромінювань та наведень (ПЕМВН).

3.8. Екранування та заземлення технічних засобів.

3.9. Просторове та лінійне зашумлення.

3.10. Оцінка захищеності інформації від витоку по каналу ПЕМВН.

4. *Методи, засоби та заходи захисту інформації від витоку через закладні пристрої.*

4.1. Класифікація та характеристика закладних пристроїв.

4.2. Пристрої та системи, здатні створювати канали витоку інформації.

4.3. Принципи перехоплення мовної інформації в мережах зв’язку.

4.4. Апаратура для проведення пошукових робіт.

4.5. Нелінійні локатори.

4.6. Детектори диктофонів.

4.7. Програмно-апаратні комплекси.

4.8. Радіоприймачі, селективні вольтметри та аналізатори спектру.

3.4. Методологія пошукових робіт закладних пристроїв.

Зазначений перелік тем актуальний нині, а також сприятиме розвитку у студентів таких навичок: аналіз технології оброблення інформації за допомогою методів функціонального аналізу та ієрархічної декомпозиції; класифікація інформації за режимом доступу та правовим режимом формування за допомогою методів структурного аналізу моделі загроз та порушників на основі визначення переліку та функціональної структури технічних каналів витоку та каналів несанкціонованого доступу; аналізування та оцінювання інформаційних ресурсів об’єкта захисту; моделювання загроз та оцінювання ризиків витоку інформації на об’єкті захисту.

*Ришкевич О.І.,*
*Член ГІС Асоціації,*
*ДП “Головний інформаційно-обчислювальний центр*
*ДП НЕК “Укренерго”*

*Житіков П.І.,*
*Член ГІС Асоціації,*
*підприємство “УКРСПЕЦЗВ’ЯЗОКМОНТАЖ”*

## ВИКОРИСТАННЯ АСУ “ТЕЗАУРУС” ДЛЯ ОПТИМІЗАЦІЇ РОБОТИ ОБ’ЄКТІВ ПОДВІЙНОГО ПРИЗНАЧЕННЯ

Необхідною ланкою державного будівництва в Україні, умовою її рівноправного й гідного входження у світове співтовариство як його конкурентоспроможного члена, є практичне вирішення питань оперативного управління на стратегічному та тактичному рівнях.

Ми говоримо про прийняття рішень державними менеджерами, на всіх рівнях ієрархії державного управління, керівництво безпосередньою діяльністю суб’єктів господарювання. Повною мірою це стосується, на нашу думку, і проблеми вдосконалення військової науки та освіти [1].

У доповіді подаємо результати розробки та практичного впровадження автоматизованої системи управління (АСУ), яка успішно вирішує перераховані вище завдання в умовах конкретного виробничого процесу (виробництво, регулювання, споживання енергії), в режимі реального часу.

Автори-розробники вважають, що застосування пропонованої АСУ буде продуктивним і дасть високі показники в роботі як у народному господарстві, так і в збройних силах та інших силових структурах нашої держави.

АСУ “Тезаурус” призначена для комплексного вирішення завдань оперативного розрахунку і оптимізації поточних встановлених режимів виробництва: комплексу робіт суб’єктами господарювання/виконання завдань підрозділами з метою підтримки прийняття рішень керівниками всіх рівнів ієрархії управління [2, с. 93].

Завдяки мережевому обміну інформацією в режимі реального часу з орієнтацією на зворотний зв’язок та застосування можливостей SCADA-систем була впроваджена верифікація розрахункових схем. У такий спосіб забезпечується автоматичний пошук і виключення помилкових даних на етапах формування топологічної моделі виробництва комплексу робіт з достоверізацією технологічних параметрів.

АСУ “Тезаурус” побудована як інтегрована ієрархічно-розподілена ергатична система, яка має сучасні засоби для збирання, реєстрації, оброблення, моніторингу, передачі, зберігання, обліку, ревізії, відображення та захисту інформації.

У складі АСУ “Тезаурус” на основі єдиної інформаційної бази з уніфікованим графічним інтерфейсом реалізовано:

– моніторинг режимів роботи всіх рівнів ієрархії АІС;

– автоматичне формування розрахункових схем взаємодії та актуальних первинних схем ведення робіт суб’єктами господарювання;

– автоматизована побудова моделі режиму формування матеріально-технічних ресурсів (яка включає в себе неспостережені підсхеми) та управління їх використанням;

– оцінки стану режиму за інформацією реального часу SCADA-систем;

– оперативний розрахунок сталих і самовстановлюваних режимів ведення робіт по інтенсивності;

– визначення допустимого перевищення (зниження) граничних параметрів при виконанні комплексу робіт суб’єктами господарювання;

– розрахунок динамічної стійкості (у випадках надзвичайних ситуацій) усіх рівнів ієрархії управління;

– оптимізацію режимів господарювання за ефективністю відповідно до критеріїв функціонування ринкових факторів (кон'юнктури ринку);

– оптимізацію режимів управління з енергозбереження;

– розрахунок інтенсивності і форм контрольно-ревізійних заходів;

– побудову мережевих режимних тренажерів для оперативно-диспетчерського персоналу суб'єкта експлуатації системи;

– еквівалентування і агрегування схем управління;

– проведення автоматизованого обліку та аудиту матеріально-технічних ресурсів суб'єкта експлуатації системи.

АСУ "Тезаурус" широко використовує можливості роботи з 3D-графічним зображенням схем управління комплексом робіт і взаємодією рівнів ієрархії, технологічних схем виробничих процесів суб'єктів господарювання. Це дає змогу оперативно, в режимі реального часу, проводити ефективний аналіз результатів розрахунків на всіх рівнях ієрархії управління.

Базовим елементом, початковим (нижнім) рівнем АСУ "Тезаурус", є "фрейм". Фрейм, як зона роботи окремого суб'єкта господарювання або його структурного підрозділу, виступає виокремленою частиною інформаційного простору АСУ, яка володіє індивідуальними параметрами, достатніми для ідентифікації за топологічним принципом. В межах "фрейму" фактично розміщені робочі місця операторів, приймається вхідна інформація, обробляється, формується вихідна інформація, також розміщується ліцензоване ПЗ, яке перебуває на балансі суб'єкта господарювання/підрозділу.

У технології роботи з "фреймом" розробники пропонують нові рішення, засновані на застосуванні планшетів (інших аналогічних подібних пристроїв) у взаємодії з дата-центрами. Такий підхід дає змогу розширити функціональність робочого місця оператора (включаючи можливість його роботи в "польових умовах", можливості проведення об'єктивного контролю виконання робіт та стану параметрів виробничих процесів) з одночасною оптимізацією витрат на його матеріально-технічне забезпечення. Більше того, такий підхід надає нові можливості для ефективної спільної роботи колективу, члени якого перебувають у різних параметрах простору з актуальною інформацією в режимі реального часу.

Переваги, які за результатами впровадження продемонструвала АСУ "Тезаурус":

– підвищення надійності та ефективності роботи суб'єкта експлуатації системи;

– забезпечення прийняття оперативно-технологічним та диспетчерським персоналом усіх рівнів управління і ланок, ефектив-

них рішень у нормальних, доаварійних, аварійних і післяаварійних ситуаціях;

– зменшення втрат, ефективне енергозбереження матеріально-технічних ресурсів за рахунок оптимізації режимів управління комплексом робіт;

– зменшення витрат фінансових ресурсів на матеріально-технічне забезпечення та функціонування АСУ;

– оптимальний розподіл, облік використання і контроль матеріально-технічних і людських ресурсів суб'єкта експлуатації системи.

У разі виникнення виробничої необхідності (навчання, перепідготовка персоналу, участь у виставках, підготовка зовнішніх інформаційних звітів різного характеру) АСУ "Тезаурус" дає змогу автоматично перетворювати технологічну інформацію зі спеціалізованих баз даних у технологічні знання, концентруючи віртуальний інформаційно-розподілений єдиний простір як для корпоративних клієнтів, так і для ЗС, спецслужб, як в Україні, так і за її межами.

## ЛІТЕРАТУРА

1. Мовчан А.П. Адаптивні та параметрично-оптимальні системи управління : навч. посіб. / А.П.Мовчан, О.В.Степанець. – К. : НТУУ "КПІ", 2011. – 108 с.

2. Ришкевич О.І. "Тезаурус", корпоративна інформаційна безпека – людина, суспільство, держава / О.І.Ришкевич, А.Д.Котов // Актуальні проблеми управління інформаційною безпекою держави : зб. матер. наук.-практ. конф., 30 березня 2012 р., м. Київ. – К. : Наук-вид. відділ НА СБ України, 2012. – С. 93-95.

*Самарай В.П.,*
*кандидат технічних наук,*
*старший науковий співробітник, доцент*

*Самарай Р.В.,*
*Київський міжнародний університет*

## МОДЕЛЮВАННЯ БЕЗПЕКИ В ТЕОРІЇ ГРАФІВ

Ефективне ухвалення рішень з управління складними системами (СС – інформаційними, енергетичними, політичними, соціальними, військовими, ідеологічними, освітніми та ін.) потребує використання формалізованої моделі керованого об'єкта. Але існує про-

блема застосування наявних інформаційних і класичних соціологічних моделей саме в критичних, нестандартних, непередбачених ситуаціях, через повний або переважний розвал економіки, в умовах, які визначаються не економічною стабільністю, а перехідними процесами в результаті політичних, екологічних і економічних криз, зміни політичних курсів і пріоритетів, терору, військових дій або воєн, переворотів.

Для таких СС винятково економічне планування не головна мета управління. У цьому випадку в перехідні періоди головна мета управління спрямовується насамперед на виявлення й подолання нестабільності, тупикових ситуацій і на підтримку в СС стабільних системоутворювальних процесів. І, навпаки, у разі планування й проведення диверсійних дій, інформаційних та інших воєн, ставляться прямо протилежні завдання.

Системний аналіз (СА) поєднується з моделюванням, оптимізацією, діагностикою погіршення структури і функціонування СС, прогнозуванням її можливих тенденцій, ситуацій, станів, поведінки. Для ухвалення найефективніших рішень з коректування тупикових і небажаних ситуацій і при ідентифікації функціональних порушень СС необхідно отримати уявлення про її структуру, внутрішній і зовнішній взаємовплив складових СС і сусідів зовні.

Для моделювання СС найефективнішими вбачаються *моделі теорії графів*: когнітивні моделі, сіті Петрі, ланцюги Маркова, системи масового обслуговування (СМО), алгоритми, імітаційні моделі, потокові оптимізаційні моделі, нейронні мережі, семантичні мережі експертних систем (ЕС), кінцеві і клітинні автомати (КА), фрактали. Найзагальнішою, відправною, базовою для подальшого розгляду, аналізу й моделювання подається *когнітивна модель*, на основі якої вже можна побудувати і складніші види графів – *динамічні і стохастичні графо-аналітичні моделі* СС.

1. *Потокові моделі оптимізації (на графах) дають змогу по* всесвітньовідомих задачах *“про MAX потік і MIN перетин”; “потоковій транспортній задачі”; “про потік MIN вартості”; “про пошук MIN шляху”; “про пошук критичного шляху ”; “комівояжера”; “немережевій транспортній задачі”:*

– вирішувати задачі безпеки й інформаційно-психологічного впливу;

– знаходити вузькі місця в структурі інформаційних та інших СС, максимальні швидкості, обсяги й оптимальні маршрути передачі інформації та знань;

– визначати критичні шляхи, тривалість і мережні графіки при плануванні інформаційних, енергетичних, політичних, військових, ідеологічних, освітніх та ін. проектів, операцій, заходів, направляти необхідне саме в “критичний шлях”.

2. *Ланцюги Маркова, СМО, Семантичні мережі ЕС, нейронні мережі* – дають змогу за аналогією з регресійними моделями прогнозувати, оптимізувати, діагностувати події на основі статистичних спостережень і теорії ймовірності.

3. *Кінцеві і клітинні автомати, фрактали* – дають змогу моделювати і прогнозувати ситуації, стани, поведінку, параметри СС.

Враховуючи необхідність побудови найадекватніших і найефективних моделей для аналізу й ухвалення рішень в умовах хаосу, протидії, конкуренції, конфліктів, кооперації та невизначеності, виникає потреба застосування не простих, а достатньо складних графо-аналітичних моделей, тобто з багатьма чинниками, динамічних, стохастичних, і навіть нелінійних і багатовимірних. Саме таким вимогам відповідають *динамічні моделі на сітях Петрі (СП) та імітаційні моделі*. Імітаційні моделі легко інтегрують в себе всі можливі види інших моделей, а прості СП можуть бути легко ускладнені до так званих “кольорових, “тимчасових”, “вірогідностних”, “функціональних”, “ієрархічних” і ін. видів СП. У СП (програмі CPN-TOOLS та ін.), імітаційних моделях на алгоритмічних мовах і в математичних програмах (Lab-VIEW, MathLAB, EXCEL та ін.) можливо реалізувати багатовимірність будь-якої складності. Існують правила взаємного перетворення “мережевого графіка”, імітаційної моделі, алгоритму, СП, когнітивних карт та інших графичних моделей.

З іншого боку, в прикладному аспекті становлять інтерес дослідження *соціальних мереж, мережні моделі спинів* з енергією Ізінга і графічні *моделі Д.Уоттса і С.Строгатца*, які запропонували такий параметр графів і мереж, як коефіцієнт кластерності, що визначає рівень зв’язності вузлів в сітці і тенденцію до створення взаємозалежних вузлів (“кліків”). Крім того, коефіцієнт кластерності показує, скільки сусідніх вузлів є також сусідніми вузлами один для іншого. В аналізі безпеки й міжнародних відносин (МВ) цей показник характеризує *ступінь зв’язку,* впливу, обміну, товарообігу, взаємодії, торгівлі, партнерства або навпаки – тиск і протиборства між державами і наддержавними структурами, а також може характеризувати вузли і зв’язки розвідувальних та терористичних мереж і *кількість ступенів свободи*.

У теорії графів можна досліджувати особливості структури і статистичні властивості, що характеризують поведінку графів і мереж, прогнозувати динамічні зміни і відстежувати вплив таких ха-

рактеристик, як розмір графа, мережна густина, ступінь централізації і децентралізації та ін.

*Терористичні мережі* часто моделюють *клітинними автоматами (КА)*. Оскільки КА є сусідами з шістьма комірками, то вони схожі на модель Уоттса і Строгаттца. Одночасно, їх шестимірність збігається з висновками психолога С.Мілграна про "ланцюг знайомств" завдовжки у шестеро осіб. КА може бути в одному з кількох можливих станів, яке залежить від попереднього стану і стану сусідніх КА (на відміну від ланцюгів Маркова, в яких стан залежить тільки від поточного стану, але не від попередніх). КА перспективно використовувати з моделями теорії ігор в задачах кооперації і конкуренції. Крім того, чотирьох- і шестимірні КА двох- і тримірної однорідної сітки легко перетворити в граф будь-якої мірності, оскільки кількість вхідних і вихідних ребер у вузлах графів не обмежена.

Для аналізу безпеки і МВ варто згадати і теорію хаосу, результатом якої є самоподібний фрактал, тобто стохастичний граф особливої будови – ієрархічний, зручний для всіх видів класифікацій, дискримінантного і кластерного аналізу і, який став основою ієрархічних баз даних, зокрема, багатьох сегментів всесвітньої павутини і всесвітньої бази даних INTERNET.

Наведені моделі включають принципи детермінованого і стохастичного, багатоагентного і системно-динамічного підходів, а також два синергетичних підходи: моделі спинів, нейронні мережі та кластерний аналіз. Слід згадати про "паралельні тирони" з повернення до теми масштабно-інваріантних мереж у зв'язку з пошуками причин закону Зіпфа в розподілах популяцій.

Інтерес становлять *"чутливі крапки" СА – найчутливіші вузли на графах* – місця, в яких навіть невеликий зсув може призвести до великих змін у всій СС. "Чутливі крапки" дають силу і владу. При ідентифікації порушень СС треба мати уявлення про "чутливі крапки", про структуру процесів і взаємозв'язки в СС, щоб ухвалити найефективніше рішення по коректуванню ситуацій. Цільова функція та система обмежень інформаційної або соціальної СС, мають описати емерджентність і взаємостосунки технічних та програмних об'єктів або для соціальних СС – належність до різних культур, груп, блоків, релігій, субкультур. Необхідно врахувати внутрішню нелінійність СС, збільшення емерджентності в часі, зростання зв'язків і взаємну дифузію підсистем. Таку поведінку описують аналітичними формулами еволюції або в графах і мережах енергією Ізінга. В *когнітивних моделях* можна зробити розрахунки, в *СП - ви-*

*значити "чутливі крапки" динамічним моделюванням у трьох можливих режимах СП*: *1) покроковому* – з відстеженням станів у вершинах і, особливо, в "чутливих крапках"; процесів у переходах і ребрах; *2) автоматичному* – з візуалізацією всіх можливих векторів станів; *3) автоматичному* – з фіксацією тупикових ситуацій в СП за певних початкових і граничних умов.

*Смолянінов В.Г.,*
*кандидат технічних наук, доцент,*
*ПВНЗ "Європейський Університет"*

*Сухопара О.М.,*
*кандидат технічних наук, доцент,*
*Науково-виробниче підприємство "МТІ"*

## АНАЛІЗ РИЗИКІВ ПРИ ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Багато підприємств та організацій використовують в своїй роботі інформаційні системи, які з одного боку підвищують ефективність їх функціонування, а з іншого – потребують вирішення питання захищеності цих систем. Для забезпечення інформаційної безпеки (ІБ) важливо використовувати комплексний підхід, який враховує як адміністративні заходи (політику безпеки підприємства та засоби безпеки, що виконує персонал підприємства), так і заходи програмно-технічного рівня (резервне копіювання, антивірусний та парольний захист, міжланцюгові екрани, шифрування даних і т. ін.). Всі ці заходи об'єднані однією загальною властивістю – аналіз ризиків при забезпеченні інформаційної безпеки підприємства [1].

При аналізі ризиків враховуються загрози та уразливості, визначаються комплекси контрзаходів, що забезпечують достатній рівень захищеності інформаційної системи. Інформаційна система залежно від свого класу повинна мати підсистему безпеки із визначеними формальними властивостями. Залежно від оцінки власниками вартості власних інформаційних ресурсів та можливих наслідків при порушенні інформаційної безпеки, використовують два підходи до аналізу ризиків: базовий, коли з точки зору підприємства цінність інформаційного ресурсу є невисокою і розглядається набір найбільш загальних загроз безпеки (віруси, відмови обладнання, несанкціонований доступ і т. ін.) без оцінки їхніх ймовірностей. В

цьому випадку забезпечується мінімальний рівень інформаційної безпеки і характеристики загрози при цьому не розглядаються. Другий підхід, це повний аналіз, що потребує визначення цінності ресурсів, імовірність загроз, вразливість ресурсу, забезпечення необхідного рівня ІБ і т. ін. [2].

При аналізі необхідно поділити увесь захищаємий ресурс, на кілька категорій: фізичний ресурс, який оцінюється з урахуванням вартості його заміни або відновлення працездатності; програмний ресурс, що оцінюється на базі визначення витрат на його придбання та використання; інформаційний ресурс, для якого існують специфічні вимоги, наприклад, по цілісності, доступності чи конфіденційності, але оцінка його також відбувається у вартісному обчисленні; технічні засоби.

Імовірність того, що загроза буде реалізована визначається такими факторами: привабливістю ресурсу (як спеціальної дії зі сторони зацікавленої особи); можливості використання ресурсу для отримання доходу; простотою використання уразливості ресурсу при проведенні атак, де уразливість – це слабкі місця в системі захисту, які дають можливості для порушника в реалізації загроз. Величину ризику визначають на основі кошторису ресурсу помноженому на ймовірність загрози розділених на величину уразливості.

Важливість ресурсу визначається величиною шкоди, яка буде заподіяна у випадку порушення специфічних вимог до ресурсу, а сама шкода підприємству може бути заподіяна в результаті локальних атак на ресурс системи, зловмисні дії персоналу, помилки в програмному забезпеченні, несправності техніки і т. ін. При розрахунку вартості заходів захисту кошторис повинен бути меншим від величини завданої шкоди та пропорційним ймовірності завдання шкоди.

Проаналізувавши ризики, можна розробити першочергові заходи щодо їх зменшення та забезпечити потрібний захист інформаційної системи підприємства.

## ЛІТЕРАТУРА

1. Волокитин А.В. Информационная безопасность государственных организаций и коммерческих структур / А.В.Волокитин, А.П.Моношкин, А.В.Солдатенко ; под общ.ред. Л.Д.Реймана. – М. : НТЦ “ФИОРД-ИНФО”, 2002. – 272 с.

2. Щербина В.М. Інформаційне забезпечення економічної безпеки підприємств та установ / В.М.Щербина //Актуальні проблеми економіки. – 2006. – № 10. – С. 220–225.

*Сторожук А.Ю.,*
*Інститут спеціального зв'язку*
*та захисту інформації НТУУ "КПІ"*

# ВИКОРИСТАННЯ ОСОБЛИВОСТЕЙ ПОБУДОВИ ФІЛЬТРУВАЛЬНОГО ГЕНЕРАТОРА ГАМИ ДЛЯ ОЦІНЮВАННЯ СТІЙКОСТІ СИНХРОННИХ ПОТОЧНИХ КРИПТОГРАФІЧНИХ СИСТЕМ

Для функціонування будь-якої синхронної поточної криптографічної системи необхідна наявність на приймальному та передавальному боці генераторів гами, яка використовується для шифрування відкритих даних. Оскільки для нормальної роботи всієї системи необхідна постійна синхронізація апаратури прийому та передачі даних, то, відповідно, необхідна синхронізація шифраторів приймача та передавача. Для синхронізації шифраторів, необхідно встановити в генераторах гами (приймача і передавача) однакові початкові стани, що залежать від криптографічного ключа та вектору ініціалізації, яким сторони обмінюються при встановлені сеансу зв'язку.

У роботі [1] продемонстрована атака на генератор гами з лінійним законом реініціалізації початкового стану. В роботі [2] запропоновано численні вдосконалення та узагальнення наведеної в [1] атаки, зокрема для випадків, коли відома обмежена кількість векторів ініціалізації. Запропоновано також атаки на криптографічні системи, що будуються на основі генераторів гами з пам'яттю або мають нелінійний закон реініціалізації початкового стану.

У доповіді наведена узагальнена атака на генератор гами з лінійним законом реініціалізації початкового стану та функцією ускладнення, що залежить від невеликої кількості змінних.

## ЛІТЕРАТУРА

1. *Daemen J.*, *Govaerts R.*, *Vandewalle J.* Resynchronization Weaknesses in Synchronous Stream Ciphers // Advances in Cryptology – EUROCRYPT'93, Proceedings. – Springer-Verlag. – 1993. – P. 159–167.

2. .*Armknecht F.*, *Lano J.*, *Preneel B.* Extending the resynchronization attack // Selected Areas in Cryptography – SAC'04. – Springer-Verlag. – 2004. – P. 19–38.

*Фролов Р.А.,*
*Національна академія Служби безпеки України*

# ПІДВИЩЕННЯ РІВНЯ ЗАХИСТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ ШЛЯХОМ ПЕРЕХОДУ НА ВІЛЬНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

При розробленні стратегії та основних заходів із забезпечення інформаційної безпеки України більшість вітчизняних фахівців схиляються до реагування на процеси, що відбуваються в інформаційному середовищі нашої країни або блокування їх негативних результатів.

На підставі визначення основних постулатів та загроз національній безпеці формується й вся система забезпечення інформаційної безпеки.

Напевно, більшість погодиться з думкою, що будь-яка система захисту інформаційного простору держави стає все більш залежною і уразливою від функціонування комп'ютерних систем та всесвітньої Інтернет-мережі.

Аналізуючи вказане питання у розрізі його реалізації в Україні, можна дійти невтішного висновку, що у нашій державі дуже мало уваги приділяється саме створенню надійного технічного підґрунтя для створення ефективної системи захисту, у тому числі, поступовому переходу від пропрієтарного до вільного програмного забезпечення (далі – ВПЗ) для всіх органів державної влади та управління.

Зокрема, переважна більшість громадян України, зокрема представників вітчизняних органів влади і управління користуються програмним забезпеченням компанії "Microsoft" (США) – "Windows" або його так званими "піратськими" версіями.

При цьому сама по собі операційна система "Windows" не відрізняється особливою надійністю. Так, за визнаннями аналітиків компанії Gather (нещодавно відбулася конференція з IT-спеціалістами) популярна система "Windows" може загинути під загрозою власних численних недоліків. Більша частина присутніх на конференції погодилася з тим, що в "Microsoft" необхідно частково переглянути свій підхід до розроблення програмних платформ.

З початку 2000-х років більшість європейських країн (а за ними – країни інших регіонів) виявляють бажання більш широкого використання відкритих стандартизованих технологій на противагу пропрієтарним і неспецифікованим. Стандартні технології розглядаються державами як засіб ефективної боротьби з домінуванням окремих постачальників, як механізм зниження порогу входження

на ринок ІТ-продуктів і послуг, а також спосіб підтримки конкурентоспроможності вітчизняних постачальників на ринку складних ІТ-систем.

У Російській Федерації ще у 2007 році вказане питання стало предметом для обговорення в Міністерстві інформаційних технологій та зв'язку. На сьогодні в Росії, відповідно до розпорядження Уряду РФ від 17.12.2010 р. № 22999-р, реалізується план переходу федеральних органів виконавчої влади і федеральних бюджетних закладів на використання вільного програмного забезпечення на 2011-2015 роки.

Дистрибутиви "Лінукс" (один із різновидів ВПЗ) мають популярність у різних державних структур: Федеральний уряд Бразилії добре відомий своєю підтримкою "Лінукса", а російські військові розробляють свій власний дистрибутив "Лінукс". Уряд індійського штату Керала випустило припис щодо переходу всіх шкіл штату на використання "Лінукс". Із метою забезпечення технологічної незалежності Китай використовує лише "Лінукс" на своїх процесорах "Loongson". Деякі регіони Іспанії розробили свої власні дистрибутиви "Лінукс", які використовуються в освіті і держуправлінні, наприклад, "gnuLinEx" в Естремадуре и "Guadalinex" в Андалусії. Португалія також користується своїм власним дистрибутивом "Caixa Mbgica", розробленим для нетбука "Magalhres" і державної програми електронної освіти. Франція і Німеччина роблять низку кроків зі збільшення використання "Лінукс".

Як стверджують дослідники компанії "Cnews", вільному програмному забезпеченню часто надають перевагу інноваційні компанії, орієнтовані на швидке зростання, а також фірми, яким необхідно вирішувати нетрадиційні завдання з управління даними.

Вільне програмне забезпечення має тенденцію до поширення серед розвинених країн. Дослідження, проведене у 2010 році організацією "National Open Source. Software Observatory", надає таку інформацію:

- у Німеччині 60 % комерційних компаній вже використовують ВПЗ, 4,1 % вводять на даний час; 8,1% – не планують введення ВПЗ;
- у Франції 67 % компаній використовують ВПЗ, а в деяких великих компаніях основні бізнес-процеси управляються рішеннями на базі ВПЗ ("Franprix", "Leader Price", "France-Presse", "Gaz de France", "Peugeot", "Citroen");
- 46% норвезьких компаній використовують ВПЗ;
- у Фінляндії станом на 2008 рік 75% приватних компаній використовують ВПЗ [19].

Враховуючи зазначене, можна дійти таких висновків:

- використання програмного забезпечення компанії “Microsoft” вітчизняними органами влади і управління економічно недоцільне та невиправдано витратне;

- “Windows” не відповідає сучасним вимогам безпеки та за певних умов може становити загрозу інформаційній безпеці України;

- рівень розповсюдження в Україні ВПЗ, у тому числі серед державних структур, залишається вкрай низьким.

Навіть неупереджений аналітик може дійти висновку, що при загостренні відносин із США або за необхідності лобіювання ними будь-яких питань, інформаційне середовище може бути використано на шкоду інтересам України.

При цьому кількість користувачів ВПЗ в Україні серед фізичних осіб або приватних підприємств залишається вкрай низькою. Окремі ініціативи вітчизняних фахівців залишаються без належної уваги на те з боку державних структур, які лише декларують свої наміри у цій сфері.

Натомість державна підтримка відкритих стандартів, яка обмежується лише деклараціями, не може бути ефективною, тому необхідно вжити відповідні заходи, які б сприяли більш широкому застосуванню відкритих стандартів у державних системах.

На сьогодні найефективнішим із таких заходів є прийняття вітчизняного зводу вимог по сумісності для урядових систем GIF, в якому перераховуються потрібні та рекомендовані стандарти і специфікації.

На наступному етапі Україні необхідно буде створити власну систему вільного програмного забезпечення, використовуючи позитивний досвід інших країн. При цьому ініціатива повинна мати загальнодержавний рівень, до розробки вказаного питання мають бути залучені різні державні та приватні структури.

При підборі ВПЗ необхідно проводити обов’язковий аудит системи на предмет її уразливості. Перед використанням програмного продукту у виробничому режимі необхідно провести сертифікацію новоствореною для цієї мети державною установою із затвердженим спеціальним державним стандартом.

Здійснивши перехід на ВПЗ, Україна поступово отримає економічну незалежність від іноземних економічних структур, що сприятиме стабільному розвитку її власних ІТ-центрів та технологій.

У результаті, наша держава гарантовано зможе забезпечити й власну інформаційну безпеку.

*Хараберюш І.Ф.,*
*доктор юридичних наук, професор,*
*Донецький юридичний інститут МВС України*

*Меживой О.В.,*
*кандидат юридичних наук,*
*Донецький юридичний інститут МВС України*

# ІНФОРМАЦІЙНА БЕЗПЕКА КОРИСТУВАЧІВ МОБІЛЬНОГО ЗВ'ЯЗКУ ТА ЗАПОБІГАННЯ ЗАГРОЗАМ ЇЇ ПОРУШЕННЯ

Розвиток інформаційних технологій – не лише важлива державна функція, а й обов'язкова умова забезпечення ефективного використання нагромаджених суспільством інформаційних ресурсів для створення розвиненого і захищеного інформаційного середовища [1, с. 149-156; 2, с. 118]. Сучасні технології надають можливість законного отримання інформації про зміст розмови абонентів мобільного зв'язку, що може бути використано як джерело цінних даних у розслідуванні кримінальних правопорушень [3, с. 10-11]. Однак стільниковий зв'язок, як і будь-який радіозв'язок, може бути перехоплено не лише суб'єктами кримінального судочинства, а і особами, не пов'язаними із розслідуванням кримінальних проваджень. Тим самим порушується інформаційна безпека користувачів мобільного телефонного зв'язку, права яких знаходяться під захистом держави [4-7].

Згідно із законодавством України інформаційна безпека – це стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається завдання шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [8].

Поняття "інформаційна безпека" включає забезпечення функціонування інформаційних систем у разі виникнення найрізноманітніших загроз [9, с. 697]. Особливого значення проблеми інформаційної безпеки набувають з огляду на швидкий розвиток глобального інформаційного суспільства, широке використання інформаційно-комунікаційних технологій у спілкуванні громадян, зокрема за допомогою засобів мобільного зв'язку.

Зважаючи на важливість цієї проблеми, для запобігання незаконного перехоплення інформації у системах мобільного зв'язку

використовується шифрування даних. У розробленні безпечного протоколу передачі GSM-систем активну участь брали фахівці з Європи та США. Основою сучасної системи захисту каналів зв'язку GSM слугують алгоритми, деталі яких відомі лише постачальникам обладнання та операторам зв'язку:

A3 – алгоритм, який захищає телефон від клонування;

A8 – алгоритм, який генерує ключ на основі вихідних даних A3;

A5 – алгоритм, який шифрує оцифровану мову для забезпечення конфіденційності переговорів. Найбільший інтерес становить алгоритм A5, адже саме він більшою мірою відповідає за конфіденційність переговорів [10, с. 11-12].

У мережах GSM використовуються дві версії алгоритму A5: A5/1 та A5/2. Поява двох версій алгоритму пояснюється існуванням експортних обмежень на технології шифрування країнами Європи та США. Так, багато країн використовують алгоритм A5/1. У країнах, на які поширюються експортні обмеження, використовується алгоритм A5/2. При цьому алгоритм A5/1 має більш високу ступінь криптостійкості.

Виходячи з технічних особливостей потокового шифрування, це досить стійкий алгоритм, який використовується у військовому зв'язку. В A5 використовують регістри розміром 19, 22 і 23 біта, в сукупності дають 64-бітний ключ. Хоча довжина ключа невелика, розкрити його в режимі реального часу на даний момент складно, тому що для цього потрібні значні обчислювальні потужності. Тому незаконно прослуховувати телефонні розмови, тобто розшифровувати перехоплену інформацію в реальному часі, практично неможливо. Однак у більш слабкому шифрі A5/2 ситуацію посилює адаптація ключа до місцевих вимог деяких країн, у результаті чого в 64-бітному ключі 10 або більше бітів замінюються нулями.

Тобто рівень стійкості ключа такий, що розшифрувати розмову може будь-який сучасний комп'ютер із середніми обчислювальними потужностями. У шифрі A5/2 початкові заповнення використовуваних для шифрування регістрів визначаються відкритим і секретними ключами. Відкритий ключ різний у кожному сеансі, але при цьому відомий.

Найпростіший тип атаки на алгоритм A5/2 – це "розкриття" секретного ключа за допомогою підбору з 240 максимальних варіантів. При підборі робиться припущення про зміст перших двох регістрів, а зміст останнього регістра відновлюється.

Програмні засоби розшифровки GSM-протоколу вже давно відомі. Апаратура для перехоплення GSM-сигналу також доступна. У світі існує приблизно 20 видів устаткування для прослуховування даних,

що передаються GSM-каналами. Проте спеціальне обладнання для прослуховуванням телефонних розмов коштує дорого та його продаж в Україні обмежений. Вартість апаратури може становити від 5000 до 20000 доларів США [10, с. 14-15].

Але для того, щоб прослуховувати телефонні розмови не обов'язково здійснювати атаку шляхом підбору. Зловмисник може отримати секретний ключ абонента і без проблем розшифровувати розмову в режимі реального часу.

Отримати доступ до секретних ключів можна, наприклад, шляхом отримання доступу до реєстру абонентів оператора телекомунікацій (Home Location Register). Для цього необхідно отримати доступ до мережі, що зробити не так складно. Справа в тому, що не всі компоненти мережі стільникового оператора з'єднані кабелем, деякі базові станції використовують для під'єднання до мережі супутниковий або радіорелейний зв'язок. Бездротова передача даних, як відомо, досить вразлива. Більш того, зловмисник може проникнути в будівлю оператора зв'язку, де встановлено апаратуру, що зберігає ключі абонентів.

Не варто виключати можливості доступу зловмисником до кабелю, що йде від базової станції. Отримавши такий доступ, можна витягти сеансовий ключ, перехоплювати дзвінки в ефірі та прослуховувати канал, розшифровуючи його в реальному часі.

Заволодіти секретними ключами, які забезпечують безпеку зв'язку, можна шляхом зчитування відповідного ключа з SIM-картки абонента, отримавши до неї фізичний чи віддалений доступ.

Фізичний доступ до SIM-картки здійснюється із застосуванням спеціального пристрою – "рідера", що під'єднується до комп'ютера. Далі програма роботи з рідером виконує приблизно 140000 викликів до SIM-картки. Секретний ключ визначається методом диференціального криптоаналізу отриманих даних. Для цього потрібна серйозна спеціальна математична підготовка [10, с. 15].

Слід зазначити, що для реалізації такого зчитування необхідно отримати фізичний доступ до SIM-картки на досить тривалий час (близько 8 годин). Так, отримати доступ до SIM-картки зловмисник може попросивши телефон під будь-яким приводом, підкупивши продавця перед продажем SIM-картки, або просто викрасти мобільний телефон, а потім повернути власникові.

Отримати секретний ключ з SIM-картки віддалено набагато складніше. Для цього застосовується імітаційна базова стільникова станція з більш потужним сигналом, ніж станція стільникового оператора. При цьому мобільний телефон обиратиме для роботи в мережі GSM саме цю станцію [10, с. 15].

Отже, можна виокремити ознаки подібних несанкціонованих атак на рухоме обладнання користувачів мобільного зв'язку та мережі зв'язку, знання яких допоможе вберегти їхні приватні розмови від прослуховувань зловмисниками, забезпечити захист їх інформаційної безпеки. Це такі ознаки: зникнення мобільного телефону з поля зору на певний час; швидка розрядка акумулятора; поява сигналу в тих місцях, де зазвичай не "ловить" стільниковий оператор. Водночас питання забезпечення цілковитої інформаційної безпеки споживачів телекомунікаційних послуг є досить вразливим, адже абонент не може вплинути на надійність зберігання інформації оператором мобільного зв'язку.

При цьому забезпечення інформаційної безпеки – це основа, на якій ґрунтується національна політика України щодо розвитку інформаційного суспільства, а поліпшення стану інформаційної безпеки в умовах використання новітніх інформаційно-комунікаційних технологій виступає однією з основних стратегічних цілей розвитку інформаційного суспільства в Україні.

## ЛІТЕРАТУРА

1. Інформаційна діяльність в правознавстві : моногр. / П.Д.Біленчук, О.В.Кравчук, В.Б.Міщенко, Ю.О.Пілюков. – К. : Наука і життя, 2007. – 244 с.

2. Медвідь Ф.М. Інформаційна безпека України: генеза і становлення / Ф.М.Медвідь // Наукові праці МАУП. – К., 2010. – № 2(25). – С. 116–122.

3. Організація протидії злочинам, пов'язаним із викраденнями мобільних телефонів : науково-практичні рекомендації / О.В.Меживой, І.Ф.Хараберюш. – Донецьк, 2013. – 72 с.

4. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР // Відомості Верховної Ради України від 02.08.1994. – К., 1994. – № 31. – Ст. 286.

5. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI // Відомості Верховної Ради України від 27.08.2010. – К., 2010. – № 34.

6. Про захист прав споживачів : Закон України від 12.05.1991 р. № 1023-XII // Відомості Верховної Ради УРСР. – К., 1991. – № 30. – Ст. 379.

7. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII // Відомості Верховної Ради України від 01.12.1992. – К., 1992. – № 48. – Ст. 650.

8. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки : Закон України від 9.01.2007 р. № 537-V // Відомості Верховної Ради України від 23.03.2007. – К., 2007. – № 12. – С. 511.

9. Теория оперативно-розыскной деятельности : учеб. / под ред. К.К.Горяинова, В.С.Овчинского, Г.К.Синилова. – М. : ИНФРА-М, 2007. – 832 с.

10. Михайлов Д.М. Защита мобильных телефонов от атак / Д.М.Михайлов, И.Ю.Жуков ; под ред. А.М.Ивашко. – М. : Фойлис, 2011. – 192 с.

*Чабан О.М.,*
*Національна академія Служби безпеки України*

## ПРОБЛЕМА НЕУЗГОДЖЕНОСТІ НОРМАТИВНИХ ДОКУМЕНТІВ, ЩО РЕГЛАМЕНТУЮТЬ СТВОРЕННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Актуальність проблеми забезпечення захисту інформації зростає з кожним роком. Основним методом захисту інформації в інформаційно-телекомунікаційних системах є створення комплексної системи захисту інформації (КСЗІ).

Сьогодні виникає безліч проблем при побудові комплексної системи захисту інформації в автоматизованих системах.

Проаналізувавши нормативні документи щодо створення КСЗІ, дійшли висновку, що не існує єдиного підходу до побудови КСЗІ. Яскравим прикладом цьому є НД ТЗІ 3.7-003-05 “Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі”, який не дає чітко визначеного порядку побудови КСЗІ та вимог до пакету документів КСЗІ.

Вся система нормативних документів в галузі технічного захисту інформації є розрізненою, при розгляді НД ТЗІ 3.7-003-05, НД ТЗІ 3.7-001, Постанови №180 та ГОСТ34.601-90, в яких висуваються вимоги до документів КСЗІ, не має єдиного визначеного комплекту мінімально необхідних документів та вимог до них. Відсутність чітко сформульованих вимог до документів КСЗІ – наслідок того, що немає чіткого порядку побудови КСЗІ, через що виникають супере-

чки та розбіжності при проведенні державної експертизи КСЗІ в АС. А саме, розроблене та погоджене технічне завдання на КСЗІ в АС регламентує достатній комплект документів, але трапляються випадки, коли державному експерту даний пакет документів є недостатнім на підставі того, що він не містить окремих документів, визначених в НД ТЗІ 3.7-003-05, Постанові №180 та ГОСТ34.601-90. Особливо гостре питання виникає при розробленні КСЗІ в АС класу 2 та 3.

При розробленні всіх документів, що прописані у зазначених вище НД ТЗІ та ГОСТ, вартість побудови КСЗІ перевищує вартість самої системи в кілька разів і становить десятки, інколи сотні, тисяч гривень. Не кожна державна установа може виділити таку суму грошей на побудову комплексної системи захисту інформації, а інформація з обмеженим доступом циркулює в кожній державній установі.

Для вирішення проблеми єдиного підходу до побудови КСЗІ в АС необхідно визначити для кожного типу системи (класу АС) мінімально необхідний перелік документів згідно з НД ТЗІ 3.7-003-05, НД ТЗІ 3.7-001, Постановою №180, ГОСТ34.601-90, іншими нормативними документами та сформувати вимоги до змісту та вигляду документів. При розробленні такого переліку документів, необхідно брати до уваги випадки, коли КСЗІ будується у вже існуючій системі. Необхідність розроблення документів, що не визначені цим переліком, повинна встановлюватися розробником КСЗІ та власником системи.

Визначаючи такий перелік, необхідно привести у відповідність і документи, що регламентують проведення експертизи в галузі ТЗІ. У такий спосіб вирішується проблема між розробником КСЗІ, власником КСЗІ та державним експертом.

## ЛІТЕРАТУРА

1. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

2. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.

*Чаплига В.М.,*
*доктор технічних наук, професор*

*Нємкова О.А.,*
*кандидат фізико-математичних наук, доцент,*
*Університет банківської справи*
*Національного банку України (м. Київ),*
*Львівський інститут банківської справи*

# ТЕХНОЛОГІЇ СУЧАСНИХ СИСТЕМ КОНТРОЛЮ НАД ІНФОРМАЦІЙНИМИ ПОТОКАМИ

Сучасні вимоги до складних інформаційних систем, що обслуговують фірми та установи, характеризуються двома протилежними тенденціями. Перша тенденція – принципова відкритість системи стосовно мережі Інтернет, що зумовлено необхідністю листування електронною поштою, консультаціями по ISQ та Skype, обміну по FTP-серверу та ін. Друга тенденція – необхідність зберегти секрети фірми, не допустити витоку інформації. Якщо врахувати, що кількість документації на фірмі з обмеженим доступом зростає щодня, а організаційно-адміністративні заходи з інформаційної безпеки не забезпечують потрібного рівня захисту внаслідок людського фактору, виникає необхідність упровадження комп'ютерних систем, що запобігають витоку інформації [1].

Системи для запобігання витоку інформації (в англомовних країнах DLP-системи) відомі на українському ринку вже кілька років. Одним із представників таких систем є Контур інформаційної безпеки SearchInform [2]. Контур оснащений кількома потужними пошуковими модулями, які дають змогу виявити рух критичної інформації у локальній мережі. Принцип роботи таких модулів базується на тому, що для кожного інформаційного каналу існує своя технологія виявлення появи інформації з певними ознаками – критичної інформації, які збігаються з наперед заданими ознаками політики безпеки. У такий спосіб можна виявити рух критичної інформації в реальному часі.

Досить часто буває, що потрібно проаналізувати інформацію, яка колись була відправлена по електронній пошті. Для проведення ретроспективного моніторингу потрібно мати архів електронних листів. Сьогодні чинний закон про збереження даних електронного листування за останні сім років. Якщо ставити питання більш широко, то потрібно проводити резервне копіювання всієї перехопленої

інформації, яка надходить у DLP-систему з сервера локальної мережі через комутатор з віддзеркаленням, що дає змогу відслідковувати діяльність співробітників по всіх каналах передавання даних. Звичайно, це потребує серверів з великим обсягом пам'яті.

Для пошуку критичної інформації Контур інформаційної безпеки використовує такі технології:

- технологія пошуку за обраними словами з врахуванням морфології;
- технологія фразового пошуку. Містить аналіз документів на наявність фрази з можливими варіаціями додаткових слів;
- технологія пошуку подібних за контентом документів. Працює зі списками слів, фраз, типових документів;
- технологія пошуку за атрибутами документів. Дає змогу шукати документи за їх атрибутами (формат, відправник, отримувач). Можна відстежити активність окремих доменних користувачів, IP-адреси, завдані адреси електронної пошти та ін.
- технологія пошуку нерозпізнаних документів;
- технологія, що поєднує кілька запитів;
- технологія пошуку за регулярними виразами. Технологія дозволяє відстежувати персональні дані, фінансові документи, структуровані записи з баз даних;
- технологія пошуку за цифровими відбитками документів. Передбачає попереднє опрацювання конфіденційних документів.
- технологія пошуку синонімічних форм. Складається словник синонімічних рядів, пошук виконується за співпадінням пар з різних рядів.

Повномасштабний контроль за рухом критичної інформації досягається за рахунок оптичного розпізнавання символів, перехоплення зашифрованих файлів по всіх каналах передавання даних, знаходження файлів зі змінним розширенням.

Розглянуті технології допомагають відстежувати настрій співробітників, їх контакти всередині та зовні компанії. Стає можливим створення груп ризику та відстеження діяльності ненадійних співробітників. В поле зору повинні входити такі співробітники: ті, хто хоч один раз порушив політику інформаційної безпеки; хто зашифровує файли або виконує з ними різні трюки (зашифровані архіви, зміна розширення файлів, велика кількість відсканованих документів); незадоволені співробітники; ті, що почали менш ефективно працювати; ті, хто працює з фінансовими документами.

Технології, що застосовуються всередині локальної мережі, можуть бути поширені і на глобальні мережі. Так, можна відслідкувати позитивне чи негативне ставлення суспільства до якої-небудь

компанії або фірми, політичного діяча та ін. Для цього треба застосувати технологію, що поєднує кілька запитів: пошук за обраними словами з врахуванням морфології (назва фірми) та пошук синонімічних форм. Варто проводити одночасно пошук як негативних відгуків, так і позитивних з подальшим порівнянням їх кількості. Таким чином можна достатньо точно оцінити суспільну думку щодо діяльності фірми чи людини.

За допомогою подібних технологій можна вивчати настрій великих соціальних груп, проводячи пошук за обраним запитом на тих ресурсах, де визначена для досліджень група в основному проводить свій час.

Нещодавно було проведено цікаве дослідження. У 2011 році факультет психології Московського державного університету, Федеральний інститут розвитку освіти та Фонд розвитку інтернету провели дослідження "Пойманные одной сетью: социально-психологическое исследование представлений детей и взрослых об интернет". Вивчалась поведінка молоді (майбутніх працівників з критичною інформацією) в інтернеті, ставлення до ризиків, безпеки спілкування. Було встановлено, що мережа стала звичним містом спілкування, при цьому велика ймовірність втрати відчуття реальності. Доволі часто трапляються випадки підвищеної агресії та немотивованого насильства. Більша частина опитуваних вважає інтернет безпечним середовищем. Підлітки спокійно роздають свої персональні дані. Вони не бачать криміналу в хакерській діяльності й готові майже на все заради прикольної зустрічі.

Змінити своє ставлення до інтернету з погляду інформаційної безпеки сучасні підлітки – майбутні працівники – самостійно не зможуть. На підсвідомому рівні вони не будуть відчувати небезпеки при спілкуванні, коли йтиметься про секрети фірми або таємниці виробництва. Тому зрозуміло, що впровадження систем контролю інформаційних потоків обов'язкове для тих державних чи приватних установ, які пов'язані зі збереженням та обробленням критичної інформації.

Сучасні технології контролю інформаційних потоків можуть надати багато інформації про її рух в інтернеті, вчасно запобігти негативним соціальним наслідкам. Для цього, по-перше, потрібно вирішити вказані питання на рівні держави, а по-друге, сформувати правову базу, яка дасть змогу встановлювати системи контролю на серверах провайдерів та вузлах Інтернет.

## ЛІТЕРАТУРА

1. Курбатов В.А. Руководство по защите от внутренних угроз информационной безопасности / В.А.Курбатов, В.Ю.Скиба. – СПб : Питер, 2008. – 320 с.

2. Контур інформаційної безпеки. Керівництво аудитора безпеки. – 2010, Searchinform [Електронний ресурс]. – Режим доступу : http://searchinform.ru/.



*Яковів І.Б.,*
*кандидат технічних наук,*
*Інститут спеціального зв'язку*
*та захисту інформації НТУУ "КПІ"*


## ПАРАДИГМА КІБЕРБЕЗПЕКИ НА ОСНОВІ АТРИБУТИВНО-ТРАНСФЕРТНОГО ПІДХОДУ ДО СУТІ ІНФОРМАЦІЇ

Створення ефективних систем протидії кібератакам на критично важливі інфраструктури потребує використання конструктивних методів математичної формалізації предметної сфери. Цьому не сприяє невизначеність понятійного наповнення термінів *кібербезпека, кіберпростір, кібернетична загроза, кібернетичний захист* тощо.

Модель кібернетичної системи уточнює суть використання інформаційних процесів в інтелектуальних багатоагентних кібернетичних системах із розподіленим об'єктом управління і дає можливість сформувати ієрархію узгоджених понять у сфері їх безпеки. Модель отримана на основі атрибутивно-трансфертного підходу до суті інформації. Поняття дають змогу застосувати математичний апарат теорії множин.

## ЛІТЕРАТУРА


1. Яловец А.Л. Представление и обработка знаний с точки зрения математического моделирования. Проблемы и решения / А.Л.Яловец. – К. : Вид-во "Наукова думка" НАН України, 2011. – 360 с.

2. Яковів І.Б. Сутність інформації та її теоретико-множинне уявлення / І.Б.Яковів // Спеціальні телекомунікаційні системи та захист інформації : зб. наук. пр. – К. : ІСЗЗІ НТУУ "КПІ", 2011. – Вип. 1(19). – С. 55–58.

3. Яковив И.Б. Канал связи с позиций атрибутивно-трансферной сущности информации / И.Б.Яковив // Інформаційні технології і безпека : зб. наук. пр. – К. : ІСЗЗІ НТУУ "КПІ", 2012. – Вип. 2(2). – С. 31–41.

# ПРОТИДІЯ СУЧАСНИМ ТЕХНОЛОГІЯМ ДЕСТРУКТИВНОГО ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ

*Бухало Л.В.,*

*Рогов П.Д.,*
*кандидат технічних наук*

*Ткаченко В.А.,*
*кандидат військових наук,*
*Національний університет оборони України*

## ПРОБЛЕМИ ОРГАНІЗАЦІЇ ПРОТИДІЇ НЕГАТИВНОМУ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОМУ ВПЛИВУ НА ОСОБОВИЙ СКЛАД ВІЙСЬК (СИЛ)

У теперішній час певна увага фахівцями приділяється проблемам формування та реалізації державної інформаційної політики в умовах використання іноземними державами та іншими суб'єктами інформаційного протиборства нових засобів і методів політичної боротьби, до яких, насамперед, належать операції інформаційно-психологічної війни, що становлять особливу соціальну небезпеку. За кордоном активно розробляється комплекс засобів, що дає змогу здійснювати прямий або прихований інформаційно-психологічний вплив на свідомість та підсвідомість, нервову систему і психічний стан людини [1-4]. У зв'язку з цим можна констатувати, що одне з важливих місць у системі морально-психологічного забезпечення військ належить захисту особового складу від негативного інформаційно-психологічного впливу, який є комплексом дій, що проводяться в мирний та воєнний час державним і військовим керівництвом країни, командуванням, штабами, іншими органами управління та посадовими особами частин (підрозділів) із запобігання, нейтралізації (ослабленню), блокування й усунення наслідків негативного інформаційно-психологічного впливу [5-9]. Саме тому, у своїй структурі захист військ (сил) від негативного інформаційно-психологічного впливу має такі елементи: прогнозування; запобігання; зрив (нейтралізація); ліквідація наслідків його дії [6-9, 11].

При прогнозуванні аналізуються: інформаційно-психологічна обстановка в районах дислокації військ (сил); сили, засоби, рубежі та райони зосередження основних зусиль психологічних операцій противника, їх можливості, спрямованість підривної пропаганди, об'єкти і канали потенційної дії; прогнозований рівень психогенних втрат особового складу від пропагандистського та психологічного впливу противника.

Запобігання негативному інформаційно-психологічному впливу передбачає:

- своєчасне виявлення початку інформаційно-психологічного впливу;

- безперервне об'єктивне, психологічно доцільне інформування особового складу та роз'яснення йому справжніх цілей, завдань, тематики, методів, технічних засобів, а також можливих наслідків дії сторони суперника; надійне перекриття каналів інформаційно-психологічного впливу; розвідку, придушення і знищення сил та засобів психологічних операцій противника;

- визначення та організацію роботи підрозділів (військовослужбовців) зі збирання та знищення матеріалів негативного інформаційно-психологічного впливу противника;

- виявлення психічно нестійких військовослужбовців і проведення з ними індивідуальної психопрофілактичної роботи, організацію в підрозділах (частинах) системи товариської взаємної підтримки і психологічної допомоги;

- ознайомлення військовослужбовців із витонченими прийомами і методами, що використовуються в цілях психологічного придушення індивідуальної та групової свідомості військ (сил);

- оцінювання ступеня уразливості своїх військ (сил) від проявів інформаційно-психологічного впливу, прогнозування наслідків та планування попереджувальних заходів щодо запобігання негативним діям військовослужбовців (зниження психологічної стійкості, рівня бойової готовності, спроби здачі в полон тощо);

- нарощування матеріально-технічної бази засобів інформаційно-психологічного впливу на свої війська (сили) та місцеве населення.

Зрив (нейтралізація) інформаційно-психологічного впливу противника на особовий склад досягається: своєчасною розвідкою, знищенням сил та засобів психологічних операцій противника; рішучим припиненням паніки, чуток, ізоляцією військовослужбовців (підрозділів), що піддалися деморалізації; постійним відстежуванням і підвищенням морально-психологічного стану особового складу; безперервним інфор-

муванням військовослужбовців про зміни обстановки; здійсненням інформаційної взаємодії.

Ліквідація наслідків інформаційно-психологічного впливу передбачає: виявлення військовослужбовців (підрозділів), що піддалися деморалізації, діагностику їх стану і надання психологічної допомоги; виявлення причин виникнення явищ дезорганізації серед особового складу та їх усунення; притягнення до відповідальності розповсюджувачів деморалізуючих чуток, панікерів тощо; аналіз і оцінювання найбільш слабких місць у системі захисту військ (сил) від інформаційно-психологічного впливу; відновлення організованості і боєздатності дезорганізованих підрозділів; вжиття відповідних заходів з оптимізації всієї системи протидії психологічним операціям противника.

З-поміж наявних засобів забезпечення інформаційно-психологічної безпеки можна виділити такі: матеріально-технічні, організаційні, інформаційні, фінансові кошти, правові, кадрові та інтелектуальні. Переведені із статичного в динамічний стан згадані вище засоби стають методами, тобто прийомами, способами дії. Відповідно можна говорити про технічні, організаційні, інформаційні, фінансові, правові, кадрові та інтелектуальні методи забезпечення інформаційно-психологічної безпеки.

Негативний інформаційно-психологічний вплив на військовослужбовців все частіше використовується різними дестабілізуючими силами, що знижує готовність і здатність їх якісно та ефективно виконувати покладені на них завдання. Основними умовами ефективної протидії негативному інформаційно-психологічному впливу є розвиток навичок виявлення, вибору і реалізації техніки та стратегій індивідуальної та групової протидії негативному інформаційно-психологічному впливу; розвиток колективних навичок протидії чуткам і домислам, що дестабілізують і деморалізують морально-психологічний стан особового складу військ (сил).

## ЛІТЕРАТУРА

1. Петрик В.М. Сучасні технології та засоби маніпулювання свідомістю, ведення інформаційних війн і спеціальних інформаційних операцій : навч. посіб. / В.М.Петрик, В.В.Остроухов, О.А.Штоквиш та ін. ; за ред. В.М.Петрика. – К. : Росава, 2006. – 208 с.

2. Литвиненко О.В. Спеціальні інформаційні операції та пропагандистські кампанії / О.В.Литвиненко. – К. : ВКФ “Сатсанга”, 2000.

3. Почепцов Г.Г. Психологические войны / Г.Г.Почепцов. – М. : Рефл-бук, К. : Ваклер, 2000. – 576 с.

4. Крысько В.Г. Секреты психологической войны (цели, задачи, методы, формы, опыт) / В.Г.Крысько. – Мн. : Харвест, 1999.

5. Інформаційна безпека держави у контексті протидії інформаційним війнам : навч. посіб. / за ред. В.Б.Толубка. – К. : НАОУ. – 2004. –179 с.

6. Богуш В. Основи інформаційної безпеки держави: Вступ до спеціальності / В.Богуш, О.Юдін. – Харків : Консум, 2004. – 439 с.

7. Бондаренко В.О. Інформаційні впливи та інформаційні операції / В.Бондаренко, О.Литвиненко. – К. : Стратегічна панорама. – № 4. – 1999. – С. 134–139.

8. Кормич Б.А. Інформаційна безпека: організаційно-правові основи : навч. посіб. / Б.А.Кормич. – К. : Кондор, 2008. - 384 с.

9. Звіт про НДР “Комунікатор - Р” (заключний). - К. : НУОУ, 2012. - 83 с.

10. Алещенко В.І. Проблеми захисту від негативного інформаційно-психологічного впливу противника / В.І.Алещенко, В.Г.Сербін // Математичні машини і системи. - 2010. - № 1.

11. Онищук М.І. Протидія інформаційно-психологічному впливу противника : навч.-метод. посіб. / М.І.Онищук. – К. : НАОУ, 2002. – 36 с.

*Биченок М.М.,*
*доктор технічних наук, професор,*
*Національний університет оборони України*

*Дзюба Т.М.,*
*кандидат технічних наук, доцент,*
*Національний університет оборони України*

*Вітковський В.В.,*
*Національний університет оборони України*

## ФОРМУВАННЯ ЗАХИСТУ ВІД ДЕСТРУКТИВНИХ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ ВПЛИВІВ

Метою будь-якого інформаційно-психологічного впливу (ІПсВ) є зміна свідомості людини як соціального об’єкта. За наслідками впливу виокремлюють два види ІПсВ: конструктивний (позитивний) та деструктивний (негативний). Оскільки го-

ловним об'єктом ІПсВ є людська свідомість, бо саме вона спричиняє діяльність або бездіяльність людини, тому саме через неї проявляється цей вплив і на групову та масову свідомість [1]. Інформаційно-психологічна безпека розглядається як такий стан захищеності свідомості та психіки людини від негативного впливу різноманітних інформаційних чинників, за якого надійно функціонує особистий механізм психологічної адаптації, тобто забезпечується відповідне інформаційно-психологічне сприйняття навколишнього середовища та самого себе як суб'єкта інформаційних відносин.

Віднесення інформаційно-психологічного захисту до окремої проблеми (ІПсЗ) людини має такі об'єктивні причини. По-перше, у результаті глобальної інформатизації суспільства зростають масштаби та ускладнюються зміст і структура інформаційних потоків, суттєво посилюється інформаційний тиск на психіку і свідомість людини. А це потребує формування нових механізмів та способів її виживання в сучасному динамічному інформаційному середовищі. По-друге, взаємодія психіки людини із цим середовищем характеризується різноплановою специфікою, оскільки немає відповідних аналогів в інформаційній взаємодії біологічних і технічних систем. По-третє, центральним об'єктом ІПсВ виступає психіка людини, бо саме від окремих осіб та їх взаємин залежить функціонування соціальних об'єктів та соціо-технічних систем різного рівня складності та структури – від малої соціальної групи (трудового колективу, військового підрозділу) до масових соціальних об'єктів (особового складу збройних сил держави або населення країни).

Основними засобами ІПсЗ людини є механізми внутрішньоособистої опірності [2], які включають базові емоційно-вольові установки. Засоби ІПсЗ проявляються у процесі взаємодії людини з іншими соціальними суб'єктами або інформаційним середовищем чи соціо-технічною системою шляхом запобігання чи нейтралізації загрозливих чинників та факторів, що спроможні завдати шкоди психічному, фізіологічному та духовному здоров'ю. Поширені ситуації, коли людина взаємодіє з іншим суб'єктом не наодинці, а у складі соціальної групи, застосовуючи при цьому різні засоби захисту та протидії негативним ІПсВ [3]. Така група виступає як суб'єкт ІПсЗ окремої особи. Зокрема, це спостерігається у родинах, етнічних громадах, релігійних спільнотах, політичних партіях, громадських організаціях і рухах, фінансово-економічних структурах, органах державної влади тощо. Таким чином, суб'єктами ІПсЗ особи

можуть бути: сама людина з її внутрішніми психо-емоційними можливостями щодо самозахисту; соціальні групи та спільноти, які надають людині підтримку і допомогу колективними психологічними засобами; суспільство та держава, що допомагають людині або підтримують її через діяльність певних соціальних інститутів [4].

Відповідно, виокремлюють три основні рівні організації ІПсЗ: особистий груповий, суспільний. На особистому рівні цей захист реалізується на основі специфічних механізмів емоційно-вольової поведінки, які утворюють систему індивідуального ІПсЗ. На груповому рівні ІПсЗ реалізується за допомогою поширення й використання внутрішньогрупових інформаційних джерел і потоків. На цьому рівні суб'єктами ІПсЗ є соціальні групи та організації (родина, суспільні, політичні, релігійні та інші соціальні об'єднання). На суспільному рівні ІПсЗ реалізується шляхом регулювання й обмеження інформаційних потоків у системі поширення масової інформації, застосуванням відповідних способів, методів і засобів оброблення та оцінювання інформації у процесі соціальної взаємодії. Суб'єктами ІПсЗ на цьому рівні виступають держава та суспільство, які діють через певні соціальні інститути (освіти, виховання, систем моральних норм і культурних цінностей, традицій, соціальних стандартів, медичного забезпечення, соціального захисту тощо).

Для забезпечення ІПсЗ вживаються заходи, які можна об'єднати у такі групи: 1) регулювання інформаційних потоків і зв'язків, або їхнє обмеження; 2) цілеспрямоване інформування, надання повної, релевантної інформації; 3) застосування способів, методів і засобів надання соціально важливої інформації; 4) формування механізмів колективного захисту від негативних інформаційно-психологічних впливів; 5) виховання індивідуальної здатності до інформаційно-психологічного противу.

На особистому рівні вжиття першої групи заходів пов'язане із відмовою людини від використання певної інформації або джерел чи каналів її поширення (наприклад, відмова від рекламної інформації) через перевірку її достовірності.

Друга група заходів пов'язана з організацією інформаційних потоків із метою запобігання й нейтралізації інформаційних впливів, які можуть мати негативні наслідки (наприклад, при виникненні чуток поширюються відомості, що нейтралізують їхній вплив). На особистому рівні це проявляється в ініціативному пошуку додаткової інформації з різних джерел та організації її надходження іншими каналами.

Третя група включає різноманітні форми регулярного надання соціально важливої інформації, зокрема через систему освіти, підготовки та перепідготовки кадрів, поширення духовних і культурних цінностей, підтримки традицій, морально-етичних норм тощо.

Четверта група заходів пов'язана із організацією колективного захисту, який ґрунтується на механізмах ідентифікації людини з певною соціальною групою, зокрема формування позитивного морально-психологічного клімату в колективі, актуалізація відчуття належності до конкретної організації, підтримка лідерів як авторитетних внутрішньогрупових джерел інформації.

П'ята група спрямована на набуття людиною практичного досвіду безпечної інформаційно-комунікаційної взаємодії (наприклад, навчання з використанням спеціалізованих форм психологічної підготовки в особливих умовах, подолання смуги психологічних перешкод та ін.) для формування індивідуального психологічного механізму самозахисту [5].

Важливе значення для формування ІПсЗ також мають особистісні (вік, стать, життєвий досвід, освіта, соціальний статус, майновий стан) та етнічні, етнопсихологічні, ментальні, релігійні або атеїстичні, світоглядні, індивідуально-психологічні, психічні особливості людини та особливості ІПсВ, взаємовплив яких дає прямий або синергетичний ефект [6].

Отже, вибір заходів для формування ІПсЗ безпосередньо залежить від конкретних способів та засобів деструктивних ІПсВ. Системний захист від деструктивних ІПсВ необхідно заздалегідь формувати як у окремої людини, так і у населення, а насамперед – у осіб, які приймають рішення.

## ЛІТЕРАТУРА

1. Жук С.Я. Тенденції та перспективи розвитку інформаційної боротьби й інформаційної зброї / С.Я.Жук, В.О.Чмельов, Т.М.Дзюба // Наука і оборона. – 2006. – № 2. – С. 35–41.

2. Информационная безопасность государства в военной сфере / [Н.Н.Быченок, Т.М.Дзюба, А.А.Рось, В.В.Витковский, В.В.Вищун]. – К. : НУОУ. – 2012. – 264 с.

3. Биченок М.М. Основи інформатизації управління регіональною безпекою / М.М.Биченок. – К. : РНБОУ. – 2005. – 196 с.

4. Уфимцев Ю.С. Методика информационной безопасности / Ю.С.Уфимцев. – М. : "Экзамен", 2004. – 544 с.

5. Горбулін В.П. Проблеми захисту інформаційного простору України / В.П.Горбулін, М.М.Биченок. – К. : РНБОУ, 2009. – 136 с.

6. Вітковський В.В. Спеціальна пропаганда радянських військ на теренах України у роки Великої Вітчизняної війни / В.В.Вітковський // Зб. наук. праць ВІКНУ ім. Т.Шевченка. – Вип. № 35. – К. : ВІКНУ, 2012. – С. 70–82.

*Ваврик Л.В.,*
*Національна академія Служби безпеки України*

## ПСИХОЛОГІЧНІ ОСОБЛИВОСТІ ВПЛИВУ ІНФОРМАЦІЇ НА ПРОФЕСІЙНУ ПОВЕДІНКУ ОСОБИСТОСТІ

Інформація на сьогодні стає одним із важливих ресурсів науково-технічного і соціально-економічного розвитку як суспільства загалом, так і формування фахівця зокрема. Він має бути освіченим та обізнаним щодо ролі, значущості та особливостей інформаційної культури в його професійній діяльності. Інформація професійного змісту впливає на особистість та формує її ставлення до професії. Актуальності набуває проблема визначення психологічних особливостей впливу інформації на фахівця.

Професіогенез особистості у процесі впливу інформації професійного змісту досліджували В.Барко, В.Бодров, С.Бочарова, Г.Запорожцева, Н.Іванова, Л.Кандибович, В.Крайнюк, М.Корольчук, С.Олексієнко, В.Розов, О.Столяренко, В.Сисоєв, О.Тимченко, В.Фармагей, Ю.Шиделко та ін. Водночас, недостатньо вивченими залишаються психологічні аспекти проблеми впливу інформації на поведінку особистості.

Розглянемо психологічні особливості впливу інформації на поведінку фахівця у процесі його професійного становлення.

Як відомо, професійне становлення фахівця починається з етапу професійного відбору й триває у процесі професійної підготовки та діяльності. На цих етапах відбувається зміна особистості фахівця в ході взаємодії з реальною дійсністю та отримання нової інформації, появи фізичних і соціально-психологічних новоутворень у структурі особистості.

Будь-яка професійна діяльність характеризується спрямованістю, наявністю специфічних цілей та конкретними методами та засобами їх досягнення, наявністю специфічних умов діяльності й потребує певної професійної поведінки, яка б дала змогу фахівцю успішно працювати. Професійна поведінка

– відповідна реакція, дії особистості на вплив умов, вимог професійної діяльності та інформації щодо неї.

Пошук та перероблення інформації відбувається на основі індивідуального досвіду фахівця, з урахуванням вимог, умов професії. Вся інформація, що надходить, сприймається з позицій її можливої належності до певних мисленнєвих моделей. Складність процесів виявлення, перероблення та відбору інформації полягає в тому, що вона надзвичайно динамічна. Момент сприймання інформації може бути одночасно й моментом вирішення питання про її значущість як для певної професійної ситуації, так і для особистості фахівця.

Особистість формується, функціонує, розвивається завдяки зовнішнім впливам. Її формування є результатом соціальних впливів із метою створення у неї соціально позитивних, моральних, духовних властивостей і рис, утворення особливих співвідношень усередині психологічної структури особистості. Особистість під впливом необхідної інформації змінює сама себе [4, с. 155].

Крім того, чим різноманітнішими й глибшими знаннями володіє фахівець, тим багатше його сприйняття світу, а отже й формування особистості як професіонала. А розвинуте сприймання, новий чуттєвий досвід є імпульсом для розвитку мислення, оволодіння новими сферами людської практики [3, с. 213].

Водночас, використання людиною будь-якої професійної діяльності неможливе без її інформаційної основи. Останню визначають як сукупність інформації, що характеризує предметні та суб'єктивні умови діяльності відповідно до вектора "метарезультат" [5]. Однією з передумов ефективності професійної діяльності є належність, точність та повнота її інформаційної основи. Важливість інформації для особистості визначатиметься залежно від наявності у неї певної мети, яка потрапляє в інформаційне поле. Інформація сприйматиметься, якщо вона відповідає ціннісним орієнтаціям конкретної особистості й включає такі елементи [1, с.120]:

- когнітивний (пізнавальний) – характеризується сукупністю знань і вмінь;
- емоційний – визначається оцінювальними судженнями і ставленням людини до норм (позитивне, нейтральне, негативне);
- поведінковий (вольовий) – припускає наявність психологічної установки.

Нова інформація, яку сприймає особистість, сприяє формуванню у неї певної системи знань та ставлень, порівняння наявних знань із новою інформацією тощо. При аналізі сприймання особистістю певної інформації слід також враховувати зміст та особливості мислення, пам'яті, уваги, спрямованості. Так, мис-

лення є психічним процесом опосередкованого й узагальненого відображення людиною предметів і явищ об'єктивної дійсності в їх суттєвих властивостях, зв'язках і взаємозв'язках. Основні мисленнєві операції (аналіз, синтез, узагальнення, порівняння, систематизація, абстрагування, конкретизація) дають змогу людині об'єктивно сприймати отриману інформацію й використовувати її у разі необхідності. Такі види мислення, як логічне, критичне, творче, практичне й конструктивне, дають змогу здійснювати власну особистісну оцінку інформації та адаптувати її до своїх індивідуально-психологічних особливостей і практичних потреб професійної діяльності [2].

Значуща інформація запам'ятовується, а за необхідності – відтворюється. Якщо інформація не дуже важлива для фахівця і він її не використовує, то відбувається процес забування інформації. До того ж, важливе місце у сприйманні інформації посідають ціннісні орієнтації, тобто цілі, до яких прагне людина і засоби, за допомогою яких вона їх досягає.

Успішність сприймання інформації залежить від індивідуально-психологічних особливостей самої особистості (від рівня розвитку її мовленнєвого слуху, пам'яті, наявності уваги, інтересу тощо), так і від особливостей інформації (мова, логіка викладу, зрозумілість, обсяг і т. ін.) та наявного досвіду сприймання інформації. Щоб ефективно сприймати інформацію, важливо вміти відсторонитися від власних емоцій, певних переживань і мати розвинену оперативну та довгострокову пам'ять. Сприйнята фахівцем інформація дозволяє йому скорегувати власну поведінку відповідно до вимог діяльності.

Отже, викладене вище дає змогу дійти певних висновків:

- сприйнята особистістю інформація стає знаннями й може корегувати поведінку таким чином, що вона набуде рис професійної;
- отримана інформація, що є значущою для особистості, дає можливість оптимізувати професійну поведінку;
- чим більше фахівець сприймає професійно-значущої інформації, тим більше він прагнутиме корегувати власну професійну поведінку і, тим самим, відповідати вимогам конкретної професії.

## ЛІТЕРАТУРА

1. Бедь В.В. Юридична психологія : навч. посіб. Видання четверте, стереотипне / В.В.Бедь. – Львів : "Новий світ-2000", 2007. – 376 с.

2. Іванова Н.Г. Психологічні аспекти сприймання особистістю інформаційних впливів / Н.Г.Іванова // Інформаційна безпе-

ка людини, суспільства, держави науково-практичний журнал. – 2012. – № 3 (10). – С. 75–79.

3. Психологія : підруч. / [Ю.Л.Трофімов, В.В.Рибалка, П.А.Гончарук та ін. ] ; за ред. Ю.Л.Трофімова. – 6-те вид., стереотип. – К. : Либідь, 2008. – 560 с.

4. Савчин М.В. Загальна психологія : навч. посіб. / М.В.Савчин. – К. : Академвидав, 2011. – 464 с.

5. Шадриков В.Д. Проблемы самогенеза профессиональной деятельности / В.Д.Шадриков. – М. : Изд-во "Наука", 1982. – 185 с.

*Заєць П.М.,*
*Національна академія служби безпеки України*

## АНАЛІЗ МОЖЛИВОСТЕЙ ДОСТУПУ ДО ПЕРСОНАЛЬНИХ ДАНИХ З ВИКОРИСТАННЯМ СОЦІАЛЬНИХ МЕРЕЖ

Світова мережа Інтернет стрімко розвивається. Так, в Україні кількість постійних користувачів вже досягла 20 млн серед населення, старшого 15 років.

Використання соціальних мереж та спілкування становить: кілька разів на день – 34 %,один раз на день – 24 %, кілька разів на тиждень – 18 %, рідше трьох разів на місяць – 16 %, ніколи – 8 %. Таким чином, 92 % користувачів інтернету України використовують соціальні мережі.

Загальна кількість облікових записів у соціальних мережах українських користувачів налічує близько 30 млн, деякі користувачі мають по кілька реєстраційних записів.

Згідно даних дайджеста Уанета, складеного Prodigi, в топ-5 мереж по місячній аудиторії Уанета на кінець минулого року увійшли: "ВКонтакте" – 9 млн користувачів, "Одноклассники" – 4,8 млн; МойМир@Mail.ru – 3,1 млн; Facebook – 2,1 млн і "Фотострана" – 1,1 млн.

Місця спілкування привертають увагу багатьох людей, більшість яких перебувають у щасливому невіданні про необхідність захисту свого комп'ютера, оскільки тут також полюють кіберзлочинці, що підстерігають необачного користувача і чекають на свою жертву.

На жаль, більшість користувачів вкрай зневажливо ставляться до тієї інформації, яку вони виставляють на загальний огляд. Наслідки цього можуть бути самими різними: особисті проблеми, проблеми на роботі, можливість бути пограбованим і навіть небезпека втрати життя.

Розглянемо типові помилки користувачів щодо розміщення інформації про себе.

1. Паролі та логіни

Як це не парадоксально, але соціальні мережі часто використовуються для зберігання та обміну логінами і паролями. Більше того, часто користувачі добровільно віддають пароль від самої соціальної мережі. Якщо обставини змушують віддати пароль, обов'язково змініть його, як тільки це стане можливим.

2. Кодові слова і фрази

Відповіді на кодові питання, які ви використовуєте для відновлення забутих паролів, також не слід зберігати в соціальних мережах. Це дивно, але більшість користувачів навіть не замислюються над цим, коли вносять в профіль дівоче прізвище матері або школу, де вони навчалися. Адже відповіді на ці питання і є ті самі популярні ключові фрази, використовувані для відновлення облікових записів або при зверненні, наприклад, у банк.

3. Персональні повідомлення

У соціальних мережах люди можуть обмінюватися повідомленнями, публікуючи записи, зображення і відео на так званій "стіні". Пам'ятайте, що "стіну" бачать і інші користувачі мережі, так що ніколи не "вішайте" туди повідомлення особистого характеру. Часто буває так, що інформація, яка здається вам підходящою для "стіни", може нашкодити адресатові. Тут немає універсальних рекомендацій, просто майте це на увазі.

4. Адреса і телефон

Ніколи не залишайте у відкритому доступі вашу домашню адресу і телефон. Зловмисники будуть знати, де вас шукати, особливо, якщо запідозрять, що вас не буде вдома в певні години. Дізнатися про це можна з ваших же повідомлень – цьому присвячений наступний пункт.

5. Плани на найближче майбутнє

Не варто ділитися з усім світом вашими планами на вечір або вихідні. Цілком можливо, що цією інформацією зацікавиться той, хто зможе скористатися вашою відсутністю в одному місці або, навпаки, присутністю в іншому.

6. Персональна фінансова інформація

Ваш добробут не повинен стосуватися нікого, крім вас. Тому краще уникати навіть натяків на те, скільки ви заробляєте, коли отримуєте зарплату, де зберігаєте заощадження або як часто відвідуєте банкомат. На перший погляд у цьому немає нічого небезпечного, але тільки доти, доки ви не зіткнетеся з тим, хто знає, як випадково залишені повідомлення перетворити в безцінні.

7. Інформація про компанію

За статистикою компанії Sophos, що займається питаннями інформаційної безпеки, близько 63 відсотків організацій побоюються, що їх співробітники можуть викласти в мережу цінну інформацію, яка стосується, наприклад, планів з розвитку бізнесу та інше. Не варто підводити свого роботодавця.

8. Фотографії дітей

Виставлення фотографій ваших дітей у відкритому доступі також може становити небезпеку. І мова тут йде не тільки про педофілів, які можуть використовувати їх у своїх цілях. Цей пункт тісно переплітається з пунктом 4, якщо, ви залишаєте повідомлення про те, що будете відсутні на вихідних, а вдома залишається тільки дитина (фотографія якого доступна в галереї), то його безпека може опинитися під великою загрозою.

9. Пам’ятайте про агрегатори

Майте на увазі, що інформація з вашого профілю, в тому числі і закрита для випадкових відвідувачів, може бути агрегована іншими сервісами.

10. Не публікуйте нічого, що не хочете щоб знали інші.

Цей пункт випливає з попереднього. Пам'ятайте, що навіть якщо налаштування приватності вашого профілю “викручені” на максимум, немає ніякої гарантії, що опублікована вами інформація не вийде за його межі. Досить сказати, що згідно з дослідженнями Університету штату Вірджинія, 90 відсотків додатків для Facebook, що входять до топ-150 за популярністю, мають доступ до вашої конфіденційної інформації. Навіщо вона їм – можна тільки здогадуватись. Але це прекрасна ілюстрація того, що абсолютно будь-які дані, які знаходяться в Інтернеті, можуть бути отримані сторонніми особами при належному старанні.

Яким чином ваша персональна інформація може стати доступною стороннім особам, знаходячись у середовищі соціальних мереж?

По-перше, необмірковані дії самого користувача, а саме: неправильне налаштування політики безпеки інтернетівського браузера; ігнорування антивірусним ПЗ; додача в “друзі” неперевірених користувачів; запуск різноманітних програм-додатків, які можуть бути шкідливим ПЗ.

При цільовому (замовному) отриманні доступу до вашого аккаунту імовірність захисту практично нульова. Для злому вашого аккаунту не треба бути фахівцем, в інтернеті безліч навчального матеріалу як можна зламати аккаунт. Якщо ж справа потребує більш кваліфікованої роботи на допомогу прийдуть хакери. Виконання подібних робіт поставлено на потік, так це бізнес. Пропозицій на надання подібних послуг дуже багато, а ціни, відповідно, низькі в межах від 30 доларів.

Також існують програми, які дають змогу збирати та аналізувати отриману інформацію з соціальних мереж як відкриту, так і приховану.

Програми парсери – це програми для автоматизації процесу парсингу, тобто оброблення інформації за певним алгоритмом. До таких можна віднести Content Downloader, Human Emulator, Datacol та багато інших. Також можна замовити програму парсингу під конкретну задачу, ціна також невелика від 35 доларів.

Неодноразові спроби влади отримати повний доступ до акаунтів соціальних мереж начебто був відхилений, але фахівці з інформаційної безпеки давно попереджали, що власті можуть почати використовувати соціальні мережі із високотехнологічним стеження за громадянами. Схоже, що вперше з’явилися докази подібних дій. Видання Guardian отримало в своє розпорядження відеозапис презентації програмного забезпечення під назвою RIOT (Rapid Information Overlay Technology), яке розробив американський військовий підрядчик Raytheon ще в 2010 році. Це система, створена для швидкого витягання інформації про підозрюваних громадянах із соціальних мереж, в тому числі Facebook, Twitter і Foursquare та інших. Буквально кількома натисками миші слідчий отримує відомості про активність підозрюваного: про його соціальні контакти, карти переміщень та інше. Інформація витягується в тому числі з EXIF-заголовків фотографій, опублікованих у особистих фотоальбомах на різних сайтах. Подібні проекти використовуються й іншими державами.

Єдине до чого закликаємо, так це, щоб кожен із вас якомога серйозніше ставився до інформації, яку публікує в мережі Інтернет, і в загалі чи потрібно її там публікувати.

*Єрьоменко А.В.,*
*Експерт з впровадження АСУ ГІС Асоціації України*

*Черненко О.Є.,*
*Департамент ГІС Асоціації України*

# ПРОГНОЗУВАННЯ РИЗИКІВ ПРИ СТРАТЕГІЧНОМУ ПЛАНУВАННІ

У сучасному суспільстві, яке ми визначаємо як інформаційне, плани стабільного існування, заходи, спрямовані на зміцнення держави та громадянського суспільства – усе, що безпосередньо залежить від якісного прогнозування ризиків при стратегічному плануванні, є результатом вибору методів, інструментів та індикаторів, які дають змогу робити висновки високого рівня відповідності.

Світ, в якому об'єктивно існує сьогодні українське суспільство швидко змінюється. Ця обставина настільки вагома, що навіть відображена у зреченні від престолу Папи Римського Бенедикта XVI: "*Однак, у сьогоднішньому світі, який так швидко змінюється і ставить під сумнів віру, щоб нести слово Боже, необхідні сила як духа, так і тіла*" [1].

Відповідно, зростає роль аналітичного прогнозування, роль застосування таких експертних рішень і систем, які максимально враховують об'єктивно існуючі фактори та дають змогу передбачати наслідки запланованих дій у ситуаціях, які можуть змінюватись непередбачувано.

Наша ціль – розглянути роль інформаційно-психологічної безпеки в процесі розроблення перспективних планів стабільного існування з урахуванням прогнозів ризиків та загроз, властивих сучасному інформаційному суспільству.

Мета доповіді – розглянути доцільність аналізу культурно-історичної традиції (КІТ) як дієвого індикатору для визначення стану суспільства, спільноти, етнічної чи релігійної громади. Ціль застосування такого індикатору – виявлення існуючих ризиків та запобігання загрозам при стратегічному плануванні.

*Характеризуючи проблему самосвідомості, та, відповідно, культурної ідентичності, як проблему важливого життєвого значення, ми зараховуємо її до розряду найважливіших, найвищих цінностей дієздатної свідомої особи.*

Ефективним інструментом, в такому контексті, є, на наше переконання, використання аналізу КІТ спільнот і держав, для підвищення ефективності виявлення ризиків при прогнозуванні.

Тобто, саме КІТ виступає тим надійним маркером, який дає змогу складати прогнози високого ступеня точності, або виступати ефективним аналітичним інструментом у разі необхідності прийняття відповідальних рішень у ситуації невизначеності.

Фундаментальною якістю будь-якого людського суспільства є здатність створювати та успадковувати об'єкти матеріальної культури і створювати різні події, які сприймаються як прояви відповідного суспільного рівня культури. Культурно-історична традиція в цьому контексті розуміється як наслідування культури, як універсальна характеристика людського способу бути.

Для сучасних держав характерна множинність традицій, одночасно існуючих у суспільстві. Елементи різних традицій у діяльності суб'єктів утворюють різноманітні поєднання. Будь-який елемент культурно-історичної традиції, успадкований навіть з далекого минулого, включається в нові системні зв'язки і навіть будучи сам по собі незмінний, має в собі не тільки сліди свого походження, але й свого руху крізь час аж до сьогоднішнього дня.

Ми можемо виділити головну характеристику закономірностей успадкування культурно-історичних традицій, характерну для суспільств сучасного типу: *опосередкованість свідомістю і діяльністю соціальних груп як суб'єктів культурно-історичної дії.*

Потрібно відзначити, що поняття КІТ поширюється не на увесь масив спадщини, а на виокремлені його частини. *Принцип виокремлення КІТ – це принцип, що виходить завжди зі світу цінностей*. Сукупність спадщини становить безліч фактів. Традиція ж є тільки там, де приймається до уваги реальне бажання суб'єкта, його індивідуальний цілеспрямований осмислений вибір, його громадянська позиція у ставленні до цих фактів. Саме в цьому контексті ми розуміємо вислів Понтифіка, Папи Римського Бенедикта XVI:

"*… у сьогоднішньому світі, який так швидко змінюється і ставить під питання віру, … необхідні сила як духа, так і тіла*" [1].

Так, типологічне поняття "культурно-історична традиція" ми відносимо до способу людини діяти стосовно спадщини. Власне, традиція – це сукупність фактів спадщини, які станов-

лять цінність для суспільства і безпосередньо відображені в державній політиці.

Саме такий спосіб успадкування КІТ в сучасності. Сукупність спадщини становить безліч фактів. Традиція ж є тільки там, де беруться до уваги результати дій суб'єктів сучасного історичного процесу, їх ставлення до цих фактів.

Традиція дає змогу успадковувати "через покоління", відновлюючи те, що було дієвим в поколінні дідів і існувало латентно або зовсім припинило існувати в поколінні батьків. Традиційні цінності мають характер практичного ідеалу, зразка, відповідно до якого суб'єкт формує себе і, погодившись з якими, діє у світі. Ціннісне ставлення передбачає вибір з безлічі об'єктивно можливого й існує завжди як система взаємопов'язаних цінностей. Через "призму" системи цінностей суб'єкт бачить поле своєї практичної діяльності в об'єкті: що йому важливо, категорично не прийнятно, куди він направить свої зусилля, що залишить без уваги.

Підставу раціоналізації КІТ ми вбачаємо в *універсальній для будь-якого суспільства ідеї* – "*системі загального життя*" *з предками*. Система загального життя народжується в переживанні почуття любові. "*Любов до предків*" *– зовсім не риторична фраза, це реальне і дуже сильне переживання, характерне для різних вимірів міжособистісних відносин*.

Превентивні дії з упередження щораз більших загроз повинні мати потужний аналітичний індикативний та практичний механізми, введення в дію та застосування яких має бути відпрацьовано буквально до автоматизму.

Застосування аналізу КІТ як дієвого індикатора для визначення стану суспільства та характеру ситуації дасть змогу, на нашу думку приймати рішення та діяти впевнено, вчасно, якісно виконуючи поставлені завдання.

## ЛІТЕРАТУРА

1. Офіційний текст оголошення про зречення від престолу Папи Римського Бенедикта XVI [Електронний ресурс]. – Режим доступу:
http://ipress.ua/articles/ofitsiynyy_tekst_ogoloshennya_papy_rymskogo_pro_zrechennya_vid_prestolu_15461.html.

*Івасишина Т.А.,*
*кандидат філологічних наук, доцент,*
*Національна академія Служби безпеки України*

# КОМУНІКАТИВНО-КОГНІТИВНИЙ ПОТЕНЦІАЛ ЛЕКСЕМИ В КОНТЕКСТІ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ

Становлення глобального комунікативного простору, яке впливає на всі сторони життя суспільства, як ніколи раніше порушує питання про особливу роль мови у визначенні буття. Оскільки найважливіші знання про світ та про себе людина отримує на основі дискурсивного мислення, роль мови як найважливішого засобу пізнання набуває неабиякого значення.

У сучасному науковому просторі спостерігається переосмислення багатьох усталених світоглядних парадигм, одна з яких стосується передусім сили слова. О.Потебня розглядав мову як активний процес, що розкриває ставлення людини до навколишнього світу й реалізується завдяки зв'язку мови та думки, відповідно, мислення – пізнання. Таке відображення дійсності реалізується через слово – одиницю мови, яка складається зі звукової частини, внутрішньої форми та значення. На погляд О.Потебні, слово – це не зовнішній додаток до вже готової в людській душі ідеї необхідності. Воно виступає засобом створення цієї ідеї, що випливає з глибин людської природи, бо лише за його допомогою структурується думка. Як у слові вперше людина усвідомлює свою думку, так у ньому ж насамперед вона бачить ту закономірність, яку відкриває у світі. Подібне тлумачення дає філософ М.Максимович, зауважуючи, що людина може трьома основними способами виражати своє внутрішнє життя, один із них – слово, що є найповнішим і найближчим душі способом її вираження, в якому немає однобічності ні образу, ні звука, проте в якому обидва злиті в досконалість, первородну єдність та цілісність.

У філологічних науках спостерігається підвищена зацікавленість Біблією як перехрестям дискурсів, так званою, особливою картиною світу. Як зауважує І.Огієнко, "тут кожний вираз відповідальний, тут кожне слово має своє особливе значення". Потенціал слова визначає й релігійна картина світу, в якій слово – це сама сила творіння "І сказав Бог: Хай станеться світло! І

настало світло" (Бут. 1:3); "Спочатку було Слово, і Слово було в Бога, і Слово було Бог. Воно в Бога було споконвіку. Усе через Нього постало, і ніщо, що постало, не постало без Нього" (Йоан. 1:1-3). Слово виступає тією первинною формою, в якій зберігається сила буття; саме у слові Христа реалізує себе основа притаманної всім людям Божественної свідомості. Це зумовлює розуміння кожної мовленнєвої фігури посередництвом тієї сили, що спільна для будь-якої свідомості.

На думку О.Потебні, слово потрібне душевній діяльності для того, щоб вона могла стати свідомою. Дух без мови неможливий, оскільки сам утворюється за допомогою мови. Недаремно В. фон Гумбольдт не міг відмовитися від метафізичного погляду, перенісши питання на психологічне підґрунтя своїми визначеннями мови як діяльності, роботи духу як органа думки. З огляду на зазначене мова постає найскладнішим феноменом.

Серед низки функцій мови мовознавці визначають як основні (базові) комунікативну та гносеологічну (А.Білецький, М.Кочерган), відповідно слово, посередництвом якого реалізуються ці функції, постає реалізатором самого комунікативного процесу і водночас механізмом творення думки.

Проте потенціал лексеми полягає не лише в утворенні думки та її реалізації, це, відповідно, позначення предметів і явищ буття, формування почуттів, виклик певних емоцій, вираження настроїв, а також пам'ять та навіть передбачення. Прояснення останніх формує категорію часу в мові.

Отже, лексеми ми можемо сприймати як знаки знаків, як знаки уже відомих понять, що сприяє розумінню нового в системі наявних концептів. Маніпулюючи словами як засобами мови, суб'єкт маніпулює значеннями, будує смислові структури, виходячи таким чином за межі актуального досвіду, розширюючи горизонти картини світу. Завдяки такій природі слова його можна вважати основним засобом інформаційного-психологічного впливу, що може реалізовувати всі, без винятку, функції мови.

*Кузьменко А.М.,*
*кандидат юридичних наук,*
*КУП НАН України*

# РОЛЬ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ ЗАХОДІВ У ЗАБЕЗПЕЧЕННІ МІЖНАРОДНОЇ БЕЗПЕКИ В ЕПОХУ ГЛОБАЛЬНОГО ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

Актуальність теми зумовлена тим, що дослідження процесів сучасного світового розвитку констатують, що нині ми спостерігаємо новітнє явище, назва якому “глобалізація”. Серед різних напрямів цього складного та мало дослідженого процесу одне із провідних місць займає інформаційна глобалізація, котра зумовлює навіть цілий епохальний суспільний зсув – перехід від постіндустріального розвитку людства до формування глобального інформаційного суспільства. У зазначених умовах спостерігається трансформація світового правопорядку на принципово нові засади. У цьому контексті цікавим є особливості перетворення концептуального мислення геостратегів і військових щодо місця і ролі техногенно-силових методів війни на користь вжиття інформаційно-психологічних заходів війни як найраціональнішої форми реалізації зовнішньої політики в нових умовах конфліктної взаємодії на міжнародній арені. Мета доповіді – визначити особливості формування наукової думки про доцільність переходу від практики застосування техногенно-силових методів реалізації зовнішньої політики щодо конкурентів, противників і ворогів до інформаційно-психологічних заходів війни. Завдання – довести до наукового співтовариства останні результати проведених автором досліджень еволюції зниження пріоритетності застосування заходів техногенно-силової війни і підвищення значення заходів інформаційно-психологічної війни в реалізації зовнішньої політики щодо конкурентів, противників і ворогів у так звану “постбіловезьку епоху”.

У роки “холодної війни” сформувалося не лише теоретико-прикладне уявлення про спеціальні інформаційно-психологічні заходи як складові елементи забезпечення сприятливих умов для реалізації заходів техногенно-силової війни, а й у військових колах, у представників спецслужб і наближених до них політиків утвердилася впевненість про доцільність в умовах процесу інформаційної глобалізації та формування світового інфо-

рмаційного суспільства виокремити інформаційно-психологічний компонент із арсеналу класичної техногенно-силової війни і надати йому в міжнародних відносинах статусу окремого самостійного виду міждержавної, міжкоаліційної війни. Досвід блокового протистояння "Схід – Захід" доводить, що стратегія військової експансії щодо подолання могутності світових конкурентів безперспективна з різних причин: 1) можливість взаємного ядерного знищення; 2) економічна нерентабельність; 3) морально-етичне неприйняття нинішньою світовою спільнотою фактів агресії; 4) окупації та анексії іноземної території тощо. Відбувався пошук, яким чином знайти замінники негативним чинникам техногенно-силової війни. Таким чином, теоретичні напрацювання ідеологів інформаційно-психологічного протиборства та практика спецслужб у сфері реалізації спеціальних таємних операцій почали домінувати над силовими методами розв'язання геостратегічних, геополітичних і геоекономічних проблем між визначеними світовими центрами сил. Проте в теорії міжнародного публічного права залишилося хибне уявлення про Право міжнародної безпеки як вузько спрямовану систему принципів і норм, котрі регулюють військово-політичні відносини держав та інших суб'єктів міжнародного права з метою запобігання застосуванню військової сили в міжнародних відносинах, відвернення техногенно-силової війни через обмеження та скорочення озброєнь. На жаль інші аспекти із сфери міжнародно-правових безпекових питань нинішнім правом міжнародної безпеки не охоплюються. В реальності поряд зі змінами, котрі відбуваються у розумінні сучасної змістовної сутності системи небезпек, ризиків, викликів і загроз, відбулися зміни у ставленні до змістовної сутності самого поняття безпека.

По-перше, нині переважна більшість безпекознавців визнає, що на першому місці має бути не стан захищеності від небезпек і т. ін., а процес безпекотворення. Отже, всі об'єкти захисту, без винятку, – фізичні особи, національні суспільства, держави та міжнародні співтовариства, – мають бути залучені до активної діяльності у сфері безпеки, спрямованої на здійснення цільового вигідного впливу (кожен на своєму рівні) на чинники небезпек, ризиків, викликів і загроз з метою запобігання матеріалізації можливого уявного, а з плином часу й градації рівня небезпек поступово більш матеріалізованого і, насамкінець, виникнення безпосередньої шкоди чи збитку об'єктам захисту – людині, національному суспільству, державі, міжнародному спів-

товариству. Процеси євроінтеграції, міждержавного співробітництва та глобалізації відчутно наштовхуються на прояви суперечливих дезінтеграційних тенденцій у різних регіонах світу. Саме це зумовило потребу у створенні нової цілісної системи безпеки, світового правопорядку, де елемент правового забезпечення має зайняти домінуючі позиції. Тут йдеться про міжнародне право, а саме про її складову – право міжнародної безпеки в оновленому вигляді, яке повинно бути всеохоплюючим та зачіпати багато питань і сфер суспільного життя держави та світового співтовариства. Сучасна міжнародна безпека має виключати із системи міждержавних відносин ідеологічну і класову боротьбу, котра природно відбувається у формі інформаційно-психологічного протиборства. Політика, особливо світова політика, основою якої є сукупність зовнішньої політики окремих держав, переводить інформаційно-психологічне протиборство із стану змагання між різними уявленнями про теоретичну суспільно-політичну модель міжнародних відносин у форму інформаційно-психологічної війни як стан і процес конфліктогенної взаємодії.

По-друге, у цьому випадку зброя та інші засоби техногенно-силової війни не можуть бути гарантом вирішення політичних, економічних, ідеологічних та будь-яких інших проблем і спірних питань. Також слід зауважити, що міжнародна безпека має забезпечити рівність прав кожної держави, стимулювати партнерські відносини та конструктивний спосіб вирішення різного роду міждержавних суперечностей, враховуючи територіальну цілісність і непорушність кордонів, не допускати навіть теоретичної можливості погроз силою та застосування сили. Принципи і норми міжнародної безпеки тісно переплітаються з принципами та нормами решти галузей міжнародного права, що створює міцний захист і правопорядок між державами. Для забезпечення міжнародної безпеки найважливішим є створення системи колективної безпеки регіонального та глобального рівнів, як універсального, так й вузькоспеціалізованого характеру, котрі мають забезпечувати рівну і загальну безпеку.

## ЛІТЕРАТУРА

1. Кузьменко А.М. Актуальні проблеми Права міжнародної безпеки епохи глобалізації: інформаційно-психологічна війна / V Наукові читання, присвячені пам’яті В.М.Корецького (21 лютого 2013 р., м. Київ) : зб. наук. праць : Київський університет права НАН України [редкол. : Ю.С.Шемшученко,

Ю.Л.Бошицький, О.В.Чернецька та ін.]. – К. : Вид-во Ліра-К, 2013 р. – С. 40−52. – Режим доступу до сайту “Моя політика” : http://www.mypolicy.com.ua/.

2. Кузьменко А.М. Актуальні проблеми сучасної парадигми права міжнародної безпеки та шляхи їх вирішення / А.М.Кузьменко // Сучасні проблеми правової системи України : зб. матер. ІІ Міжнародної наук.-практ. конференції (28 жовтня 2010 р., м. Київ) Київського університету права НАН України; [редкол. : Ю.С.Шемшученко, Ю.Л.Бошицький, О.В.Чернецька та ін.]. – Вип. 2. – К. : Вид-во Європейського університету, 2010. – С. 75–80. – Режим доступу до сайту “Моя політика” : http://www.mypolicy.com.ua/.

3. Кузьменко А.М. Війна в умовах глобалізації: міжнародно-правові та безпекознавчі аспекти / А.М.Кузьменко // Законодавство України: проблеми та перспективи розвитку : зб. наук. пр. XII Всеукраїнської наук.-практ. конф. / Київський університет права НАН України [редкол. : Ю.С.Шемшученко, Ю.Л.Бошицький, О.В.Чернецька та ін.]. – К. : Вид-во Європейського університету, 2011. – С. 449–459. – Режим доступу до сайту “Моя політика” : http://www.mypolicy.com.ua/.

*Камінник І.С.,*
*Міністерство соціальної політики і НАН України*

## ЗАБЕЗПЕЧЕННЯ КОНСУЛЬТУВАННЯ З ГРОМАДСЬКІСТЮ ТА УЧАСТЬ ГРОМАДСЬКИХ ОБ’ЄДНАНЬ У ПРИЙНЯТТІ ПОЛІТИЧНИХ РІШЕНЬ

Розвиток Україн як демократичної держави європейського типу неможливий без функціонування двох взаємопов’язаних важливих чинників: розвитку громадянського суспільства як гарантії демократичних перетворень та реформування соціальної сфери із залученням недержавного сектору в реалізації сучасної, ефективної соціальної політики.

Важливими завданнями недержавних організацій є надання якісних та економічно ефективних соціальних послуг, у тому числі таких, які не можуть забезпечити ні держава, ні комерційні організації. Країни розвиненої демократії системно залучають громадян та їх об’єднання до формування та реалізації соціальної політики. Це дає змогу звільняти державу від реалізації окремих надмірно обтяжливих для неї соціальних завдань із

збереженням високих соціальних стандартів для населення. Децентралізація та роздержавлення соціальної сфери є важливою умовою створення ефективної системи соціального захисту та соціального обслуговування населення.

Сьогодні недержавний сектор у сфері надання соціальних послуг поступово стає рівноцінним партнером держави у впровадженні ефективної державної політики щодо соціального захисту та соціального обслуговування населення. Важливим інструментом реалізації соціальної політики може стати механізм Громадських рад, який регламентується Постановою КМУ від 3 листопада 2010 р. № 996 "Про забезпечення участі громадськості у формуванні та реалізації державної політики" [1]. Проте практика реалізації цього механізму показує, що необхідні доопрацювання та удосконалення.

## ЛІТЕРАТУРА

1. Постанова Кабінету Міністрів України від 3 листопада 2010 р. № 996 "Про забезпечення участі громадськості у формуванні та реалізації державної політики" [Електронний ресурс]. – Режим доступу : http://zakon1.rada.gov.ua/laws/show/996-2010-%D0%BF.

*Мельник О.В.,*
*ГІС асоціація України*

*Прокоф'єва К.О.,*
*ГІС Асоціація України*

## АНАЛІЗ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ РИЗИКІВ ФУНКЦІОНУВАННЯ ОБ'ЄКТІВ ПОДВІЙНОГО ПРИЗНАЧЕННЯ

Мета виступу – висвітлити питання, які потребують дослідження та визначення в нових умовах, які фактично існують сьогодні. Розглянути можливості аналізу та прогнозування ризиків при середньо- та довготерміновому плануванні використання об'єктів подвійного призначення [1, с. 22].

Двадцять перше століття продемонструвало нові, раніше не відомі, характеристики війн та локальних конфліктів на прикладі Косово, Росії (Друга Чеченська війна), Афганістану, Лівії,

Сомалі, Малі. Ми хочемо виокремити кілька відмінностей, характерних для цих конфліктів останнього покоління.

По-перше, у війнах останнього покоління полем бою є вся територія зони конфлікту, все суспільство проти якого противник веде війну. У цих умовах розосередження, а також, підвищення значимості дій дуже маленьких груп, вимагають від бойових одиниць навіть самого нижнього рівня гнучких дій на основі знання і розуміння намірів вищого командування, їх взаємодії з керівництвом цивільних адміністративно-територіальних утворень.

По-руге – це зниження залежності від централізованої системи логістики. Розосередження у купі зі зростаючим значенням швидкості, потребує високого ступеня готовності до того, щоб підтримувати існування та боєздатність за рахунок навколишньої місцевості і противника, залучення ресурсів цивільного сектора, взаємодії з суб'єктами господарювання.

По-третє, – ключовою ідеєю стала спрямованість дій на досягнення внутрішнього колапсу сил противника, а не на їх фізичне знищення. У число цілей для враження входять такі "речі", як підтримка бойових дій населенням, стан екосистем, релігія та культура противника. Величезну важливість має точна ідентифікація стратегічних джерел ворожого бойового потенціалу.

По-четверте, – психологічні операції у формі медійно-інформаційного втручання стають фактично переважаючою оперативною і стратегічною зброєю. "Логічні бомби" і комп'ютерні віруси можуть бути використані для зриву як військових, так і цивільних операцій. Протиборчі сторони у війнах останнього покоління стали настільки майстерними в маніпулюванні ЗМІ з метою зміни громадської думки в країні і у світі, що вміле застосування психологічних операцій іноді вже робить зайвим введення в дію бойових підрозділів. Найважливішим об'єктом впливу є підтримка населенням свого уряду і війни та дій гуманітарного характеру, які цей уряд проводить. Телевізійні новини або звернення релігійних лідерів фактично стали більш потужною зброєю оперативного призначення, ніж бронетанкові дивізії.

Загалом, майбутні військові дії останнього покоління, ймовірно, будуть найвищою мірою розосередженими й не визначеними; межа між миром і війною буде розмита аж до повного зникнення. Війна буде нелінійною в такій мірі, що, цілком мож-

ливо, в ній буде ускладнена точна ідентифікація поля бою і лінії фронту. Різниця між “громадянським” і “військовим” контингентами, ймовірно, зникне. Дії будуть одночасно направлені на всю “глибину” території сторін, які беруть участь у протиборстві, включаючи усе їх суспільство, що розуміється не тільки в його фізичному, але і в екологічному і в культурному та релігійному аспектах. Великі військові об’єкти, такі як аеродроми, стаціонарні вузли зв’язку і крупні штаби стануть рідкістю по причині їх вразливості; те ж саме, ймовірно, торкнеться і їх громадянських еквівалентів, таких як урядові резиденції, електростанції і промислові майданчики (це стосується не тільки обробної промисловості, але і “економіки громадянського сектору”, наприклад, – виробництва добрив і сільського господарства). Успіх залежатиме від ефективності спільного управління цивільним і військовим секторами, оскільки лінії розподілу між задачами та відповідальністю військового і цивільного керівництва виявляться не визначеними.

У таких умовах введення сил і засобів МНС у структуру МО України є обґрунтованим і своєчасним. Відповідно, важливого значення набуває точна ідентифікація об’єктів подвійного призначення, актуальними стають питання їх ресурсного забезпечення, формування, зберігання та використання як самого середовища проживання, так і стратегічних резервів життєзабезпечення.

Ідентифікувати об’єкти господарчого комплексу та природні ресурси як такі, які мають подвійне призначення ми пропонуємо за ознаками їх одночасного використання (військового та цивільного) під час подолання наслідків природних і техногенних катастроф та використання в ході військового протиборства. Відповідно, до об’єктів подвійного призначення пропонуємо відносити: електрогенеруючі потужності та мережі, об’єкти видобутку, транспортування, переробки та зберігання вуглеводнів, засоби зв’язку та ЗМІ, об’єкти водогосподарського комплексу, об’єкти транспортної інфраструктури, об’єкти санітарно-епідеміологічного та медичного призначення, релігійні та культові споруди.

Із метою прогнозування ризиків, формування стратегічних резервів та оперативного управління об’єктами подвійного призначення ми пропонуємо застосовувати ГІС з метою точного відображення в просторі факторів ризиків та загроз, процесів, які забезпечують життєдіяльність та стабільний розвиток.

## ЛІТЕРАТУРА

1. Сучасні перспективи застосування ГІС-технологій у роботі санітарно-епідеміологічної служби МО України. Геоінформаційні системи та інформаційні технології у військових і спеціальних задачах. “Січневі ГІСи”. / А.А.Кожокару, О.М.Іванько, А.В.Рожков, О.В.Мельник : збірка матеріалів, статей, доповідей і тез третього науково-практичного семінару, 27-28 січня 2012 року. – Львів : АСВ, 2012. – 288 с.



*Онищук М.І.,*
*кандидат історичних наук, доцент,*
*ВІ КНУ ім. Тараса Шевченка*


## ІНФОРМАЦІЙНИЙ ТЕРОРИЗМ ЯК СУЧАСНЕ СОЦІАЛЬНО-ПОЛІТИЧНЕ ЯВИЩЕ

Тероризм стає все більш масштабним соціально-політичним явищем, що становить серйозну загрозу безпеці та життєво важливим інтересам як особи, так і суспільства. Сучасний тероризм істотно відрізняється від використання терористичної тактики екстремістськими групами у минулому.

Тероризм як складне, багатоаспектне негативне соціально-політичне явище давно переріс національні рамки і перетворився на масштабну загрозу для безпеки всього людства. Ця проблема ускладнюється ще й тим, що тероризм акумулює в собі соціальні протиріччя, що досягли в нашому суспільстві рівня багатостороннього конфлікту. Інформаційна епоха розширила сферу діяльності тероризму, що призвело до появи “інформаційного тероризму”, який визначається як злиття фізичного насильства зі злочинним використанням інформаційних систем, а також умисне зловживання цифровими інформаційними системами, мережами або їх компонентами для здійснення терористичних операцій або акцій.

Становлення феномену інформаційного тероризму як самостійного явища пов’язане з появою і розвитком високих технологій у другій половині XX століття, хоча поняття тероризму як механізму насадження загальної паніки і страху для досягнення певних соціально-політичних цілей і відоме історії понад дві тисячі років.

Актуальність протидії тероризму полягає в тому, що високотехнологічний тероризм нової епохи здатен призвести до системної кризи всього світового співтовариства, особливо країн з розвиненою

інфраструктурою інформаційного обміну. Сьогодні практично всі комп'ютерні засоби оброблення та зберігання інформації вразливі для терористів. Банківські, біржові, архівні, дослідницькі, управлінські системи, інтернет, засоби комунікації від супутників до пейджерів, електронні засоби масової інформації, видавничі комплекси, будь-які бази персональних даних – все це може атакуватися з одного-єдиного комп'ютера, якщо терорист має відповідну кваліфікацію.

Охарактеризувати сутність і зміст поняття "*інформаційний тероризм*" досить складно, загальноприйнятого визначення цього явища досі немає, незважаючи на те, що вчені й урядові організації запропонували сотні дефініцій. Складність полягає в тому, що необхідно виділити специфіку саме цієї форми тероризму, а це нелегко. Нелегко також встановити чіткі межі між інформаційним тероризмом та інформаційною війною.

Під терміном "інформаційний тероризм" прийнято розуміти:

1) використання інформаційних засобів у терористичних цілях – погрози застосування або застосування фізичного насильства в політичних цілях, залякування і дестабілізація суспільства, відповідно, вплив на населення або державу;

2) дії з дезорганізації автоматизованих інформаційних систем, що створюють загрозу для життя людей, призводять до заподіяння значної майнової шкоди чи настання інших суспільно-небезпечних наслідків, якщо вони вчинені з метою порушення громадської безпеки, залякування населення або здійснення впливу на прийняття рішень органами влади, а також погроза вчинення зазначених дій з тією самою метою.

У вузькоправовому сенсі інформаційний тероризм може трактуватися як навмисне зловживання засобами інформаційної системи, інформаційної мережі або їхніми компонентами з метою підтримки або сприяння терористичній діяльності чи окремій акції. У цьому випадку зловживання системою (мережею) не обов'язково призводить безпосередньо до насильства над людьми, але може стати причиною катастроф або диверсій, в результаті яких можуть бути людські жертви.

Інформаційний тероризм визначається також як психоінтелектуальна небезпечна диверсія, спрямована проти нормального стану людської свідомості. Інформаційний тероризм здійснюється посиланням неправдивої (хибної) інформації з метою створення у людей суперечливих уявлень, обурення й помилкового розуміння.

Такий вид тероризму є вкрай небезпечним асоціальним явищем. Ніщо не справляє такого сильного впливу на окремих людей, суспільство чи державу, як правдива чи хибна інформація. Зважаючи на

особливу руйнівну силу, непередбачуваний характер наслідків дезінформації, інформаційний тероризм можна вважати найскладнішим видом негативного інформаційно-психологічного впливу. За відсутності достовірних знань інформаційні терористи навмисне дезорієнтують свідомість, уявлення й розуміння людей про навколишні обставини в полі реального сприйняття дійсності, викликаючи тим самим реальні дії – акції протесту, дестабілізацію суспільства.

Тобто, *інформаційний тероризм* – це форма негативного впливу на особистість, суспільство і державу всіма видами інформації. Однією з його цілей є ослаблення й розхитування усталеного суспільного ладу за допомогою спецслужб, ЗМІ, заяв авторитетних людей. Інформаційний тероризм застосовується, як правило, в галузях, де є передумови до ідейної або фінансової боротьби, наприклад, політика, економіка, релігія.

Інформаційний тероризм має свої механізми. До них відносять: створення громадських організацій певного спрямування; формування суспільної думки за допомогою ЗМІ (преса, телебачення, інтернет); розповсюдження агітаційних та інформаційних матеріалів.

Отже, інформаційний тероризм не призводить до швидкого фізичного знищення людей, проте його наслідки можуть бути куди більш трагічними. Оскільки суспільство на сучасній стадії розвитку є інформаційним, то для нав'язування йому певних ліній поведінки потрібно управляти інформацією, яка циркулює інформаційними потоками суспільства. Цим і користуються терористи. Інформаційний тероризм як директивне нав'язування малою групою людей певних ліній поведінки владі й суспільству поки що малопомітний і досягає своєї мети, не привертаючи особливої уваги. Проте з часом це може призвести до непередбачуваних наслідків.

Зважаючи на викладене, надзвичайно важливим в сучасних умовах є вдосконалення механізмів протидії сучасним технологіям терористичної діяльності. Наявність суттєвих перешкод для спільного використання інформації правоохоронними органами різних держав, відсутність єдиної дефініції злочинів та їх статистики, культури співробітництва між відповідними установами та представниками громадського і приватного секторів, а також проблеми відповідного регулювання захисту інформації створюють додаткові перешкоди на шляху вирішення цієї проблеми. Сучасний стан розвитку інформаційного суспільства та достатньо високий рівень потенційних загроз з боку тероризму (зокрема "інформаційного тероризму") визначають нагальність надання відповідного правового статусу органам кримінального переслідування та установам, що відповідають за попередження злочинності й тероризму, а також забезпе-

чення оперативного доступу до необхідних і актуальних даних у складі сучасних національних і міжнародних інформаційно-аналітичних систем з метою ефективної протидії терористичним проявам та актам.

Таким чином, ефективність інформаційно-аналітичної роботи у напрямі протидії терористичним актам та проявам може бути забезпечена через запровадження принципу права рівного доступу до даних, як основи відомчої інформаційної політики. Базовими положеннями принципу є загальна відповідальність персоналу силових відомств за безпеку використання інформаційних ресурсів, взаємозалежність нормативно-правових актів про боротьбу з тероризмом та організованою злочинністю, легітимність дій органів кримінального переслідування тероризму, встановлення нормативів для баз даних інформаційних ресурсів, а також створення центральної бази даних.

*Петрик В.М.,*
*кандидат наук з державного управління, доцент,*
*Національна академія Служби безпеки України*

## СУТНІСТЬ ДЕЗІНФОРМАЦІЇ ТА ДЕЗІНФОРМУВАННЯ

Сьогоднішні реалії наочно показують активне вживання різних дезінформаційних технологій в протистоянні як окремих соціальних груп, підприємств, фінансово-промислових груп, так і транснаціональних корпорацій і держав. У ролі суб'єктів дезінформації виступає широкий спектр персоналій – від домогосподарок до глав держав і транснаціональних корпорацій. Тому актуальним є розгляд питань, пов'язаних з дезінформуванням.

*Дезінформація* (фр.des – префікс, що означає знищення чи вилучення чого-небудь, + інформація) – спотворені або не достовірні відомості, які поширюються для досягнення пропагандистських, військових, політичних або інших цілей.

При поширенні дезінформації використовують такі *дефекти сприйняття інформації:*

1. Вибірковість людського сприйняття - ми бачимо лише те, що можемо розпізнати і що присутнє в нашому минулому досвіді. Автоматичне реагування на знайомі слова, з опорою на колишній досвід без розуміння загального контексту, тобто позиціювання інформації за зовнішніми ознаками, без її осмислення.

2. Найгрубіша дезінформація легко втрачає свою значущість, якщо об'єкт сам не хоче її бачити. Тобто, навіть помічаючи певні натяжки і помилки, багато персонажів швидше придумають їм виправдання, ніж спробують зробити самостійну оцінку.

3. Віра людини в значущість інших. Біля кожного є коло значимих для нього осіб, від яких дезінформація приймається на віру, з меншою долею критичності.

*Фактори, що сприяють сприйняттю дезінформації:*

- людина не в змозі самостійно оцінювати сотні подій, що відбуваються в світі;
- ЗМІ наводять факт разом з його інтерпретацією, і часто тільки зусиллям розуму можна відокремити факт від його інтерпретації;
- за людину інтерпретацію події робить хтось, хто є для неї авторитетнішим, компетентнішим (журналіст, експерт);
- статус пасивного глядача/слухача не дозволяє (або рідко дозволяє) виходити на статус свідка, що може сформувати свою власну думку поза інтерпретацією, яка вводиться, автономно від неї;
- читач/глядач у більшості випадків навіть не зацікавлений в альтернативних думках, оскільки тоді процес вибору інтерпретації переходить на нього;
- ЗМІ посилаються, або надають можливість висловлюватись людям, які недосяжні в реальному житті (наприклад, відомий актор, авторитетне інформаційне агентство);
- ЗМІ як найпотужніший апарат для генерації повідомлень заповнюють інформаційний простір повністю, не дозволяючи реально конкурувати з ними окремій людині, якій доводиться вибирати між вже готовими інтерпретаціями.

*Дезінформування* – це процес, який передбачає обман чи уведення об'єкта впливу в оману щодо справжності намірів для спонукання його до запрограмованих дій. Слід зазначити, що дезінформування може проводитись не тільки за допомогою неправдивої інформації. Наприклад, у процесі "білого дезінформування" (до якого належать тенденційне викладення фактів та дезінформування "від зворотного") використовується правдива інформація, а термінологічне "мінування" викривляє правильну суть принципово важливих, базових понять. Тільки "сіре" і "чорне" дезінформування обов'язково передбачає наявність неправдивої інформації.

*Форми дезінформування*:

- тенденційне викладення фактів – полягає в упередженому висвітленні фактів чи іншої інформації щодо подій за допомогою спеціально підібраних правдивих даних. Як правило, використовуючи цей метод, об'єкту впливу доводять дозовано, із постійним зростанням напруження, спеціально сформовану інформацію. Такий на-

пружений стан об’єкта підтримується шляхом постійного “підкидання” нових порцій суворо обмежених і дозованих даних у середовище інформаційного дефіциту;

- дезінформування “від зворотного” – відбувається шляхом подання правдивих відомостей у перекрученому вигляді чи в такій ситуації, коли вони сприймаються об’єктом впливу як неправдиві. Внаслідок застосування подібних заходів виникає ситуація, коли об’єкт фактично знає правдиву інформацію про наміри чи конкретні дії протилежної сторони, але сприймає її неадекватно та не готовий протистояти негативному впливу;

- термінологічне “мінування” – полягає у викривленні первинної правильної суті принципово важливих, базових термінів і тлумачень загальносвітоглядного та оперативно-прикладного характеру;

- “сіре” дезінформування – передбачає використання синтезу правдивої інформації з дезінформацією;

- “чорне” дезінформування – означає застосування переважно неправдивої інформації.

*Базові методи дезінформування:*

1. Переконання.

2. Навіювання.

Переконання звернене до власного критичного сприйняття дійсності об’єктом впливу. Воно має певні алгоритми впливу:

- логіка переконання має бути доступною для інтелекту об’єкта впливу;

- переконання варто здійснювати, спираючись на факти, відомі об’єкту;

- переконлива інформація повинна містити узагальнювальні пропозиції;

- переконання має містити логічно несуперечливі конструкти;

- факти, що доносяться до об’єкта впливу, повинні мати відповідне емоційне забарвлення.

Навіювання, навпаки, спрямовується на суб’єктів, які некритично сприймають інформацію. Його особливостями є:

- цілеспрямованість і плановість застосування;

- конкретність визначення об’єкта навіювання (селективний вплив на певні групи населення з урахуванням їхніх основних соціально-психологічних, національних й інших особливостей);

- некритичне сприйняття інформації об’єктом навіювання (навіювання засноване на ефекті сприйняття інформації як інструкції до дії без її логічного аналізу);

- визначеність, конкретність поведінки, що ініціюється (об’єкту необхідно дати інструкцію щодо його конкретних реакцій і вчинків, які відповідають меті впливу).

**ЛІТЕРАТУРА**

1. Сугестивні технології маніпулятивного впливу : навч. посіб. / [В.М.Петрик, М.М.Присяжнюк, Л.Ф.Компанцева та ін.] ; за заг. ред. Є.Д.Скулиша. – К. : Наук.-вид. відділ НА СБ України, 2010. – 248 с.

2. Доценко Е.Л. Психология манипуляции: феномены, механизмы и защита / Е.Л.Доценко. – СПб. : Речь, 2003. – 304 с.

*Поліщук М.М.,*
*кандидат психологічних наук, доцент,*
*Науково-дослідний інститут*
*Державної прикордонної служби України*

## ОСОБЛИВОСТІ ВПЛИВУ АВТОРИТЕТУ ПЕРСОНАЛУ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ НА СТАН ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

На забезпечення технічного захисту інформації в органах державної влади витрачаються значні матеріально-технічні ресурси, вартість розробки та експлуатації яких постійно збільшується. Проте слабким місцем будь-якої програмно-технічної системи захисту інформації залишається персонал організацій, який свідомими або несвідомими діями може спричинити витік інформації з обмеженим доступом. Це зумовлює зосередження уваги на формуванні позитивного авторитету персоналу органів державної влади, який може запобігати небажаним діям або бездіяльності у сфері інформаційної безпеки.

Питання формування авторитету персоналу організацій розглядались у соціологічному, етичному, педагогічному, психологічному та соціально-психологічному аспектах В.Шамраєм, М.Кейзеровим, В.Алещенко, М.Семеновим, В.Шепелем, Д.Іщенко, М.Литвиним, Б.Олексієнко та іншими вченими. Проте проблематика формування психологічно-свідомого ставлення прикордонників щодо якісного виконання своїх обов’язків у сфері інформаційної безпеки органів та підрозділів Державної прикордонної служби залишається недостатньо дослідженою.

Метою дослідження є визначення підходів щодо удосконалення психологічних здібностей прикордонників та зменшення впливу людського фактора щодо можливого витоку інформації з обмеженим доступом, яка обробляється у системі інтегрованого управління кордонами.

На думку О.Ф.Приліпко, авторитет персоналу – це полімодальний соціально-психологічний феномен, сутність якого полягає в комплексному поєднанні у свідомості прикордонника соціальної значущості та цінності тих властивостей, які забезпечують його ефективне професійне функціонування як суб'єкта суспільно значимої і престижної діяльності. Він складається з єдності авторитету посади та авторитету особистості [1].

Авторитет посади – це міра соціальної значущості суб'єкта як носія комплексу юридично закріплених владних повноважень, якими наділена відповідна посада. В основному він характеризує владно-правові стосунки персоналу. Авторитет особистості є більш значущим для ефективності діяльності фактором, який формується під впливом соціально-психологічних механізмів та залежить від особистісних властивостей і рис суб'єкта, його професійної майстерності й життєвого досвіду [2].

Феномен авторитету прикордонника виникає під час виконання ним завдань професійної діяльності в особливих умовах, має певну специфічність за своїми цілями, мотивами, завданнями, умовами, засобами та психологічним змістом. Екстремальність діяльності персоналу прикордонного відомства є відбиттям тих завдань, виконання яких покладене на Державну прикордонну службу України, сутність яких полягає у: забезпеченні недоторканності державного кордону, запобіганні злочинам та іншим правопорушенням у сфері прикордонної безпеки, підтриманні правопорядку і військової дисципліни серед прикордонників, захисті їх життя, здоров'я, прав і законних інтересів [3].

На нашу думку, на формування позитивного авторитету прикордонника впливають наступні групи факторів, які пов'язані з його професійними здібностями:

– особисті загальнокультурні, індивідуально-психологічні та соціально-психологічні властивості (культура професійної діяльності, ввічливість, тактовність, принциповість, доброзичливість, чесність, справедливість, порядність, сумлінність та мужність);

– психічні і психофізіологічні особливості прикордонника, що сприяють досягненню ефективності його професійної діяльності (старанність, дисциплінованість, професійний інтелект, кмітливість, діловитість, емоційно-вольова стійкість, комунікабельність, самокритичність).

Як було показано М.М.Литвиним, запровадження у систему інтегрованого управління кордонами загальних функцій державного управління (організація, планування, координація, мотивація, контроль) дозволяє цілеспрямовано управляти її окремими елементами

[4]. Також вважаємо за доцільне враховувати найбільш вагомі зв'язки між ними [5], що може підвищити рівень керованості процесів формування позитивного авторитету персоналу.

Так, на нашу думку, кожен окремий цикл управлінської діяльності може передбачати визначення під час організації, планування та координації діяльності мотиваційних факторів та стимуляторів, які можуть впливати на розвиток як загальнокультурних, індивідуально-психологічних, соціально-психологічних властивостей прикордонника, так і на його психічні й психофізіологічні здібності. Застосування функції контролю може передбачати виявлення розбіжностей між:

– очікуваним та реальним впливом на персонал мотиваційних факторів та стимуляторів;

– бажаною та реальною поведінкою персоналу під час виконання посадових обов'язків.

Результати застосування функції контролю доцільно використовувати для визначення переліку змін, які необхідно внести до всіх загальних функцій державного управління, включаючи і систему контрольних заходів. Зазначений підхід дозволяє зменшити ризики негативного впливу людського фактора в діяльності органів та підрозділів прикордонного відомства. Також зазначений підхід може зменшувати бюджетні витрати на забезпечення системи інформаційної безпеки органів державної влади без зменшення досягнутого рівня інформаційної безпеки.

З урахуванням викладеного, удосконалення системи інформаційної безпеки може бути досягнуто шляхом цілеспрямованого використання загальних функцій державного управління, які були адаптовані М.М.Литвиним до системи інтегрованого управління кордонами, щодо зростання авторитету персоналу прикордонного відомства. Напрямами подальших розвідок може бути визначення підходів до суб'єктивно-незалежного оцінювання авторитету персоналу органів державної влади.

## ЛІТЕРАТУРА

1. Приліпко О.Ф. Теоретичний аналіз сутності поняття "Авторитет військовослужбовців ВСП ЗСУ" [Електронний ресурс] / О.Ф.Приліпко // Вісник Національної академії Державної прикордонної служби України: електрон. наук. фах. вид. / гол. ред. Л.М.Романишина. – 2012. – Вип. 1. – Режим доступу : http://archive.nbuv.gov.ua/e-journals/Vnadps/2012_1/12pofvsp.pdf.

2. Максименко С.Д. Загальна психологія : навч. посіб. / С.Д.Максименко, В.О.Соловієнко. – К. : МАУП, 2000. – 256 с.

3. Зонь В.В. Виховання вольових якостей у курсантів вищих військових навчальних закладів : автореф. дис. канд. пед. наук : 13.00.04 / В.В.Зонь – Центр. ін-т післядиплом. пед. освіти АПН України. – К., 2002. – 20 с.

4. Литвин М.М. Інтегроване управління кордонами / М.М.Литвин. – Хмельницький : НАДПСУ. – 2012. – 416 с.

5. Кукан І.В. Удосконалення процесів управління у сфері прикордонної безпеки / І.В.Кукін // Інвестиції: практика та досвід. – 2012. – № 17. – С. 81–84.

*Присяжнюк М.М.,*
*кандидат технічних наук,*
*старший науковий співробітник,*
*Національна академія Служби безпеки України*

## ВИЯВЛЕННЯ ОЗНАК ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ В ЗАСОБАХ МАСОВОЇ КОМУНІКАЦІЇ

Аналіз інформації з метою виявлення ознак інформаційно-психологічних впливів, які можуть бути складовою спеціальних інформаційних операцій (СІО), передбачає потребу охоплення величезних масивів інформації та, найчастіше, обробки не їх тематичного змістового навантаження (економіка, культура, освіта), а контекстів, відтінків та прихованого і непомітного неозброєним оком змісту.

Здійснення зазначеного аналізу, незалежно від його зовнішніх форм (програмними засобами чи фахівцями), передбачає володіння теоретично та емпірично обгрунтованими критеріями оцінки інформації. Критерії повинні бути універсальними, не прив’язаними до конкретної події, особи тощо.

Першочерговою метою аналізу, дещо спрощеною (але чіткою і зрозумілою), є виявлення недостовірної або спеціально підібраної інформації, яка викривляє факти. Варто наголосити на важливості пошуку яскраво емоційних текстів, які внаслідок апеляції до емоцій, а не розуму людини, також володіють значним маніпулятивним потенціалом.

Виявлення маніпулятивної інформації є “сигналом” для подальшого пошуку логічних зв’язків, джерел та каналів поширення інформації, визначення авторства тощо. Можна стверджувати, що по-

єднання ознак маніпулятивності з системністю та організованістю інформаційного впливу (тобто інформації, поєднаної спільним предметом) з великим ступенем достовірності свідчить про проведення спрямованого інформаційного впливу.

Маніпулятивність текстової інформації виступає своєрідним сигналом для подальшої перевірки інформації. Для фіксації маніпулятивності інформації варто застосовувати узагальнені ознаки маніпулятивності та системності й організованості, які доцільно постійно удосконалювати.

Системний моніторинг відкритих інформаційних потоків можна здійснювати в інтересах держави загалом, її гілок влади, для захисту національних інтересів в економічній чи зовнішньополітичній сферах. Моніторинг може організовуватись і в інтересах окремих фінансово-промислових чи політичних груп.

Проведення об'єктивного аналізу з метою попередження негативних наслідків маніпулятивних інформаційних впливів ускладнюється "real-time" режимом роботи аналітичних служб. Це означає, що найчастіше інформації для об'єктивного порівняння фактів немає: звучить заява про зв'язки високопосадовця з резидентом зарубіжної розвідки, додається картинка (фото, відео) потискання рук можновладця з невідомою особою..., робляться відповідні висновки. Але ж достеменно ніхто не знає, чи є ця особа іноземним агентом, чи студентом театрального інституту. Або набуває розголосу матеріал про корупційність особи. Як доказ наводяться фотографії шикарного автомобіля. Але ми не знаємо, чий це автомобіль, а на перевірку зазначених фактів не завжди вистачає часу, сил та засобів. А рішення необхідно приймати "ще вчора".

Завданням аналітиків за таких умов стає розпізнавання інформаційних загроз "на льоту" за непомітними, другорядними ознаками в умовах обмеженості інформації та часу.

Найбільшої уваги заслуговують інформаційні випуски новин, оскільки саме вони формулюють актуальні на сьогодні теми для громадського обговорення. Так, із величезної кількості катастроф у ЗМІ будуть відображені лише ті, які, образно кажучи, вдало потрапили в об'єктив телекамер: ідеальний варіант – ефектне падіння пасажирського потягу в морську безодню на фоні багряного заходу сонця. Звідси інша закономірність: боротьба ведеться за саме право потрапити в інформаційні випуски. Отже, сам порядок денний новин (так звана "agenda") підлягає першочерговому аналізу.

Для визначення мети інформаційно-психологічного впливу важливо ідентифікувати цільову аудиторію впливу. В інтересах цього виду аналізу доцільно класифікувати споживачів інформації за такими ознаками:

1. За соціальним статусом: робітники, селяни, середній клас, еліта.

2. За релігійною належністю: християни (православні, католики), мусульмани (шиїти, суніти), іудеї, атеїсти та інші.

3. За національною ознакою: українці, росіяни, татари, євреї тощо.

4. За мовною ознакою: для України важливим є поділ на російськомовне та україномовне середовище.

5. За віком: діти, студенти (молодь), працююче населення, пенсіонери тощо.

6. За сферою діяльності: політики, економісти, правоохоронці, військові тощо (наприклад, основною аудиторією інтернет-сайту ОРД (ord.com.ua) є правоохоронці).

Вибір перелічених соціальних груп не випадковий. Як родові ознаки для класифікації було обрано площини можливого протистояння в суспільстві: багаті – бідні, мусульмани – християни, батьки – діти тощо, – оскільки підтримка конфліктної, нестабільної ситуації є пріоритетною передумовою маніпулятивного інформаційного впливу. Спрацьовує "стадний" психологічний захисний ефект згуртування перед загрозою (людина – соціальна, "стадна істота"). Сприйняття зовнішніх команд (інформації) для спільного виконання при цьому спрощується: стояти – бігти; вперед – назад. Жодних напівтонів чи раціоналізму: або ворог чи свій. Невиконання принципово (підсвідомо) неможливе – це загрожує "виживанню стада". Що може бути краще для маніпулювання?

Яскравий приклад – штучний розкол українського суспільства за лінією схід-захід, який із періодичністю та впертістю свідомо культивується українськими політиками з 1998 року і до теперішнього часу.

Завдання ідентифікації цільових груп вирішується шляхом аналізу: джерела інформації, мови інформаційного повідомлення, часу виходу в ефір (оприлюднення), читацької (глядацької) аудиторії ЗМІ, форми оприлюднення (телебачення, друковані ЗМІ, інтернет, листівки, бігборди), особи – озвучувача інформації.

Особливу увагу варто звертати на ключові слова, загальний контекст повідомлення: соціальні пільги – отже, аудиторією є пенсіонери; ціни на горілку – робітники; ціни на зерно, м'ясо та добрива – селяни; житло для військовослужбовців і т. ін.

Ознаки, які дозволяють виявити маніпулятивність інформаційного впливу, можна поділити на *організаційні* (за системністю та організованістю) та *змістовні* (за змістом). Кількість ознак може накопичуватися у процесі досліджень висвітлення певної сфери життєдіяльності суспільства у засобах масової комунікації.

Ймовірність наявності маніпулятивного інформаційно-психологічного впливу як складової СІО залежить від низки ознак. Об'єктивність та неупередженість оцінок на основі ознак маніпулятивного впливу може забезпечити колектив фахівців-аналітиків, використовуючи апарат математичної теорії ймовірності.

Для оцінки змісту текстових повідомлень широко використовується контент-аналіз – формалізований метод вивчення текстової і графічної інформації, який полягає у переведенні інформації, що вивчається, в кількісні показники та її статистичній обробці.

## ЛІТЕРАТУРА

1. Інформаційна безпека (соціально-правові аспекти) : підруч. / [В.В.Остроухов, В.М.Петрик, М.М.Присяжнюк та ін. ] ; за заг. ред. Є.Д.Скулиша. – К. : КНТ, 2010. – 776 с.

2. Інформаційна безпека особистості, суспільства, держави : підруч. / [Я.М.Жарков, М.Т.Дзюба, І.В.Замаруєва та ін.]. – К. : Видавничо-поліграфічний центр "Київський університет", 2008. – 256 с.

3. Сугестивні технології маніпулятивного впливу : [навч. посіб. / В.М.Петрик, М.М.Присяжнюк, Л.Ф.Компанцева та ін.]. – за заг. ред.. Є.Д.Скулиша. – К. : Наук.-вид. відділ НА СБ України, 2010. – 248 с.

*Пшеничнюк О.В.,*
*кандидат філософських наук, доцент,*
*Національна академія Служби безпеки України*

## МАНІПУЛЯТИВНІ ІНТЕРПРЕТАЦІЇ РЕЗУЛЬТАТІВ СОЦІОЛОГІЧНИХ ДОСЛІДЖЕНЬ ЯК ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ СУСПІЛЬСТВА

Соціологічні дослідження як наукове вивчення суспільної реальності мають важливі особливості через те, що з їх допомогою здобувається унікальна інформація про події в суспільстві з подальшою їх інтерпретацією. Головне джерело знань у такому випадку – це конкретний індивід, який повідомляє суб'єктивну інформацію. Надалі спрацьовує діалектичний закон переходу кількісних явищ у якісні, і суб'єктивні міркування людей шляхом застосування спеціальних методик, соціологічних процедур перетворюються на об'єктивні достовірні знання, які мають прикладний характер та широко використовуються в практиці соціального управління, про-

гнозування, при розробці соціальних, у тому числі політичних, технологій, надають можливості не тільки діагностувати суспільні проблеми, а й знайти ефективні шляхи їх вирішення та виробити практичні рекомендації щодо удосконалення соціального життя. Проте при проведенні таких досліджень громадської думки виникає низка проблем: належного узагальнення, належної вибірки з метою охоплення повної сукупності одиниць, що підлягають вивченню, і, нарешті, належного витлумачення чи інтерпретації отриманих даних. І.Бекешкіна, директор Фонду "Демократичні ініціативи" імені Ілька Кучеріва наголошує: "Інтерпретація та подача даних соціологічних опитувань у ЗМІ є справжньою ахилесовою п'ятою української журналістики" [1, с. 37].

Обнародування результатів соціологічних досліджень: чи-то простих опитувань громадської думки, чи-то соціологічного моніторингу, чи, скажімо, передвиборчого екзит-полу має за мету забезпечити органи державної влади та управління, політичних лідерів, пересічних громадян країни об'єктивною, достовірною, неспотвореною соціологічною інформацією. На жаль, практика інформування населення щодо проведення певних соціологічних досліджень має непоодинокі приклади використання "чорної соціології", коли в угоду меркантильним чи іншим такого роду цілям, подається не об'єктивна інформація, а така, яка вигідна замовнику. Спеціалісти-соціологи зауважують, що фальсифікація соціологічних даних – справа складна і недешева, але все ж таки змушені констатувати, що особливо розширюється поле для розповсюдження такої інформації під час політичних виборів, про що свідчать останні парламентські вибори 2012 р. в Україні, коли були зафіксовані особливо яскраві приклади маніпуляцій соціологією з боку деяких політичних партій - аутсайдерів. При цьому важливо враховувати як особливості подання соціологічної інформації, що, за влучним висловом американських соціологів, має ефект "фургона з оркестром", тобто здатність привертати увагу, підсилювати зацікавленість її споживачів, так і психологію людини, яка на підсвідомому рівні прагне приєднатися до більшості. Саме тому різні маніпулятивні технології, прийоми, до яких вдаються недобросовісні виробники соціологічної інформації, чи журналісти, які супроводжують її відповідними коментарями, можуть розглядатися як специфічні загрози інформаційній безпеці. На упередження таких випадків спрямоване виборче законодавство України, яке вимагає при публікації, наприклад, рейтингів політиків вказувати: організацію, яка проводила опитування, час його проведення, кількість опитаних, метод збору інформації, точне формулю-

вання запитання, дані про репрезентативність, статистичну оцінку можливої похибки. З огляду на це, всі, хто причетний до виробленя, розповсюдження та споживання інформації: від тих, хто приймає управлінські рішення до пересічного громадянина, повинні володіти знаннями щодо проведення соціологічних досліджень з метою убезпечення себе від отримання неякісної, спотвореної інформації.

Серед найбільш поширених прийомів маніпуляцій результатами соціологічних досліджень виділяються наступні.

Навмисне спотворення інформації у формулюваннях при повідомленні результатів дослідження, наприклад, переплутування цифр рейтингів осіб, поява розбіжностей у показниках реального опитування та під час оприлюднення його результатів.

Перенесення думки певної спеціальної групи людей на усю генеральну сукупність, наприклад, здійснювалося опитування жителів західних чи східних областей України, а інформацію розповсюдили щодо всього населення України. Таким чином, фактично нерепрезентативне дослідження у висновках подається як репрезентативне.

Викривлення інформації шляхом замовчування дати проведення дослідження. Особливо чутливий такий прийом під час політичних виборів, адже відомо, що рейтинги політиків можуть з часом змінюватись, як в один, так і в інший бік, а отже, банальна відсутність інформації про істинну дату проведення виборів може розглядатися як маніпулятивна технологія.

Підміна запитання, сформульованого у дослідженні, іншим формулюванням, адресованим громадськості (наприклад, досліджується якій партії найбільше симпатизують виборці, а у повідомленні про результати йдеться про партію, за яку вони будуть голосувати чи, скажімо, ототожнюються рейтинги довіри, рейтинги оцінки діяльності та виборчі рейтинги).

Підміна рейтингів, основою яких є відсоток від усіх виборців, рейтингами, основою яких є інформація про те, хто має намір взяти участь у голосуванні.

Маніпулятивні технології при складанні анкети: формулювання запитань, яким наперед надається перевага, “зсунутих” чи акцентуйованих запитань, які “підштовхують” до потрібної замовникам відповіді, розташування їх у такому порядку, що призводить до викривлення інформації.

Знання цих та інших маніпулятивних прийомів при інтерпретації соціологічних досліджень та вміння їх належно оцінювати має убезпечити споживача від використання неякісної, спотвореної та сфальсифікованої інформації.

**ЛІТЕРАТУРА**

1. Опитування громадської думки. Посібник для журналістів / [укл. та ред. І.Бекешкіна, В.Довгич]. – К. : Фонд "Демократичні ініціативи". – 2012. – 96 с.

*Руденко Ю.Ю.,*
*кандидат політичних наук, доцент*
*Національна академія Служби безпеки України*

## ПРОТИДІЯ ДЕСТРУКТИВНИМ ПРОЯВАМ ПЛЮРАЛІЗМУ В ІНФОРМАЦІЙНІЙ СФЕРІ: ЗАГРОЗА ДЕМОКРАТИЧНИМ ЦІННОСТЯМ ЧИ ОЗНАКА ПРАВОВОЇ ДЕРЖАВИ

Суспільствознавці стверджують, що однією з ознак демократичного політичного режиму є плюралізм. Плюралізм чи багатоманітність думок, який безпосередньо пов'язаний зі свободою слова, дійсно є однією з ознак політичного режиму "демократія" або "поліархія", як прийнято називати реально існуючі у світі держави з демократичним режимом. Плюралізм також, безумовно, передбачає, як наслідок, певну неоднорідність (ідеологічну й духовну) суспільства.

Сьогодні в Україні у серйозну небезпеку для держави і суспільства перетворилася традиція плюралізму у вигляді непримиримої конфронтаційності, постійної налаштованості на боротьбу, на "продукування" конфліктів. Можемо констатувати факт, що ще за радянських часів ідеологічні кліше, наприклад, щодо "непримиренності буржуазної (читай, олігархічної) і комуністичної (читай, альтруїстичної) ідеологій", гасла типу "хто не з нами, той проти нас" міцно вкарбувалися у суспільну свідомість. Ставлення до боротьби як до самодостатньої цінності знімало питання про її необхідність, ціну, соціальні наслідки.

На жаль, можна з упевненістю стверджувати, що цей стереотип стосовно боротьби частково пролонгований і в незалежній Україні. Такі форми політичного існування, виявляється, не нові, демократичні (як інколи, запевняють політики), а швидше "архаїчно-традиційні".

Окреслений стереотип масової свідомості перенесений у нашому суспільстві і на взаємовідносини політичної влади та політичної опозиції (хто б персоніфіковано не представляв ці інститути – авт.), в яких "опозиція" завжди пригнічена владою, тому у будь-якому конфлікті завжди права. Не заглиблюючись у теоретичні тонкощі

(цей термін має суперечливе змістовне наповнення, особливо на рівні масової свідомості), з'ясуємо зміст поняття "політична опозиція". Отже, політична опозиція – спосіб протиставлення одних політичних поглядів, ідей, дій іншим поглядам, ідеям, діям [2]. Опозиція – політичний інститут, який має за мету формування та прояву інтересів і цінностей, які не представлені у діяльності правлячого режиму [3]. Тобто опозиція – це носій "критичного духу" в політиці. Разом з тим, потрібно акцентувати увагу на тому, що вона буває конструктивною та деструктивною, поміркованою й радикальною, інституціалізованою та неінституціалізованою, парламентською і позапарламентською тощо. Тобто, в певних формах з необхідного атрибуту демократичної правової держави, який не дозволяє правлячому режиму узурпувати владу, стає її руйнівником, тому що може ініціювати революції, заколоти, масові безпорядки, громадянські війни тощо та продукувати "деструктивні" для існування такої держави ідеї, скажімо, профашистські чи будь-які інші людиноненависницькі.

Тому, попри всі прагнення до багатоманітності і плюралізму, держави з розвиненими традиціями у сфері правової культури все ж таки прагнуть підтримувати певний мінімальний рівень гомогенності, принаймні виробити, цивілізовані, раціональні способи взаємин з політичними опонентами, і, навіть, якщо конфлікти і виникають, то їх розв'язання відбувається не стихійно та "безвекторно", а із залученням вироблених формалізованих, переважно правових процедур. Тобто плюралізм існує не як стихійне явище, а як явище, яке має "формальний", правовий супровід – "моя свобода закінчується там, де починається свобода іншого". Як не банально звучить вище наведена теза, але вона є дієвою для країн з розвиненою правовою культурою і демократичними традиціями.

Як же "реалізується" плюралізм в Україні? У Конституції України зазначено: "здійснення цих прав (право на свободу думки і слова – авт.) може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку", "утворення і діяльність політичних партій та громадських організацій, *програмні цілі або дії* яких спрямовані на ліквідацію незалежності України, зміну конституційного ладу насильницьким шляхом, порушення суверенітету і територіальної цілісності держави, підрив її безпеки, незаконне захоплення державної влади, пропаганду війни, насильства, на розпалювання міжетнічної, расової, релігійної ворожнечі, посягання на права і свободи людини, здоров'я населення, забороняються" [1].

Цілком зрозуміло, що реалізація програм подібних політичних партій та організацій на рівні *дій* повинна викликати протидію з бо-

ку правоохоронних органів держави. Інша справа, де та межа, коли, як то кажуть, потрібне хірургічне втручання – у випадку, коли "протиправна ідея" ще не стала дією. Тобто, "при констатуванні" правоохоронцями наявності протиправних *дій,* аргументованість щодо доцільності протидії викликає значно менше сумнівів, ніж коли "протиправна ідея" функціонує на рівні *"програмної цілі"*. Бо "програмна ціль" може ніколи не стати дією. Постає певне коло питань. Що таке поширення ідеї? Яка аудиторія, з якої кількості осіб потрібна для поширення забороненої протиправної ідеї, цілі, щоб певну організацію визнали, скажімо, як таку, що своєю діяльністю загрожує національній безпеці держави у сфері інформаційної безпеки? І насамкінець, якого роду "протидія" у цьому випадку необхідна і чи необхідна вона взагалі? Бо, дійсно, вже на сьогодні можемо знайти у програмних документах деяких радикальних політичних партій та організацій як лівого, так і правого спрямування ідеї, що, на нашу думку, порушують права особи, розпалюють міжетнічну ворожнечу, або, навіть, містять ідеї, що дозволяють кваліфікувати їх як такі, що порушують державний суверенітет чи територіальну цілісність держави. Наприклад, у програмних документах певної політичної партії або будь-якої іншої політичної організації можуть бути зазначені "програмні цілі", що порушують, наприклад, права людини - "заборонити змішані шлюби", а також, можуть заважати нормальному функціонуванню держави, скажімо, "приєднати певну частину території України, на якій компактно проживає певна етнічна група, до іншого державного організму" (ця програмна ціль пов'язана із порушенням територіальної цілісності України), або "встановити диктатуру" (ця "програмна ціль" пов'язана із закликами змінити форму держави незаконним шляхом) і. т. ін. У політичному просторі України достатньо подібних політичних організацій, які мають легальний статус і ідеї яких знаходяться, так би мовити, "на межі" з порушенням законодавства, але питання щодо аргументованості, меж, форм та методів втручання у діяльність подібних організацій та протидії їм, і на сьогодні, на нашу думку, залишається відкритим.

## ЛІТЕРАТУРА

1. Конституція України // Відомості Верховної Ради України. – 1996. – № 30.

2. Политология: Словарь / [под ред. Коновалова В.Н.]. – М., 2010.

3. Соловьев А.И. Политология: Политическая теория, политические технологи / А.И.Соловьев. – М., 2000.

*Самаріна М.В.,*
*Національна академія Служби безпеки України*

# ДОСВІД КНР У ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Актуальність проблеми забезпечення безпеки інформації в інформаційно-телекомунікаційних системах, насамперед, обумовлена тим, що на сьогодні інформаційні ресурси, інформаційна інфраструктура й інформаційні технології значною мірою визначають рівень і темпи соціально-економічного, науково-технічного й культурного розвитку країни.

Рівень розвитку й безпека інформаційного простору, які є системоутворюючими факторами у всіх сферах національної безпеки, активно впливають на стан політичної, економічної, оборонної та інших складових національної безпеки кожної держави.

Слідом за підключенням до глобального інтернету в Піднебесній розгорнулося будівництво інформаційних мереж. Однією з перших загальнонаціональних мереж стала науково-дослідна CSTNet (ChinaScienceandTechnology NET), яка об'єднує науково-дослідні інститути. Пізніше до мережі приєдналися державні структури, включаючи владу на місцях.

З 1996 року Китай починає розробляти законодавство, що регулює мережевий простір. Серйозні поправки, що посилюють первинні правила, були прийняті керівництвом країни відповідно до загальної концепції реформ останніх десятиліть: стимулювання модернізації економіки і одночасне стримування політичних перетворень.

Контролю, передусім, підлягають ідеологічні ресурси, а також ресурси, які містять морально й етично неприйнятну інформацію. Необхідність цензури мотивується "захистом національної культури та соціальних цінностей". Забороні підлягає будь-який контент, що "підриває державну владу", "розхитує соціальну стабільність", "завдає шкоди репутації" Китаю або "заважає зусиллям щодо возз'єднання" з Тайванем. При цьому визначення нелегального контенту часто сформульовані досить туманно: "поширення чуток" або "захист культів і феодальних забобонів" (маються на увазі "антигуманна й антиурядова діяльність" прихильників незалежності Тибету, забороненої секти Фалуньгун та ін.). Крім того, правила накладають категоричну заборону на гральний бізнес і порнографію. У країні, інтернет-населення якої збільшується на мільйон кожен місяць, здійснювати повсюдний моніторинг електронних ресурсів виключно поліцейськими підрозділами стає нереальним завданням. З цієї причини правила перекладають відповідальність за блокування всіх категорій нелегального контенту на компанії-утримувачі сайтів

і чатів. Інтернет-провайдери контенту (ICP – Internet ContentProvider) зобов'язані вести повний облік всієї інформації, яка з'являється на сайті, включаючи і коментарі в онлайнових чатах, а також фіксувати час публікації. Усі облікові записи мають зберігатися протягом 60 днів. Цей же термін передбачений і для провайдерів інтернет-послуг, які забезпечують під'єднання користувачів до інтернету, а також вони повинні фіксувати час підключення користувачів до мережі, їхні реєстраційні імена, інтернет-адреси, доменні імена або телефонні номери, з яких користувачі виходять в інтернет. Всі збережені облікові записи провайдери зобов'язані надавати в поліцію за її запитом. У десяти великих містах встановлені урядові сервери, покликані відфільтровувати весь інформаційний потік, що надходить в китайську частину глобальної мережі. Всі провайдери доступу (IAP – Internet Access Provider) також зобов'язані встановлювати сервери, що блокують доступ до іноземних електронних ресурсів небажаного політичного змісту [1].

Ще одна особливість регулювання полягає у введенні досить заморочливих і дорогих поліцейських процедур, що в обов'язковому порядку супроводжують всю інфраструктуру комп'ютерних мереж у країні. Для того, щоб стати користувачем інтернету, кожен бажаючий зобов'язаний пройти перевірку в місцевому відділенні поліції і надати провайдеру довідку встановленого зразка. Процедура перевірки корпоративних користувачів ще суворіша і займає дуже багато часу. Компанія може чекати рішення влади протягом декількох місяців. Поведінка співробітників компаній в інтернеті ретельно відстежується за допомогою технічних засобів. Фірми зобов'язані заводити спеціальні журнали для пояснення причин відвідування сайтів, що викликають заперечення уряду.

У 2002 р. боротьба із зарубіжними сайтами вперше торкнулася пошукових систем. Китайська філія Yahoo погодилася самостійно заблокувати доступ до деяких сайтів відповідно до розпорядження місцевої влади. Надалі були повністю заблоковані ще дві американські пошукові машини – Google і AltaVista. Після відновлення доступу до Google пошуковик запрацював інакше: ряд запитів блокується, а комп'ютер, з якого прийшов небажаний запит, на деякий час відключається від кібермережі. Компанія Google ухвалила рішення зняти всі цензурні обмеження для жителів Китаю в 2010 р. Щоб уникнути порушення законів країни, IT-гігант перебазував свої сервери в Гонконг[2].

На сьогодні в КНР діє низка нормативно-правових документів, що регламентують питання інформаційної та кібернетичної безпеки, зокрема: "Положення про телекомунікації", "Положення про захист комп'ютерної інформаційної системи", "Положення про захист прав на поширення інформації в мережах", "Положення про контроль за

телекомунікаційними підприємствами, заснованими за рахунок іноземних інвестицій", "Регламентація контролю за безпекою підключення вітчизняних інформаційних мереж до міжнародних мереж", "Положення про контроль за інформаційним обслуговуванням в Інтернеті", "Щодо безпеки Інтернету", "Про електронний підпис", "Регламентація контролю за інформаційним обслуговуванням у комп'ютерних мережах" тощо.

У мирний час завдання з формування державної політики у сфері інформаційної та кібернетичної безпеки покладені на Держраду КНР, а її реалізація - на Міністерство громадської безпеки (МГБ), Міністерство державної безпеки (МДБ) і Міністерство промисловості та інформаційних технологій. При цьому ключова роль у формуванні та реалізації стратегії інформаційного протиборства належить Народно-визвольній армії Китайської Народної Республіки.

## ЛІТЕРАТУРА

1. Аверкієв С.Д. Сучасні проблеми розвитку інформаційної безпеки / С.Д.Аверкієв. – М, 2005. – 132 с.

2. Буланов М.І. Економіка Азії / М.І.Буланов. – С.-Пб., 2005. – 76 с.

*Сніцаренко П.М.,*
*кандидат технічних наук,*
*старший науковий співробітник,*
*Національний університет оборони України*

*Саричев Ю.О.,*
*кандидат технічних наук,*
*старший науковий співробітник,*
*Національний університет оборони України*

*Кацалап В.О.,*
*Національний університет оборони України*

## МЕТОДИКА ОЦІНЮВАННЯ ДЕСТРУКТИВНОГО ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ

У сучасному інформаційному просторі значно підвищується можливість цілеспрямованого деструктивного інформаційного впливу на Україну, в першу чергу на керівництво держави та осіб, які приймають рішення на всіх рівнях влади та місцевого самоврядування, що становить одну з основних загроз інформаційній безпеці держави.

Результативна протидія деструктивному інформаційно-психологічному впливу повинна опиратися на ефективну систему, завдання якої – об'єктивно оцінити його рівень для прийняття адекватних рішень щодо нейтралізації такого впливу. З метою вирішення цього завдання пропонується можливий алгоритм створення методики оцінювання деструктивного інформаційно-психологічного впливу на об'єкти такого впливу.

Одним із підходів до вирішення цього завдання може бути застосування методів експертного оцінювання, які враховують досвід фахівців інформаційної сфери.

З метою оцінювання рівня деструктивного інформаційно-психологічного впливу необхідно на основі експертного опитування розробити певну систему показників, а для визначення його критичного (допустимого) значення – відповідні критерії. Для реалізації цього підходу пропонується структурувати ескалацію деструктивного інформаційного процесу відносно об'єктів впливу (від його зародження до набуття агресивних форм). Очевидно, що загальною характеристикою (показником) такого процесу може бути його рівень інтенсивності, тобто міра дії процесу в одиницю часу. Позначивши цю узагальнену характеристику символом $\chi$, динаміку ескалації деструктивного інформаційного процесу за деякий період часу $\Delta T$, її можна умовно представити ступінчатою функцією рівнів, як показано на рис. 1. При цьому, переходу на кожен із рівнів доцільно поставити у відповідність певний критерій за шкалою оцінок $\chi$: $\chi_1, \ldots, \chi_5$.

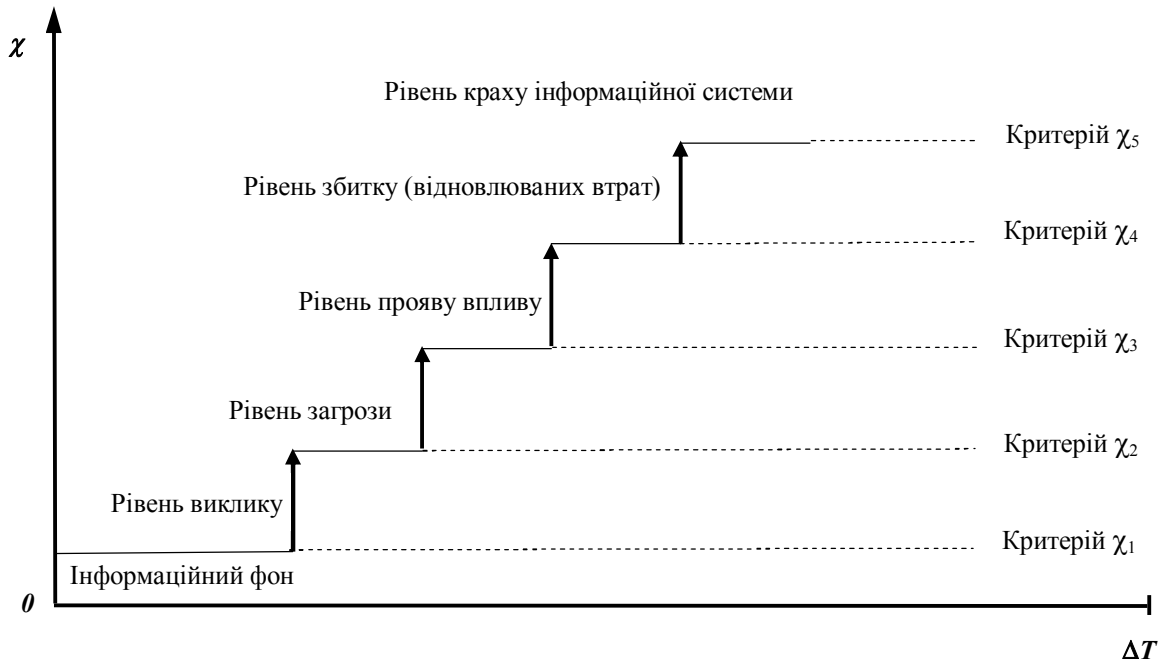



Рис. 1. Динаміка ескалації деструктивного інформаційного процесу

Із наведеного стає зрозумілим головне завдання, яке полягає у визначенні кількісних значень критеріїв $\chi_1, \ldots, \chi_5$. Це завдання вирішується у процесі реалізації 5-етапного експертного опитування.

При цьому ключовими особливостями при розробці базової методики є оцінювання визначення критеріїв рівня інтенсивності деструктивного інформаційно-психологічного впливу, а при застосуванні методики – оцінювання реального стану деструктивного інформаційного процесу.

Методика дозволяє оцінити стан деструктивного інформаційного процесу шляхом постійного моніторингу реальних деструктивних інформаційно-психологічних дій щодо об'єктів впливу за визначений сталий період $\Delta t$ ($\Delta t << \Delta T$), їх узагальнення та порівняння із кількісними значеннями критеріїв $\chi_1, \ldots, \chi_5$, отриманими на попередніх етапах експертної роботи. Слід зазначити, що важливою перевагою описаної методики, після її практичного відпрацювання, є можливість пропорційного "стиснення в часі" (масштабування) результатів квантування рівнів (зі зменшенням періоду $\Delta T$ пропорційно знижуються значення критеріальних оцінок $\chi_1, \ldots, \chi_5$), що дає можливість за проміжок часу $\Delta t << \Delta T$ визначити рівень небезпеки для об'єктів інформаційно-психологічного впливу.

Запропонована методика, після її відпрацювання, може бути покладена в основу комп'ютеризованої системи попередження про рівень інформаційних загроз та інформаційної безпеки держави загалом.

*Стрельбицький М.П.,*
*доктор юридичних наук, професор,*
*Національна академія Служби безпеки України*

*Стрельбицька Л.М.,*
*доктор юридичних наук, професор,*
*Національна академія Служби безпеки України*

## ДУХОВНІ ТА НАЦІОНАЛЬНІ ЦІННОСТІ ЯК ЗАСІБ ПРОТИДІЇ ДЕСТРУКТИВНОМУ ІНФОРМАЦІЙНОМУ ВПЛИВУ

Сьогодні дуже часто можна почути, що нібито у нас немає *об'єднувальної національної ідеї,* тому відсутнє взаєморозуміння у суспільстві. Це міф для довірливих, оскільки вічною, незалежно від

ситуативних революцій та їх вождів, ідеєю в Україні була і залишається *християнська ідея*, в основі якої лежить віра в духовні цінності і силу нації. Християнство традиційно залишається самою найбільшою релігією і об'єднує 33 % населення на Землі.

У розвинених країнах спостерігається падіння інтересу широких прошарків населення до релігії. Інша картина спостерігається в економічно слабких країнах, зокрема в Україні, де населення свої сподівання пов'язує із релігією і переважно вірно служить їй. Національна особливість нашої країни полягає в тому, що відродження релігійної самосвідомості відбувається одночасно не лише з одержанням давно омріяної незалежності і створенням самостійної держави, але й після войовничого атеїзму.

Із набуттям Україною незалежності ми насправді позбулись атеїстичних догм. Стара мораль вже віджила, а нова ще не опанувала свідомості індивідуума. І пустоти людських душ, що утворились внаслідок цього, миттєво заповнили такі антиподи як корупція, вимагання, алкоголізм, наркоманія, проституція, зокрема політична, тощо, які стали діагнозом цілого суспільства. Для підтвердження цієї тези достатньо навести динаміку злочинності серед населення України у відповідальний період становлення молодої державності, коли злочинці кинули смертельний виклик державі, що лише спиналася на ноги: хто-кого?

До складу сучасного *інформаційного українського суспільства* входять як віруючі, так і не дуже, або й вчорашні атеїсти, як заможні так і не дуже, або зовсім збіднілі верстви населення, представники різних релігійних конфесій, але головне, щоб вони у спілкуванні між собою проявляли християнську любов один до одного.

На заваді цьому стає зайва заполітизованість людей, міжконфесійні чвари, протистояння, внаслідок чого вже тривалий час українці борються за незалежність України… один з одним. Не може бути жодних виправдань міжконфесійному протистоянню чи то на етнічній, чи то іншій основі, оскільки це не від Бога, бо воно суперечить його вченню. Стає прикро, коли окремі священики у духовній одежі, що призначена для релігійних обрядів, очолювали колони різних політичних мітингів та маніфестацій, що було особливо характерно в перші роки незалежності, замість того, щоб проводити духовну роботу із паствою в напруженій соціальній ситуації. Для цього є політичні партії, яких в Україні задекларовано найбільшу кількість із країнах СНД – більш ніж півтори сотні. Не потрібно їм уподоблятись, адже релігійні організації згідно з чинним законодавством не мають права брати участі в діяльності політичних партій, висувати кандидатів до органів влади, вести агітацію за них. У церкви інші цілі, методи, засоби, ніж у партій.

А тим часом чимало стурбованих українців подалися в авторитарні секти на кшталт колишнього кримінального “Білого братства” Деві Марії чи сьогоднішнього пастора церкви “Посольства Божого” Сандея Аделаджі. Там у результаті цілеспрямованого інформаційного впливу через засоби психологічної обробки, гіпнозу та зомбування, маніпулювання їх свідомістю і вчинками, довірливі українці віддали свої кошти, квартири, майно і самих себе, ставши жертвами аферистів, які вміло використовували релігійну риторику.

Одним із ефективних видів впливу на свідомість людей в сучасних умовах є інформаційна війна, яка у широкому розумінні спрямовується проти конкретної держави, а у вузькому – проти особистості чи групи людей, соціума, основним засобом ведення якої є інформаційна зброя. В нашому випадку ця зброя спрямовується на психіку людей, їх індивідуальну і суспільну свідомість, стійкі особисті і морально-психологічні якості з метою досягнення поставленої мети.

Характерними особливостями інформаційної зброї, що відрізняють її від інших видів зброї, є те, що вона: найдешевша за вартістю, її не потрібно заново виготовляти, достатньо скористатися існуючими можливостями та засобами, найефективніша за наслідками, має найбільшу уразливість, вибірковість, необмежену масштабність, всі властивості інформаційної сфери тощо. До цих властивостей належить: невичерпність інформаційних ресурсів, миттєвість безперешкодної доставки до місця і об’єкта призначення, можливість легендування джерел інформації та контролювання реакції протилежної сторони, дозування і коригування змісту інформації за часом у процесі розвитку подій тощо.

Такою зброєю можуть бути вже існуючі і широко вживані засоби та види: ЗМІ (радіо, преса, телебачення), інтернет, мобільний зв’язок, наукова, художня та спеціальна література, фільми, телепередачі, твори мистецтва. Крім того, в *спеціальних операціях* широко застосовуються психотропні засоби, призначені для дистанційного зомбування населення і військового персоналу; оптико- і радіоелектронні засоби, що випромінюють електромагнітні хвилі та імпульси; лінгвістичні засоби (спеціальна термінологія); психотропні засоби (медпрепарати, наркотики, алкоголь і т. ін.).

Українська держава є секулярною інституцією, нейтральною щодо різних релігій та вірувань. Держава гарантує особі свободу совісті, віросповідання, але нормативно не закріплює, які релігійні організації вважаються деструктивними. Тому маємо орієнтуватись і розраховувати на власні сили, опиратись на свідомість, активність, мудрість християн, відстоювати наші християнські ідеї, примножу-

вати їх, створювати сучасне християнське інформаційне середовище і суспільство. Це наше історичне покликання, сам Бог нам послав незалежність, створивши необхідні для цього передумови і це відбувається в контексті світових тенденцій щодо відтворення традицій попередніх мудрих християнських поколінь, які про сьогоднішні умови споконвічно лише мріяли.

Виходячи з викликів та загроз інформаційній безпеці України в сучасних умовах, до групи найбільш суспільно небезпечних впливів можна віднести такі як: трансформована злочинність; кібернетичний тероризм; кібернетична інтервенція; інформаційна експансія; маніпулювання свідомістю населення.

У сукупності вони в сьогоднішніх умовах становлять реальну загрозу суверенній українській державі, мають стати предметом постійної уваги як з боку всіх гілок влади, правоохоронних органів, так і науковців, забезпечуючи своєчасний моніторинг, відпрацювання та вжиття адекватних заходів щодо надійного забезпечення *інформаційної безпеки України*. Цим впливам притаманні ряд загальних характеристик та ознак, які відрізняють їх від інших дій, або споріднюють з ними. До них, на наш погляд, можна віднести мету, риси, суб'єкти, об'єкти планування, а також сили, методи, засоби реалізації. Мету і способи ми розглядали раніше, до викладеного можемо додати наступне. На наш погляд основними і найбільш поширеними елементами, характерними для інформаційних впливів, є такі.

*Риси*: висока латентність і конспірація замовників, виконавців, джерел фінансування; швидка ескалація, що забезпечує миттєве досягнення запланованої мети; становлять реальну загрозу владі, органам управління, викликають нестабільність у суспільстві; безпосередньо впливають на прийняття політичних та управлінських рішень; групують населення навколо певних ідей та лідерів або проти них; легко контролюються ззовні, що дає змогу оперативно вносити корективи; дешеві за вартістю, масштабні за охопленням і відчутні за наслідками.

*Суб'єкти*: іноземні держави, їхні спецслужби, позаурядові організації юридичні та фізичні особи, які проводять агресивну інформаційну політику стосовно України; закордонні та окремі вітчизняні ЗМІ; релігійні фанатики (ваххабізм, ісламський фундаменталізм тощо), неокульти, організації сектантів та церковників; різного роду місіонерські організації, окремі екстремістські організації та групи.

*Об'єкти:* суспільні відносини, на які посягають суб'єкти інформаційної війни; система влади та державного управління (законодавча, виконавча та судова гілки влади, зокрема, Верховна Рада

України, Адміністрація Президента України, вищі суди та Конституційний суд України, Кабінет Міністрів, міністерства і відомства, органи місцевого самоврядування); лідери держави, партій, громадських рухів; безпека та система життєдіяльності держави, суспільства, права і свободи окремих громадян; інформаційні ресурси, бази даних, статистична звітність; молодь, студенти, соціально незахищені прошарки населення, безробітні, чорнобильці, афганці, дрібні підприємці.

*Засоби:* поширення повідомлень через видання засобів масової інформації (ЗМІ, інтернет, радіомовлення, телебачення), що викликають паніку серед населення; не зафіксовані на матеріальних носіях погрози; хибні повідомлення про очікуваний дефолт країни, вибухи, вбивства, отруєння, які нібито готуються, тощо.

Протидія зазначеним категоріям діянь має бути сформована первинно на політико-правовому рівні шляхом розробки й запровадження державних тактичних і стратегічних засобів протидії цим загрозам. Сталі терміни "загрози" і "виклики", які повною мірою відображають роль негативних уражень національній безпеці на рівні права мають знайти відображеннях у запровадженні спеціальних інститутів у рамках, зокрема, імперативних галузей права: конституційного, адміністративного, кримінального.

Натомість процеси реалізації у праві нового бачення сьогодні відбуваються надто повільно. Навіть на рівні сучасних стратегій не відчувається адекватної оцінки реальних загроз, і тим більше – необхідності протидії їм. Ці питання бере на себе правова політика. Основною рисою сучасної правової політики у сфері убезпечення суспільних відносин, притаманних інформаційному суспільству, від делінквентних і, зокрема, девіантних проявів має стати розробка и запровадження таких, що базуються на доктринальних вченнях про інформаційну безпеку та безпеку інформаційного простору, відповідних концепцій та стратегія їх реалізації. Такий процес є еволюційним, хоча часу на цю еволюцію стає все менше, адже право поки що, навіть за наявності розроблених доктрин та опублікованих концепцій, до цього часу майже не відображує необхідності ефективного протистояння вчинюваним небезпечним проявам. Запровадження превентивних заходів протидії сучасним викликам і загрозам в інформаційній безпеці України повинне супроводжуватись розробкою нових законодавчих актів та вдосконаленням чинних, запровадженням нового відповідного напряму у сфері державного управління, зокрема, державного контролю інформаційного простору, широкої бази підзаконних нормативно-правових актів, які формують якісно нові норми суспільної поведінки, виходячи з міжнародно-правових рекомендацій. Більш ефективною в цій системі має бути діяльність спеціальних підрозділів правоохоронних органів під

час здійснення оперативно-розшукового супроводження зазначеної сфери суспільних відносин.

Напрошується висновок: людство навчилось використовувати великі відкриття не лише собі на користь, але й на зло. *Як розщеплення ядра атома дало світу не лише мирний атом, але і ядерну зброю, так і інформаційні технології тепер мають подвійне призначення.* І як тут обійтись без релігійної моралі, основу якої становить християнська цивілізація?! Оскільки є реальна небезпека розв'язання глобальної інформаційної війни.

Розробка і запровадження своєчасних та ефективних заходів правової протидії загрозам нової доби потребує щоденної уваги вітчизняної юридичної науки, своєчасного реагування законодавця на її пропозиції та запровадження у державі належної правової політики.

*Шлапаченко В.М.,*
*кандидат юридичних наук,*
*Національна академія Служби безпеки України*

## ПРОТИДІЯ НЕГАТИВНОМУ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОМУ ВПЛИВУ ЯК СКЛАДОВА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Зростаюча значимість інформації в сучасному інформаційному суспільстві зумовлює актуальність вирішення проблем інформаційної безпеки.

На сьогодні насиченість новітніми засобами відтворення, передавання і отримання інформації значно розширює можливості інформаційно-психологічного впливу (ІПВ) на особу та суспільство. Зрозуміло, що в умовах конкурентної боротьби держав, коли контроль над суспільною думкою став метою глобальної політичної боротьби, цей вплив не завжди є позитивним. Саме тому Доктрина інформаційної безпеки України захищеність від негативного інформаційно-психологічного впливу відносить до життєво-важливих інтересів особи в інформаційній сфері системи забезпечення національної безпеки України. У той же час до основних реальних та потенційних загроз інформаційній безпеці України на сучасному етапі законодавець відносить:

- зовнішні негативні інформаційні впливи на суспільну свідомість через засоби масової інформації, а також мережу Інтернет;
- негативні інформаційні впливи, спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності і недоторканності кордонів України;

- інформаційно-психологічний вплив на населення України, у тому числі на особовий склад військових формувань, з метою послаблення їх готовності до оборони держави та погіршення іміджу військової служби;

- негативні інформаційні впливи, в тому числі із застосуванням спеціальних засобів, на індивідуальну та суспільну свідомість у внутрішньополітичній сфері [1];

Одним із головних напрямів державної політики у сфері інформаційної безпеки України Доктрина інформаційної безпеки України визначає *інформаційно-психологічний*, спрямований на забезпечення конституційних прав і свобод людини і громадянина, створення сприятливого психологічного клімату в національному інформаційному просторі задля утвердження загальнолюдських та національних моральних цінностей.

Протидія негативному інформаційно-психологічному впливу (НІПВ) є частиною забезпечення інформаційної безпеки держави, яка є складовою національної безпеки. Отже, протидію НІПВ можна розглядати і як елемент системи забезпечення інформаційно-психологічної безпеки особи, суспільства й держави, – стану захищеності психіки народу (нації) від впливу різних інформаційних чинників, що перешкоджають або утруднюють формування і функціонування адекватної інформаційно-орієнтувальної системи соціальної поведінки людини та в цілому життєдіяльності в сучасному суспільстві.

Небезпечність негативного (деструктивного, небажаного) ІПВ полягає, насамперед, в тому, що він здійснюється, як правило, непомітно для особи, має потужну і продовжувану дію (оскільки, здійснюється не лише на рівні свідомості, але й підсвідомості) та спрямовується переважно на орієнтувальну основу діяльності людини, тобто на сам психологічний механізм людської діяльності. Його системне застосування дозволяє контролювати не лише поведінку окремих осіб, але й соціальних груп (формальних чи неформальних), органів влади та управління, здійснюючи таким чином приховане втручання у внутрішні справи суверенних держав, впливаючи на їхню внутрішню та зовнішню політику.

Протидія НІПВ має бути невід’ємною складовою діяльності державних органів влади та управління не лише через виконання ними функцій держави із забезпечення інформаційної безпеки, але й тому, що саме вони (їх співробітники), в силу своїх функцій та повноважень, є найбільш бажаним об’єктом маніпуляцій.

Розглядаючи інформаційну безпеку як властивість системи мінімізувати інформаційні загрози вважаємо, що організація протидії НІПВ має передбачати:

1. *Визначення потенційних та реальних загроз*, тобто якому впливу здійснювати протидію. А саме:

- моніторинг інформаційного простору з метою виявлення ознак чи фактів здійснення НІПВ, або передумов до здійснення НІПВ;

- усвідомлення факту (або загрози) здійснення НІПВ, в т.ч. прихованого, неявного. Наскільки цей ІПВ є негативним, тобто наскільки позначається на виконанні функціональних завдань;

- хто супротивник, якими можливостями він володіє, який саме НІПВ, наскільки потужний і на якому рівні він може здійснювати;

- які канали поширення впливу може застосувати (ЗМІ, листівки, листи, телефонні контакти, SMS-повідомлення тощо);

- визначення зони НІПВ, тобто визначення частини інформаційного простору, де поширюється вплив, а також можливих об'єктів ураження, які потрапляють в зону дії впливу.

2. *Визначення об'єктів захисту*, тобто на що саме спрямований НІПВ, які об'єкти, що потрапили в зону дії впливу, потребують захисту (органи влади та управління, керівництво (командування), персонал, комунікаційні лінії тощо), а також можливих збитків від реалізації задуму НІПВ та чого саме необхідно запобігти чи уникнути (знищення, руйнування, підпорядкування, формування неправдивих установок, деморалізації, заворушень тощо).

3. *Визначення шляхів та засобів протидії*, тобто того, як уникнути можливих збитків, яким чином протидіяти НІПВ, виходячи з можливостей об'єкта захисту, характеристик небезпеки, сил і засобів наявних у суб'єктів протидії. А також, визначення необхідності відновлення певних функцій, якщо негативний вплив вже здійснено або здійснюється.

4. *Визначення суб'єктів протидії* (керівництво, органи управління, громадські організації, співробітники).

5. *Здійснення контролю та корекції вжитих заходів*.

Таким чином у протидії НІПВ можна визначити наступні *етапи*:

- моніторингу та виявлення загроз;
- визначення об'єктів захисту, заходів та суб'єктів протидії;
- здійснення контролю виконання та корекції вжитих заходів.

При організації протидії НІПВ важливо чітко усвідомлювати *цілі протидії*, основними з яких є наступні:

- досягнення або підтримання морально-психологічного стану, що забезпечує виконання окремими співробітниками та колективами поставлених завдань, уникнення деморалізації людей;

- підвищення морально-емоційної стійкості населення, передусім співробітників державних структур, до НІПВ, формування і стимулювання у об'єктів впливу думок, поглядів, емоцій, поведінки, що відповідають інтересам забезпечення інформаційної безпеки України;

- нейтралізація або значне послаблення наслідків НІПВ.

*Основними заходами інформаційно-психологічної протидії є:*

1. Прогнозування тематики й тактики здійснення деструктивних інформаційно-психологічних акцій з метою попередження впливів і тим самим зниження їх ефективності або нейтралізації.

2. Превентивне регулярне інформування, що передбачає роз'яснення:

а) цілей і завдань деструктивних інформаційно-психологічних акцій (їх спрямованості, істинних намірів та інтересів);

б) прийомів і тактики проведення деструктивних інформаційно-психологічних акцій.

3. Моніторинг громадської думки в умовах триваючого НІПВ з метою виявлення уразливості масової свідомості, прогнозування його наслідків та коригування заходів протидії.

4. Удосконалення закріплених в нормативно-правових актах вимог до психічного стану осіб – державних службовців, уповноважених приймати рішення, а також періодичності його перевірки та моніторингу.

5. Системне удосконалення нормативно-правового регулювання діяльності ЗМІ, а також рекламної, кінопрокатної, книговидавничої діяльності, з метою запобігання чи мінімізації їх використання як каналів поширення НІПВ.

6. Своєчасне реагування правоохоронних органів та спеціальних служб на ознаки проведення спеціальних інформаційних операцій, що сприяють дестабілізації ситуації в державі, розпалюють національну чи релігійну ворожнечу.

## ЛІТЕРАТУРА

1. Доктрина інформаційної безпеки України, затверджена Указом Президента України від 8 липня 2009 р. № 514/2009 [Електронний ресурс] // Офіційне інтернет-представництво Президента України. – Режим доступу : http://www.president.gov.ua.

*Штоквиш О.А.,*
*кандидат філософських наук,*
*старший науковий співробітник,*
*Український інститут національної пам'яті*

## МАНІПУЛЯЦІЇ ІСТОРИЧНОЮ СВІДОМІСТЮ ЯК ЗАГРОЗА НАЦІОНАЛЬНІЙ ДЕЗІНТЕГРАЦІЇ

У національній доповіді "Соціально-економічний стан України: наслідки для народу та держави", підготовленій Національною академією наук України у 2009 р., зокрема зазначається, що **"***українсь-*

*ке суспільство періоду незалежності (1991-2009) стало "історичним", "хворим на історію", таким, що болісно реагує на будь-які проблеми, пов'язані з власним минулим" [1, с. 462]. Такий стан речей свідчить про певні проблеми* з історичною свідомістю *нашого* суспільства, що може серйозно загрожувати його цілісності та втраті національної ідентичності.

Під історичною свідомістю в сучасній науці розуміється сукупність уявлень, притаманних суспільству в цілому і складових його соціальних груп окремо, про своє минуле і про минуле всього людства. У свою чергу важливою складовою історичної свідомості є такий різновид колективної пам'яті, як національна пам'ять, яка виступає важливою складовою самоідентифікації та консолідації народів, що населяють Україну, в єдину політичну націю – Український народ.

Під поняттям "національна пам'ять" розуміється феномен суспільної свідомості, селективно збережена нацією сукупність знань, уявлень та ціннісних оцінок тих подій минулого, які справили вирішальний вплив на її становлення, самоідентифікацію, державотворчі й цивілізаційні досягнення. Національна пам'ять має своєю основою історичну пам'ять певного народу (або народів). Історична пам'ять – явище значно ширше, аніж національна пам'ять, і включає у себе практично всю ретроспективну інформацію, яка "природним" шляхом закарбувалася у пам'яті народу, атрибутах його духовної та матеріальної культури. Проте головна відмінність між цими двома видами колективної пам'яті полягає у тому, що національна пам'ять є швидше атрибутом політичної нації (громадянської спільноти), має більш загострений суспільний зміст, більше навантаження суспільно корисного досвіду та підлягає коригуванню (актуалізації) залежно від історичних викликів та завдань, які стоять перед суспільством [2, с. 40]. Крім того, переважна більшість фахівців (істориків, соцілогів, психологів) дотримуються думки про штучне походження національної пам'яті.

На їхню думку, національна пам'ять є наслідком символічної та інструменталістської боротьби різних суспільних груп за те, якими мають бути образи їхнього спільного минулого. Національна пам'ять як відповідь на виклики сучасності відіграє важливу роль у процесах соціальної солідарності, колективної свідомості тощо. Будь-які репрезентації минулого є продуктом маніпуляції сучасних еліт, а суспільна пам'ять змінюється зі зміною політичної влади та суспільних домовленостей.

Період XVIII – XX ст. називають епохою націоналізму, саме тоді в Європі починають формуватися нації (в сучасному розумінні) і постають національні держави. Відбувається явище, яке відомий

англійський вчений Е.Гобсбаум назвав “винаходом традицій”. По-суті це процес масштабної і цілеспрямованої ідеологічної “імплантації” певних спільних культурно-політичних символів (національний прапор, національний гімн, національні свята, історичні постаті) у масову свідомість з метою інтегрування етнічного населення певної території в більш згуртовану, культурно однорідну спільноту – націю. “Нація” у цьому варіанті – результат суспільної інженерії з обов’язковим застосуванням технологій маніпулювання свідомістю, свідомо сконструйована спільнота [3].

При цьому в галузі історіографії науковий підхід до інтерпретації складних перипетій у становленні певного народу, особливо стосовно стосунків із сусідніми народами, нерідко підмінявся впровадженням загальновизнаних національних міфів і стереотипів, які в свою чергу зберігали в собі пам’ять про давні кривди і утиски, сприяли зростанню міжетнічної напруги та слугували підґрунтям для екстремістських рухів. Тобто, наукове дослідження минулого, використання наукової методології для опису і пояснення історичних подій було визначено менш вартісним, порівняно зі створенням спрощених “картинок-схем” “героїчного” або “трагічного” минулого конкретного народу, які пропонувалися ідеологами національних рухів. У цьому контексті значна роль відводилася “редагуванню” минулого за допомогою політичного міфу та конструюванню історичної пам’яті.

Такий стан був наслідком так званої історичної політики, тобто дій певних суспільних і державних інститутів, спрямованих на політичну, культурну або соціальну мобілізацію чи то окремих сегментів суспільства, чи то суспільства в цілому, або на формування громадянської лояльності тим чи іншим інститутам або колективам (державі, нації, церкві тощо). Отже, провадження історичної політики в будь-якому випадку є необхідним завданням “держав, що націоналізуються”. Але тут ми спостерігаємо маніпулювання історичною свідомістю – один із способів соціального управління, шляхом створення нової або зміни існуючої думки щодо перебігу історичних подій, ролі певних осіб, причин явищ та їхніх наслідків, за допомогою цілеспрямованого впливу на суспільну або індивідуальну психологію, свідомість та підсвідомість; програмування думок і прагнень мас, їхніх настроїв і навіть психічного стану з метою забезпечити таку їхню поведінку, яка потрібна суб’єкту маніпулювання.

У річище подібної історичної політики владна верхівка чи домінуюча еліта завдяки маніпуляціям історичною свідомістю здійснює контроль над конструюванням знань (уявлень) про минуле. Цьому сприяє монополізація сфери освіти (держзамовлення на підручники,

в яких викладено офіційний курс історії для навчальних закладів), музейної й архівної бази, монументальної пропаганди, комомеративної діяльності.

Особливо яскраво такі маніпулювання історичною свідомістю проявили себе в ряді тоталітарних держав Європи у період між двома світовими війнами. Так, історична наука гітлерівської Німеччини базувалася на так званій "расовій теорії", яка розглядала історичний процес винятково як боротьбу рас – вищої (арійської) і нижчих. Усі видатні досягнення світової культури, на думку вчених ІІІ Рейху, створені представниками арійської раси, занепад же тих чи інших цивілізацій минулого пов'язаний із недотриманням расових законів і забрудненням нордичної арійської крові. На цих "наукових" положеннях базувалися претензія німців, як єдино чистих представників арійської раси, на світове панування, а також політика щодо "очищення" світу від неповноцінних рас.

Поступово серед політиків, фахівців у галузі маніпулювання свідомістю та працівників ЗМІ утверджується думка про те, що маніпулювання спогадами та пам'яттю є могутнім знаряддям управління індивідуальною і суспільною свідомістю, а отже управління процесами ідентифікації/самоідентифікації та консолідації спільнот, а значить і можливістю їх інтеграції/дезінтеграції. У процесі виявлення механізмів формування уявлень про минуле, у тому числі й на рівні масової свідомості, увагу науковців привернула політична складова цього механізму. Історики-постмодерністи зацікавились пам'яттю як засобом мобілізації політичної влади. Тому в історичних роботах, зорієнтованих на проблематику історичної пам'яті, найрозробленішою є тема "політики пам'яті": вивчення ролі політичного проекту, замовлення на формування та закріплення цінностей, знань про минуле з певною соціально-політичною метою.

Політика, яка означає контроль над колективною (національною) пам'яттю – це боротьба за контроль над суспільством. Ж. Ле Гофф зазначав, що колективна пам'ять "була і є важливим питанням у боротьбі за владу між суспільними силами. Однією з найбільших турбот класів, груп чи окремих індивідів, які панували і надалі панують в історичних суспільствах, є перетворення себе на господарів пам'яті і забування" [4, с. 250].

На жаль, Україні не вдається, на сьогодні, уникнути політизації історії. Публічні дебати щодо переоцінки минулого й формування нової версії національної пам'яті та власної історії перетворилися на невід'ємну частину політичної боротьби. І тому не дивно, що саме національна пам'ять сьогодні використовується як інструмент для численних маніпуляцій з боку різноманітних сил, адже завдяки їй

можна впливати на перебіг подій і прогнозувати національні настрої з різних питань, а отже і маніпулювати свідомістю громадян у своїх власних цілях.

Нині існує величезна кількість різноманітних технологій здійснення негативного впливу на духовно-ідеологічну сферу життєдіяльності суспільства. Їх можуть застосовувати спецслужби іноземних держав, терористичні організації, політизовані радикальні угруповання, кримінальні структури, транснаціональні корпорації та інші формальні й неформальні учасники сучасних міжнародно-правових відносин. В Україні маніпуляціями національною пам'яттю з великим завзяттям займаються, насамперед, різноманітні політичні угруповання.

Також рівень загрози підвищують і загальносвітові, глобалізаційні тенденції. Сучасні інформаційні засоби перетворили історію на "інформаційний продукт масового споживання", істотно підірвавши "монополію" науковців та "канонічних" підручників. Оцінки минулого серйозно впливають на морально-психологічний клімат у суспільстві. Навіть віртуально створені картини минулого виступають дієвим чинником, котрий визначає реальні уподобання й поведінку спільнот та індивідів, і не завжди на користь їм самим. З погляду забезпечення безпеки Української держави, протидії загрозам її інформаційній складовій, відповідні заходи із протидії їм дедалі більше і більше усвідомлюються фахівцями як одне із найістотніших, найактуальніших завдань у справі захисту державного суверенітету. Але беззаперечо й те, що вироблення дієвих моделей протидії загрозам такого гатунку можливе лише за умови об'єднання зусиль фахівців різних галузей: істориків, психологів, соціологів, політологів, працівників масмедіа та сектору безпеки.

## ЛІТЕРАТУРА

1. Соціально-економічний стан України: наслідки для народу та держави: національна доповідь / [за заг. ред. В.М.Гейця та ін.]. – К. : НВЦ НБУВ, 2009. – 687 с.

2. Вєдєнєєв Д. Національна пам'ять українського народу в контексті інформаційно-психологічних впливів глобалізованого світу / Д.Вєдєнєєв // Національна та історична пам'ять. Державотворчі та цивілізаційні здобутки українського народу : зб. наук. праць. – 2011. – Вип. 1. – С. 38–52.

3. Винайдення традиції / [за ред. Е.Гобсбаума та Т.Рейнджера] ; пер. з англ. М.Климчука. – К., 2005. – 448 с.

4. Касьянов Г.В. Danse macabre: Голод 1932–1933 років у політиці, масовій свідомості та історіографії (1980-ті – початок 2000-х) / Г.Касьянов. – К. : "Наш час", 2010. – 271 с.

*Шульмін С.О.,*
*Національна академія Служби безпеки України*

# ВІРТУАЛЬНА РЕАЛЬНІСТЬ ТА БЕЗПЕКА ОСОБИСТОСТІ

Поняття "віртуальна реальність" в сучасному значенні вперше використав наприкінці 80-х років XX ст. Жерон Ланьє, відомий діяч кіберкультури. За останні роки розвиток інформаційних технологій та формування знань про них актуалізували необхідність розуміння віртуальної реальності як у "широкому", так і в "вузькому" сенсах слова. У "широкому" сенсі – "віртуальна реальність" є результатом переживання людиною низки екзистенціально–психологічних станів (уява, фантазія, сон тощо). У "вузькому" сенсі – це комп'ютерна віртуальна реальність. Цей різновид формується відносно недавно, хронологічно він є останнім з віртуальних культурних форм, в яких об'єктивується феномен віртуальної реальності.

Тривалий час проблеми віртуалістики залишались на узбіччі філософської думки. За досить невеликий період спроби філософського аналізу віртуальної реальності набули певного рівня зрілості, а концептуальне оформлення цього феномену дає можливість активно включати їх до соціально-філософської проблематики.

У сучасній філософії "віртуальна реальність" досліджується в широкому спектрі. У тому числі концепції, пов'язані з оцінками впливу віртуальної реальності на природу людини, стан безпеки особистості. Все частіше говорять про загрозу деградації особи під впливом сучасних комп'ютерних технологій, про втрату людиною фундаментальних основ свого буття, про поширеність таких феноменів, як інтернет-залежність тощо.

На нашу думку, відповіді на ці і багато інших питань слід шукати на шляхах визначення онтологічного статусу віртуальної реальності. У філософській літературі є достатньо спірні, дискусійні варіанти вирішення цієї проблеми. Відомий російський дослідник С.Хоружий обґрунтовує можливість осягнення віртуальної реальності в межах енергійного дискурсу [1, 69]. Однак визначення ним віртуальності як недобуття свідчить про неявне визнання пріоритету за сутнісним дискурсом, що применшує статус і значення віртуальної реальності. Київський філософ І.Шамша взагалі вважає віртуальність "ознакою небуття" [2, 58].

Незважаючи на семантичну невизначеність понять "віртуальний" і "віртуальна реальність", звернення філософської думки до вивчення станів і способів буття з нефіксованим статусом дозволяє включити віртуальну реальність до обрію онтологічного розряду і визначити її як інтерактивну, символічну форму буття зі специфічними властивостями.

До основних властивостей віртуальної реальності слід віднести поліонтичність (множинність), ситуативну актуальність і ситуативну елімінованість, динамізм і незавершеність. Фахівці виділяють також так звану нон-процесуальність та високий креативний потенціал.

Відрізняються від традиційних і характеристики віртуального простору і часу. Простір, що формується інформаційними потоками, є мінливим, симуляційним, принципово відкритим, антиієрархічним, децентралізованим. Віртуальний час – багатомірний, відносний, зворотній.

Саме названі онтологічні особливості віртуальної реальності створюють сприятливі умови для різнопланового використовування її як в інтересах особистості і її безпеки, так і проти неї. Тому поділ антропологічних парадигм, що визначають впливи віртуальності на природу людини, на прогресистські та регресистські ми вважаємо однобічною абсолютизацією і розглядаємо більш плідною точку зору представників так званої вірогіднісної парадигми: характер впливів віртуальної реальності як специфічної форми буття на особистість і її безпеку залежить від вольових імпульсів, якими керується людина при переході до віртуальної реальності.

## ЛІТЕРАТУРА

1. Хоружий С.С. Род или недород? Заметки к онтологии виртуальности / С.С.Хоружий // Вопросы философии. – 1997. – № 6.

2. Шамша І.В. Віртуальність як ознака філософії небуття / І.В.Шамша // Науковий вісник Міжнар. гуманітарн. універ. : збірник наукових праць. – Вип. 2. – Одеса, 2011.

# ІНФОРМАЦІЙНА БЕЗПЕКА ОЧИМА МОЛОДИХ ДОСЛІДНИКІВ

*Артюх В.Ю.,*
*Інститут підготовки юридичних кадрів*
*для СБ України НУ "ЮАУ ім. Я.Мудрого"*

## СОЦІАЛЬНІ МЕРЕЖІ ЯК ДЖЕРЕЛО ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ДЕРЖАВИ ТА ОСОБИ

Тенденції розвитку суспільства диктують свої умови, яких індивід повинен дотримуватися, щоб відчувати себе частиною соціуму. Однією з таких умов у сучасному світі є використання соціальних мереж. Це явище стало настільки звичним та буденним для нас, що ми навіть не замислюємося про ті потенційні загрози, що можуть виникнути внаслідок такої звичної діяльності. Як свідчить статистика, на сьогодні близько 81 % інтернет-користувачів є учасниками соціальних мереж. Україна увійшла у п'ятірку країн, інтернет-користувачі яких найактивніше відвідують соціальні мережі [1]. Тому забезпечення інформаційної безпеки в цьому загальнодоступному, глобальному способі спілкування є одним з важливих питань порядку денного нашої держави та міжнародного товариства.

Не секрет, що соціальні мережі можуть використовуватися зловмисниками, у тому числі іноземними спецслужбами, для збирання інформації про особу – від її смаків та уподобань до членів сім'ї та друзів, а також для створення згубного маніпуляційного впливу на суспільство та державу в цілому.

Реєстрація на соціальних сайтах має природу цивільно-правового договору, у якому користувач добровільно погоджується на всі умови, що, на жаль, створені для захисту насамперед адміністрації цих сайтів. Тобто до відповідальності, фактично, притягнути нікого, адже користувач добровільно погоджується на всі негативні наслідки використання його особистої інформації адміністрацією сайту та будь-яких третіх осіб. Соціальні сайти функціонують в мережі Інтернет, яка є всесвітнім ресурсом, відповідно, забезпечувати інформаційну безпеку особи потрібно на міжнародному рівні у тісній співпраці з адміністрацією цих сайтів. При цьому необхідно діяти демократичним шляхом, не порушуючи основоположних прав та свобод людини та громадянина. Акцент при вирішенні цієї проблеми потрібно зробити на превентивних методах.

Вважаємо можливим виділити такі основні шляхи врегулювання діяльності соціальних мереж:

- створення відповідного міжнародного та національного законодавства;

- реорганізація та належний розподіл повноважень між уповноваженими органами;

- розробка і впровадження механізмів прийняття рішень у цій сфері;

- сприяння процесам самоорганізації;

- активне інформування суспільства про потенційну небезпеку;

- розробка й удосконалення підстав і порядку притягнення до юридичної відповідальності;

- використання методу моніторингу шляхом "контролю та перехвату";

- примусові заходи (закриття чи обмеження доступу до серверів).

Комплексна реалізація вказаних пропозицій, на наш погляд, здатна забезпечити національну безпеку держави та інформаційну безпеку особи у сфері функціонування соціальних мереж. Звичайно, все це потребує залучення фахівців різних галузей науки та значних матеріальних і фінансових вкладень держави. Наприклад, США витрачають на кібербезпеку $14 мільярдів (весь державний бюджет України становить близько $50 мільярдів). За неофіційною інформацією для забезпечення безпечної роботи соціальних мереж потрібно близько 15 млн. грн. в місяць [2]. Для України це значна сума, але витрати на забезпечення національної безпеки в кінцевому результаті завжди будуть виправдані.

## ЛІТЕРАТУРА

1. Центр стратегічних досліджень [Электронний ресурс]. – Режим доступу : http://www.niss.gov.ua/articles/534/.

2. Користувачі соціальних мереж допомагатимуть міліції та СБУ. А поки що в Україні воюють з кіберзлочинцями на допотопних комп'ютерах [Електронний ресурс]. – Режим доступу : http://uzhgorod.in/ua/statti/2012/aprel/koristuvachi_social_nih_merezh_dopomagatimut_miliciyi_tasbu.

*Богословець Д.В.,*
*Європейський Університет*

## ІНФОРМАЦІЯ В ЖИТТІ ДЕРЖАВИ ТА СУСПІЛЬСТВА

Бурхливий розвиток інформаційних технологій, який особливо активізувався наприкінці XX століття, призвів до переоцінки ролі деяких компонентів національної безпеки. Внаслідок так званої інформаційної революції особливого значення набуває інформація. Інформатизація та комп'ютеризація докорінно змінили обличчя суспільства.

У цій ситуації однією з найважливіших складових національної безпеки стає інформаційна політика держави, яка в свою чергу формує умови для належної присутності держави на світовій арені.

Розглядаючи сутність інформації та її значимість в житті суспільства і окремої особистості, у багатьох джерелах прийнято цитувати відомі слова батька кібернетики Норберта Вінера: "Інформація – це інформація, а не енергія і не матерія". У цьому визначенні інформація становить окрему категорію поряд з енергією та матерією. Але слід зазначити, що інформаційні процеси неможливі без використання цих двох субстанцій і нерозривно пов'язані між собою.

"Інформація – це позначення змісту, що одержується із зовнішнього світу в процесі нашого пристосування до нього і пристосування до нього наших почуттів. Процес одержання і використання інформації є процесом нашого пристосування до випадковості зовнішнього середовища і нашої життєдіяльності в цій сфері" (Н.Вінер). Іншими словами, інформація проникає у всі пори життя людей і суспільства, а життя неможливе в інформаційному вакуумі.

Щодо визначення провідної ролі інформації слід сказати, що вона майже завжди займала вагоме місце в житті людини. Еволюція людства, формування нашого суспільства та виникнення державних інституцій завжди були пов'язані з накопиченням, поширенням та обробкою відповідної інформації.

Важко собі уявити повноцінну людську спільноту без інформаційних процесів, де відсутній обмін мовною чи малюнково-письмовою інформацією, спілкування між окремими особистостями. Інтелект дає можливість .людині, на відміну від тварин, повноцінно сприймати інформацію від навколишнього середовища, робити осмислені висновки та породжувати нову інформацію, обмінюватися нею.

За допомогою інформації можна впливати на зміну свідомості і поведінку людей, що само по собі може бути небезпечним для держави в цілому. Будь-яка культура породжує свою систему символів та стереотипів, яка стає основою національного суспільства.

## ЛІТЕРАТУРА

1. Бондаренко В.О. Інформаційна безпека сучасної держави: концептуальні роздуми / В.О.Бондаренко, О.В.Литвиненко // www.crime-research.iatp.org.ua/library/strateg.htm.

2. Інформаційна потужність держави, як складова національної безпеки // propolis.com.ua/node/13.

*Буновський А.В.,*
*Національна академія Служби безпеки України*

# ЗАХИСТ ІНФОРМАЦІЙНИХ РЕСУРСІВ ДЕРЖАВИ ЯК ФУНКЦІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

Інформація як результат інтелектуальної творчої діяльності має колосальний потенціал забезпечення ефективного державного управління та розвитку громадянського суспільства. Не є винятком й інформаційні ресурси, створені державою (державними органами). Однак переважно економічні чинники зумовлюють практичну доцільність чіткого визначення переліку і форм інформаційних ресурсів держави. Не менш важливим є осмислення питання захисту інформаційних ресурсів держави з огляду на їх вартість, важливість для ефективного державного управління і, звичайно, з урахуванням можливої шкоди внаслідок несанкціонованого оприлюднення (розкриття) відповідних відомостей. Захист інформаційних ресурсів є одним із пріоритетних завдань національної безпеки України. В умовах постіндустріального етапу інформація, інформаційні ресурси перетворились на стратегічний ресурс економічного і науково-технологічного прогресу та є важливим фактором успішної внутрішньої і зовнішньої політики й національної безпеки.

З огляду на викладене визначимо, що "інформаційні ресурси держави" – це взаємозв'язана, упорядкована, систематизована, закріплена на матеріальних носіях інформація, яка створена, зібрана на законних підставах органами державної влади або іншими суб'єктами за рахунок державного бюджету.

Отже, на нашу думку, "захист інформаційних ресурсів держави" доцільно визначити як діяльність уповноважених державних органів, що спрямована на попередження, усунення (нейтралізацію) або послаблення загроз (небезпек) взаємопов'язаній, упорядкованій, систематизованій, закріпленій на матеріальних носіях інформації, яка створена, зібрана на законних підставах органами державної влади або іншими суб'єктами за рахунок державного бюджету, з метою запобігання несанкціонованим діям з цією інформацією.

Як свідчить іноземний досвід, функція захисту інформаційних ресурсів держави в більшості випадків покладається на спецслужби.

Тепер перейдемо безпосередньо до діяльності Служби безпеки України у сфері захисту інформаційних ресурсів держави. Служба безпеки України – це державний правоохоронний орган спеціального призначення, який забезпечує державну безпеку України. До завдань СБ України віднесено захист державного суверенітету, кон-

ституційного ладу, територіальної цілісності, економічного, науково-технічного і оборонного потенціалу України, законних інтересів держави та прав громадян від розвідувально-підривної діяльності іноземних спеціальних служб, посягань з боку окремих організацій, груп та осіб, а також *охорона державної таємниці*. [10, ст.ст. 1, 2]. СБ України, яка визначена законодавцем як один із суб'єктів забезпечення національної безпеки України [11, ст. 4], є одним із провідних суб'єктів реалізації державної політики України в інформаційній сфері.

Діяльність СБ України в інформаційній сфері держави здійснюється властивими їй формами і методами, передбаченими законами України "Про Службу безпеки України", "Про оперативно-розшукову діяльність", "Про контррозвідувальну діяльність" та ін., у тісній взаємодії з іншими суб'єктами забезпечення національної безпеки та спрямована на нейтралізацію загроз національним інтересам і національній безпеці України.

## ЛІТЕРАТУРА


1. Соснін О. Національні інформаційні ресурси у сучасних умовах: проблемні питання вітчизняного законодавства / О.Соснін // Право України. – 2003. – № 10. – С. 124–128.
2. Сировой О.В. Організаційно-правові засади управління інформаційними ресурсами органів внутрішніх справ України : автореф. дис. … канд. юрид. наук: 12.00.07 / О.В. Сировой – Х. : Харк. нац. ун-т внутр. Справ, 2006. – 20 с.
3. Марущак А.І. Щодо поняття "інформаційні ресурси держави" / А.І.Марущак // Інформаційна безпека людини, суспільства, держави. – 2009. – № 1(1). – С. 11–15.
4. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України // ВВР України. – 2006. – № 30. – Ст. 258.
5. Про бібліотеки і бібліотечну справу : Закон України // ВВР України. – 1995. – № 7. – Ст. 45.
6. Концепція формування системи національних електронних інформаційних ресурсів, затверджена Розпорядженням Кабінету Міністрів України від 05.05.2003 р. № 259-р.
7. Вавженчук В.Я. Сутність та зміст захисту трудових прав у законодавстві України / В.Я.Вавженчук // Юридична наука і практика. – 2011. – № 1. – С. 89–94.
8. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України // ВВР України. – 1994. – № 31. – Ст. 286.
9. Про інформацію : Закон України // ВВР України. – 1992. – № 48.

10. Про Службу безпеки України : Закон України // ВВР України. – 1992. – № 27. – Ст. 382.

11. Про основи національної безпеки України : Закон України // ВВР України. – 2003. – № 27. – Ст. 45.

12. Доктрина інформаційної безпеки України від 08.07.2009 р., затверджена указом Президента України № 514/2009 // Режим доступу : www.president.gov.ua.

13. О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации от 15 января 2013 р., утверждена указом президента РФ № 31с // Режим доступу : http://www.pravo.gov.ru/laws/acts/4/51491089.html.

*Грошко П.І.,*
*Європейський університет*

## ІНФОРМАЦІЙНА БЕЗПЕКА ЯК НЕВІД'ЄМНА СКЛАДОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ ДЕРЖАВИ

В умовах зростаючих взаємозв'язків і взаємозалежності держав при збереженні багатьох глобальних небезпек і загроз національна безпека стає складовою загальної світової безпеки, зусиль усіх народів у збереженні миру, демократії, гуманізації сучасних відносин.

Важливою змістовною складовою національної безпеки є інформаційна безпека. Із зростанням науково-технічного прогресу буде зростати і важливість питання інформаційної безпеки громадянина, суспільства, держави. Тобто інформація стала чинником, який може призвести до значних технологічних аварій, військових конфліктів та поразок у них, дезорганізувати державне управління, фінансову систему, роботу наукових центрів, і чим вищий рівень інтелектуалізації та інформатизації суспільства, тим потрібнішою стає надійна інформаційна безпека, оскільки реалізація інтересів, людей та держав все більше здійснюється за допомогою інформатизації [1].

Враховуючи той факт, що під впливом інформаційних атак може цілеспрямовано змінюватися кругозір та мораль як окремих осіб, так і суспільства в цілому, нав'язуються чужі інтереси, мотиви, спосіб життя, на перший план виходить аналіз сутності та форм проявів сучасних методів скритого агресивного впливу, виявлення дій, що мають цілеспрямований агресивний характер і які протирічать інтересам національної безпеки, вироблення механізмів протидії їм у всіх напрямах.

Комісія з питань національної безпеки визначила такі потенційні загрози в інформаційній сфері:

- незбалансованість державної політики та відсутність необхідної інфраструктури в інформаційній сфері;
- повільне входження України до світового інформаційного ринку;
- відсутність у міжнародного співтовариства об'єктивного уявлення про Україну;
- інформаційна експансія з боку інших країн;
- відтік інформації, що містить державну таємницю, а також конфіденціальної інформації, що є власністю держави.

Інформаційна безпека здатна нейтралізувати такі впливи. Недостатню координацію діяльності вищого державного керівництва, органів влади та військових формувань у реалізації єдиної державної політики забезпечення національної безпеки теж можна вважати джерелом посилення організованої злочинності та збільшення кількості комп'ютерних злочинів, зниження рівня освіченості громадян, що суттєво ускладнює підготовку трудових ресурсів для використання новітніх інформаційних технологій.

Інформаційна безпека суспільства та країни характеризується рівнем їх захищеності і, як наслідок, стійкістю основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, воєнної справи, суспільної свідомості тощо) стосовно небезпечних (дестабілізуючих, деструктивних, таких, що уражають інтереси країни, та ін.) інформаційних впливів. Вона обумовлюється спроможністю країни нейтралізувати такі впливи.

Інформаційна безпека особистості характеризується рівнем і якістю її інформування щодо реального стану справ у всіх сферах життєдіяльності, захищеністю її психіки і свідомості від небезпечних інформаційних впливів – маніпулювання, дезінформування, спонукання до самовбивства, образ тощо. Слід звернути увагу на принципову різницю в змісті понять "інформаційна безпека" і "безпека інформації". Безпека інформації – стан, що забезпечує захист інформації від загроз для неї.

Визначення інформаційної безпеки є комплексним і багатозначним. Інформаційна безпека є невід'ємною складовою безпеки національної [2].

Саме тому різні органи державної влади мають приділяти особливу увагу гарантуванню цієї безпеки, особливо в контексті неухильного руху розвинених суспільств (до яких активно, в силу нещодавніх політичних змін, намагається долучитися і наше суспільство) до всеохопної інформатизації всіх сфер їх життєдіяльності.

Особливо це стосується правоохоронних органів та органів безпеки, які мають не лише протидіяти інформаційним атакам всере-

дині держави та на міжнародному рівні, в контексті інформаційної війни (концепт, розглянутий нами вище), а й бути готовими до боротьби з новою категорією злочинів: кіберзлочинами – правопорушеннями в сфері інформаційних технологій.

Забезпечення інформаційної безпеки досягається у процесі свідомої цілеспрямованої діяльності органів виконавчої влади, щодо запобігання можливого порушення їх нормального функціонування в результаті дії загроз та небезпек.

Метою забезпечення інформаційної безпеки є створення нормальних умов функціонування конкретного міністерства, іншого центрального та місцевого органу виконавчої влади, а також проведення моніторингу стану інформаційної безпеки для розроблення оптимальної моделі функціонування системи забезпечення інформаційної безпеки

Розвиток держави неможливий без забезпечення її безпеки в усіх сферах, що відносяться до державної компетенції. Через те найважливішою особливістю соціальної форми розвитку є якнайтісніший зв'язок та взаємозалежність між розвитком і безпекою як двома сторонами загального процесу життєдіяльності відкритої соціальної системи. Первісним є розвиток; безпека - вторинна й покликана забезпечити цей розвиток, захистити його від різних загроз.

## ЛІТЕРАТУРА

1. Баринов А. Информационный суверенитет или информационная безопасность? / А.Баринов // Національна безпека і оборона. – 2001. – № 1. – С. 70–76.

2. Богуш В.М. Інформаційна безпека держави / В.М.Богуш, О.К.Юдін. – К. : "МК-Прес", 2005. – 432 с.

*Євдокимов Ю.О.,*
*Інститут підготовки юридичних кадрів*
*для СБ України НУ "ЮАУ ім. Я. Мудрого"*

## УДОСКОНАЛЕННЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ ТА СПЕЦІАЛЬНИХ СЛУЖБ УКРАЇНИ

Розвиток людського співтовариства на сучасному етапі характеризується процесами глобалізації, тенденціями до формування пріоритетів сталого розвитку цивілізації та інформатизації. Ці в цілому позитивні тенденції супроводжуються не менш масштабними

деструктивними явищами й процесами: боротьбою за новий геополітичний порядок, міжнародним тероризмом, інформаційними війнами [1].

Інформаційні ресурси в силу зростання їх ролі в системі соціальних зв'язків набувають не тільки ролі стратегічного національного ресурсу, але й зумовлюють формування інформаційних методів управління соціальними процесами регуляції і саморегуляції поведінки людей. Складаючи основу управлінської діяльності, інформація в процесі її переробки та аналізу перетворюється в управлінські рішення в самих різних сферах життєдіяльності людини. З урахуванням цього, ефективність інформаційно-аналітичної діяльності набуває все більш вагомого значення у всіх сферах діяльності, і перш за все – у діяльності правоохоронних органів і спеціальних служб.

Сутність інформаційно-аналітичного забезпечення правоохоронних органів та спецслужб полягає в доцільній діяльності людини, спрямованій на вихідні фактичні дані, з тим, щоб використовуючи відповідні технічні засоби та аналітичні технології, перетворити їх у форму, придатну для розв'язання завдань виявлення, попередження, припинення і розкриття правопорушень та злочинів, розшуку правопорушників і злочинців, які сховалися, а також безвісти зниклих громадян, протидії розвідувально-підривній діяльності та іншим загрозам державній безпеці України. Ядром інформаційно-аналітичного забезпечення є інформаційно-аналітична діяльність як поглиблений моніторинг процесів у суспільно-політичній, економічній, екологічній, оборонній та інформаційній сферах, виявлення загроз і дослідження актуальних проблем національної безпеки, оцінка й прогнозування їх можливих наслідків. Її результатом є аналітична інформація.

У правоохоронному аспекті аналітична інформація може розумітися як принципово нова (по відношенню до вихідної) інформація, що містить оцінки, висновки, прогнози та пропозиції щодо перспектив, можливостей, умов і шляхів вирішення проблем забезпечення правопорядку та державної безпеки.

Як будь-яка інша організаційна система інформаційно-аналітична діяльність правоохоронних органів повинна удосконалюватися, змінюватися і розвиватися з урахуванням актуальних потреб, дотримуючись при цьому динамічної відповідності прав, розпорядчих функцій, відповідальності та ресурсів для досягнення результатів у належному обсязі, необхідної якості і своєчасності.

Однією з основних вимог, що висуваються до організації інформаційно-аналітичного забезпечення правоохоронних органів та спецслужб, є системність інформації, а також безперервність її збору та аналізу. Значну роль в оптимізації інформаційного забезпечення діяльності правоохоронних органів відіграє систематизація

інформації, що акумулюється в них. Вона забезпечується використанням різних обліків, стандартизація ведення яких спрямована на створення і гармонізацію єдиного інформаційного простору правоохоронних органів[2].

Важливим напрямом удосконалення інформаційно-аналітичної діяльності правоохоронних органів і спецслужб є їх інформатизація. Під нею розуміється процес організації оптимальних соціально-економічних і науково-технічних умов для задоволення інформаційних потреб зазначених органів, що змінює весь комплекс способів та умов розвитку інформаційних процесів, а також створення відповідної технічної бази та необхідного нормативно-правового забезпечення. За рахунок інформатизації забезпечується впровадження передових технологій у процес збору, систематизації, зберігання та аналізу інформації, а також використання соціально орієнтованих методів управління як самою системою правоохоронних органів, так і зовнішніми по відношенню до неї об'єктами.

Перспективою розвитку процесів інформатизації є створення єдиної інформаційно-телекомунікаційної інфраструктури, що забезпечуватиме функціонування єдиного інформаційного простору правоохоронних органів, необхідного рівня інформаційної безпеки та впровадження електронного документообігу і діловодства. Це зумовлює необхідність розробки нових і модернізації існуючих інформаційних ресурсів правоохоронних органів та забезпечення оперативного віддаленого доступу до них, а також відповідну підготовку співробітників правоохоронних органів і спеціальних служб.

## ЛІТЕРАТУРА

1. Кузнецов И.Н. Информация: сбор, защита, аналіз : учебник по информационно-аналитической работе / И.Н.Кузнецов. – М. : ООО Изд. Яуза, 2001.

*Єрмачков О.В.,*
*Інститут підготовки юридичних кадрів*
*для СБ України НУ "ЮАУ ім. Я.Мудрого"*

## УДОСКОНАЛЕННЯ ПРАВОВИХ ГАРАНТІЙ ОХОРОНИ ПРИВАТНОГО ЖИТТЯ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОСОБИ

Проблема безпечного існування людини в XXI ст. за умов технологічних революцій набуває нового розвитку. Інформація стає об'єктом суперництва держав, організацій, окремих груп та осіб.

Інформаційна безпека особи нерозривно пов'язана з її приватним життям і потребує особливого захисту. Приватне життя як об'єкт правового впливу – це система суспільних відносин, що характеризують існування і визначають розвиток людини як приватної (пересічної) особи, стосуються тільки її, не пов'язані з виконанням нею публічних функцій, вилучені з поля зору громадськості, охороняються і захищаються правом. Чи може особа відчувати себе у безпеці, коли інформація про неї незаконно потрапляє у розпорядження інших осіб?

Інформаційна приватність гарантується ст. 32 Конституції України. Конституційне регулювання дотримання права на повагу до приватного життя узгоджується з низкою міжнародно-правових норм: ст. 12 Загальної декларації прав людини 1948 року, ст.8 Конвенції про захист прав людини і основоположних свобод 1950 року, п.1 ст. 17 Міжнародного пакту про громадянські і політичні права 1966 року та ін.; а також з національним законодавством: Цивільний кодекс, Закони України "Про захист персональних даних", "Про інформацію", "Про доступ до публічної інформації" та ін.

Відповідно до законодавства лише особа має право вільно, на власний розсуд, визначати порядок ознайомлення із сферою свого приватного життя інших осіб, держави та органів місцевого самоврядування, а також право на збереження її у таємниці, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини [4].

Враховуючи практику Європейського суду з прав людини, можна стверджувати, що "приватне" життя – не суворо окреслене захищене коло відносин, а велика зона з доволі розмитими кордонами. Ця обставина пов'язана з постійним розвитком суспільних відносин. Питання "приватності" повинно співвідноситися з правами інших осіб і суспільства. Держава контролює дотримання права на повагу до приватного життя не лише з боку державних службовців, але і з боку приватних осіб, наприклад приватних детективів або репортерів [2, с. 114].

Зазвичай втручання у приватне життя здійснюється лише з боку правоохоронних органів і відбувається в рамках оперативно-розшукової діяльності або негласних слідчих (розшукових) дій та є законним і співвідноситься з інтересами суспільства. Але трапляються випадки, коли у межах законно заведених оперативно-розшукових справ або кримінальних проваджень щодо реальних злочинців здійснюються спроби проведення заходів з прослуховування переговорів осіб, які реально не мають відношення до справи [3].

Також останнім часом у ЗМІ дедалі частіше можна зустріти інформацію про те, що правоохоронні органи і спецслужби прослухо-

вують засоби мобільного зв'язку, надають послуги приватним детективам у зібранні інформації про людину тощо. Де-юре, приватної детективної діяльності в Україні не існує. Але інтернет переповнений пропозиціями приватних детективів. Приватні детективи та детективні агентства в Україні діють поза межами правового поля, вони не вправі здійснювати будь-які оперативно-розшукові заходи. Приватним детективам надається право отримувати інформацію методами, які не заборонені законодавством. Але аналізуючи запропоновані приватними детективами послуги, більшість з яких обумовлені делікатним характером справи або конфіденційністю інформації, необхідні відомості не можуть бути отримані гласно. Отже, законодавче врегулювання приватної детективної діяльності, що й досі відсутнє, повинно гарантувати забезпечення конституційних прав людини, захист законних прав та інтересів підприємств (контроль за діяльністю приватних детективів, забезпечення таємниці отриманих результатів тощо) [1].

Почастішали випадки збирання і поширення журналістами інформації без дозволу особи. У приватне життя журналісти втручаються, зазвичай, у комерційних цілях (наприклад, підвищення рейтингу видання), нерідко це може бути "замовлення" зацікавлених осіб з метою "чорного PR". Оскільки журналістська діяльність має на меті публічне висвітлення певних фактів, передбачено механізм забезпечення права на повагу до приватного життя, закріплений Главою 20 Цивільного кодексу України [4], але він не завжди є ефективним.

Така діяльність підриває довіру населення до держави і закону, негативно позначається на стані захищеності прав і свобод громадян, а отже потребує відповідного реагування шляхом створення відповідних гарантій охорони приватного життя та захисту конфіденційної інформації про особу. Інформаційна безпека особи нерозривно пов'язана з її приватним життям і потребує особливого захисту.

Враховуючи вище викладене, пропонуємо:

1. Внести зміни до законодавства, передбачивши оприлюднення щорічного звіту зі знеособленими даними відносно зняття інформації з каналів зв'язку в порядку оперативно-розшукової діяльності та негласних слідчих (розшукових) дій: забезпечити доступ громадян до інформації про кількість дозволів, а також результативність інформації, отриманої таким шляхом, її необхідність у кримінальному судочинстві.

2. Виключити пункт 4.4.8. зі Зводу відомостей, що становлять державну таємницю, "Відомості про статистичні показники оперативно-розшукової, контррозвідувальної чи розвідувальної діяльнос-

ті, що дають змогу здійснити кількісну оцінку оперативних сил і засобів, які застосовувалися для здійснення цієї діяльності, але не розкривають об'єкти спрямувань цих заходів".

3. Ухвалити закон, що врегулює діяльність приватних детективів та детективних агентств.

## ЛІТЕРАТУРА

1. Гусаров С. Юристи пропонують узаконити приватних детективів / С.Гусаров // Голос України [Електронний ресурс]. – Режим доступу : http://golosukraine.com/publication/zakonoproekti/parent/6402-yuristi-proponuyut-uzakoniti-privatnih-detektiviv/#.UTTsaHYyqN0.

2. Комментарий к Конвенции о защите прав человека и основных свобод и практике её применения/ [под ред. В.А.Туманова]. – М. : "Норма". – 2002. – 336 с.

3. Морозов О.Л. Інформаційна безпека в умовах сучасного стану і перспектив розвитку державності / О.Л.Морозов // Віче. – 2007. – № 12. [Електронний ресурс]. – Режим доступу : http://www.viche.info/journal/598/.

4. Правове регулювання інформаційних відносин: законодавство, судова практика // [упоряд. В.С.Ковальський, О.С.Захарова, І.С.Примак]. – К. : Юрінком Інтер. – 2011. – 336 с.

*Касярум Я.О.,*
*Черкаський інститут банківської справи*
*Університету банківської справи НБУ*

## ПІДГОТОВКА КОМПЕТЕНТНИХ КОРИСТУВАЧІВ КОРПОРАТИВНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ ЯК ЗАСІБ ПОПЕРЕДЖЕННЯ ВНУТРІШНІХ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

Проблема інформаційної безпеки в Україні набула значущості з початку впровадження автоматизованих інформаційних систем до структури державних служб та економіки. Особливо актуалізувалась вона останнім часом. В Україні кіберзлочини входять в топ-5 найпоширеніших економічних злочинів. Кожна п'ята українська компанія в 2012 р. піддавалася кібератаці [1]. З іншого боку, за результатами дослідження провідного німецького оператора зв'язку Deutsche Telekom, який візуалізував карту країн – джерел кібератак,

Україна виявилася на 4 місці в світі за кількістю кібератак, що здійснюються з її серверів: 566531 атак [2]. Це примусило Кабінет міністрів України 6 березня 2013 р. схвалити законопроект "Про внесення змін до Закону України "Про основи національної безпеки України" щодо кібернетичної безпеки України" [3].

Проблема інформаційної безпеки має власну історію, але поки що не має перспектив завершення, її розвиток нагадує спіраль, яка поступово збільшується та набирає обертів. Удосконалення фахівцями інформаційної безпеки систем захисту інформації активізує зусилля зловмисників, спрямовані на її руйнування, спричинює більші втрати від помилкових ненавмисних дій користувачів. Таке враження, що у вирішенні цієї проблеми техніка і людина не навчилися взаємодіяти за певними правилами.

У проблеми інформаційної безпеки є два аспекти: боротьба із зовнішніми та внутрішніми загрозами. Досі між науковцями та практиками точаться суперечки щодо пріоритетності напряму боротьби. Тим часом, частина науковців вважає, що за останні роки в інформаційній безпеці відбулися певні зміни пріоритетів [4; 5]. Якщо раніше більшого значення надавали зовнішнім атакам на інформаційну систему, то сьогодні набуває важливості проблема боротьби з внутрішніми загрозами. Про це свідчать результати аналітичних звітів фахівців з інформаційної безпеки, аналіз публікацій та конференція з цього приводу (Лондон, 2010 р.) – "Людський чинник в інформаційній безпеці". До речі, у вітчизняних конференціях більша увага приділяється технічним і технологічним аспектам безпеки.

Р.Дейсі, К.Роудс, Е.Джонстон, фахівці США з безпеки інформації вважають, що у вирішенні цієї проблеми дуже важливим є навчання персоналу виконанню професійної діяльності в умовах систем захисту інформації (СЗІ): "…Технологія і люди повинні працювати разом, здійснюючи політику, процеси і процедури, які служать, як контрзаходи до ідентифікованих ризиків. Персонал, який навчений розсудливо оцінювати штатні процедури безпеки, може істотно зменшити уразливість системи. Володіння кращою технологією безпеки не гарантує захисту, якщо люди не навчені тому, як використовувати це належним чином. Технології вимагають персоналу, що освоїв певні знання і має навички зі здійснення безпеки" [6, с. 78].

Проблема інформаційної безпеки є актуальною для економіки, де інтенсивно впроваджуються інформаційні автоматизовані системи. Розширення доступу до фінансових послуг змусило фінансово-кредитні установи відійти від концепції "замкнених дверей". Науковці вважають, що за умов, коли локальна комп'ютерна мережа організації має тісний зв'язок із зовнішнім світом і вихід в інтернет, сис-

тема інформаційної безпеки є одним з її найуразливіших місць (М.Браіловський, М.Гербер і Р. вон Солмс, Г.Кавусоглу, Е.Коул, С.Норткат і Дж. Новак, Т.Оглрті, А.Олійник, Б.Скиба, Л.Стрельбицька і М.Стрельбицький, В.Хорошко та ін.). До цього часу було важко зробити певні висновки щодо дійсної картини комп'ютерних злочинів, бо організації, які понесли збитки, намагаються не розголошувати таку інформацію, оскільки це впливає на їх імідж, репутацію.

Нас цікавить такий важливий аспект проблеми інформаційної безпеки, як роль людського чинника в збереженні і захисті корпоративної інформації. Ця проблема є актуальною для банківської сфери діяльності та корпоративних організацій, які здійснюють економічну діяльність [4; 5].

Аналіз статистичних відомостей свідчить, що більшість корисливих зловживань у фінансово-кредитній та страховій галузі скоюються персоналом, що має легальний доступ до платіжних й інформаційних систем організації [5]. Окремі аналітики висловлюють думку, що в "зони підвищеного ризику" потрапляють особи, що займаються оформленням платежів і відповідають за роботу з банками-кореспондентами, співробітники бухгалтерії, вузькі фахівці кредитних і вексельних відділень банків" [7]. Поряд із внутрішньою інсайдерською злочинністю викликають занепокоєння й постійні порушення співробітниками організацій вимог СЗІ. Вони не мають характеру навмисного злочину, а пов'язані з негативними діловими якостями фахівця, недбалістю, недисциплінованістю, безвідповідальністю.

Із метою упередження порушень і злочинів, які здійснюють працівники організацій, існує кілька шляхів. Перший полягає в створенні потужної сучасної системи захисту інформації. Вирішення одного завдання неможливо без залучення фахівців і значних коштів. Водночас це не дозволяє уникнути внутрішніх порушень співробітниками системи безпеки організації. Другий шлях – це зміна ролі працівника на співвласника, який має певні активи в організації і тому зацікавлений в її ефективній роботі.

Третій шлях – формування економіста як компетентного користувача СЗІ – дає змогу зменшити кількість внутрішніх порушень вимог СЗІ. Отже, у програмах підготовки майбутніх економістів зовсім не відображено специфіку їх роботи в умовах СЗІ. Такий стан є незрозумілим, оскільки проблему захисту інформації вивчають фахівці з міжнародної економіки, з архівної справи та документознавства, студенти юрфаків. Для економіста, який буде працювати в банківській структурі, страховій компанії, займатися аудиторською діяльністю, працювати на виробництві, знання особливостей роботи в умовах СЗІ є необхідними. Відповідні знання можна сформувати при вивченні курсу "Безпека інформації в економічній діяльності".

Отже, зростання інформаційних ризиків економічної діяльності змусило переосмислити сучасні виклики та вимоги до професійної підготовки фахівців економічного профілю, яких готують ВНЗ України.

## ЛІТЕРАТУРА

1. Киберпреступность и бизнес: что нельзя, а что – нужно [Электронный ресурс] – Режим доступа : http://www.cripo.com.ua – Дата: 06.03.2013.

2. Украина на 4 месте в мире по количеству исходящих кибератак [Электронный ресурс] – Режим доступа : http://ain.ua/tag/kiberprestupnost – Дата: 07.03.2013.

3. Уряд схвалив законопроект про кібернетичну безпеку України [Електронний ресурс] – Режим доступу : http://www.kmu.gov.ua/control/uk/publish/article?art_id=246124630&cat_id=244276429 – Дата: 06.03.2013.

4. Балановская А.В. Модель угроз информационной безопасности промышленных предприятий / А.В. Балановская // Вестник Самарского государственного экономического университета. – 2011. – № 9(83). – С. 19–23.

5. Банківське безпекознавство / [Л.М.Стрельбицька, М.П.Стрельбицький, В.К.Гіжевський] ; за ред. М.П.Стрельбицького. – К. : Кондор, 2007. – 602 с.

6. Information Security. Technologies to Secure Federal System / Robert F. Dacey, Keith Rhodes, Elizabet Johnston // GAO. Report to Congressional Requesters. – United States General Accounting Office. – Gao-04-467. – March 2004. – 89 p.

7. Варава А. В тихом банке инсайдеры водятся. – [Электронный ресурс]. – Режим доступа : http://www.bosinform.com/ru/bezopasnost-bankov/47-bankovskaja-bezopasnost/46-v-tihom-banke-insajdery-vodjatsja.html.

*Кісіль Н.О.,*
*Інститут спеціального зв'язку*
*та захисту інформації НТУУ "КПІ"*

## ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПЕРЕДАЧІ ДАНИХ У МЕРЕЖІ ІНТЕРНЕТ

Передача даних в інтернеті є дуже важливою, оскільки набуває комерційного характеру. Найбільш поширений спосіб безпечної передачі даних – використання криптографічного протоколу SSL (Socket Security Layer).

Такий протокол реалізований у всіх відомих веб-браузерах таких, як Google Chrome, Opera, Yandex та інших. SSL/TLS (Transport Layer Security) також широко використовується не тільки в браузерах. Наприклад, SSL/TLS використовується для передачі клієнтами платіжних реквізитів від серверів електронної комерції платіжних систем таких, як PayPal і Amazon, для обміну миттєвими повідомленнями клієнтів в онлайн-сервісах і аутентифікації сервера для мобільних додатків на Android і IOS.

Значний інтерес до захищеності SSL-з'єднань викликаний, зокрема, розвитком хмарних технологій. Все більше число компаній і домашніх користувачів використовують хмарні сервіси для зберігання, адміністрування і обробки важливої інформації, а підключення до таких служб в більшості випадків здійснюється через веббраузер з використанням технології SSL. Вразливість у системі захисту потенційно дає зловмисникам практично необмежені можливості для несанкціонованого доступу до конфіденційної інформації.

Тай Дуонг (Thai Duong) і Джуліано Ріццо (Juliano Rizzo), відомі дослідники комп'ютерної безпеки, володарі премії Pwnie Awards 2011 за розробку методу компрометації додатків ASP.NET, на конференції Ekoparty 7 розкрили завісу над новим способом атаки на SSL/TLS. Вони виявили серйозні слабкості практично у всіх сайтах, захищених Secure Sockets Layer протоколом, які дозволяють зловмисникові розшифрувати дані, які проходять між веб-сервером і браузером користувача [1].

Для здійснення атаки створено інструментарій, що відомий під ім'ям BEAST (Browser Exploit Against SSL/TLS) і дозволяє організувати перехоплення переданого в рамках зашифрованого з'єднання Cookie з параметрами аутентифікації користувацької сесії [2]. Зокрема, дослідники продемонстрували успішне перехоплення захищеної сесії для сервісу PayPal і стверджують, що метод можна застосовувати і для будь-яких сайтів. Вразливість знаходиться у версії 1.0, версії TLS 1.1 і 1.2 не піддаються такій атаці. Нині BEAST потрібно близько 2 секунд щоб розшифрувати байт зашифрованого cookie. Це означає, що аутентифікаційні cookie розміром в 1000-2000 символів буде розшифровуватися півгодини. Проте ця техніка становить загрозу для мільйонів сайтів, які використовують ранні версії TLS.

На сьогодніс існує наступна статистика сервісів, що підтримують протокол SSL/TLS [3]:

- TLS v1.2 підтримує 11 сервісів;
- TLS v1.1 підтримує 838 сервісів;
- TLS v1.0 підтримує 604242 сервіси;
- SSL v3.0 підтримує 607249 сервісів;
- SSL v2.0 підтримує 302886 сервісів.

Чергову уразливість протоколів SSL, TLS і SPDY продемонстрували недавно ті ж дослідники – Джуліано Ріццо і Тай Дуонг на конференції в Буенос-Айресі [3]. Атака з використанням нової вразливості отримала назву CRIME (Compression Ratio Info-leak Made Easy).

Під час атаки CRIME експлуатуються алгоритми стиснення даних. Отримавши повідомлення для відправки, SSL розбиває його на блоки, за необхідності стискає, обчислює код автентичності MAC, шифрує, додає заголовок і передає. Стиснення є необов'язковою, але часто використовуваною функцією SSL. Атака CRIME основана на зміні розміру стиснених повідомлень, наприклад, при додаванні аутентифікаційних даних Cookies. Той факт, що стиснення відбувається до шифрування, а інформація не піддається додатковій рандомізації, дозволяє зловмисникові розшифрувати повідомлення і, якщо вкрадені Cookies, провести несанкціоновану авторизацію в системі. Для проведення атаки CRIME на комп'ютер жертви необхідно завантажити шкідливий код. Це можна зробити, наприклад, перенаправивши користувача на інфіковану веб-сторінку.

Марш Рей (Marsh Ray) і Стів Діспенса (Steve Dispensa) з компанії PhoneFactor виявили критичну вразливість в протоколах SSL/TLS, що дозволяє зловмисникові організувати підстановку своїх даних у встановлюване між двома точками захищене з'єднання [4]. Для успішного проведення атаки зловмисник повинен мати можливість вклинитися в захищений трафік, наприклад, отримати контроль над проміжним шлюзом, проксі сервером або встановити своє обладнання в розрив мережевого кабелю.

Цей протокол часто використовується, не тільки у веб-браузерах, а й в інших додатках. У них, як правило, не реалізовується SSL/TLS протокол. Замість цього, вони покладаються на SSL/TLS бібліотеки, такі як OpenSSL/TLS, GnuTLS, JSSE, CryptoAPI і т.ін., а також більш високого рівня бібліотек, таких, як Apache, HttpClient, URLLIB, які виступають в якості "обгортки" навколо SSL/TLS бібліотеки. Дуже часто розробники таких додатків допускають помилки при реалізації, що призводить до зниження надійності бібліотек SSL/TLS.

Одним із критичних моментів протоколу, який реалізовано не в браузері, є підтвердження справжності сертифікатів. Робота Мартіна Георгієва (Martin Georgiev), Віталія Шматікова (Vitaly Shmatikov), Дена Бона (Dan Boneh) та інших зосереджена на поглибленому вивченні SSL/TLS аутентифікації, яка здійснюється в додатках і бібліотеках, призначених для роботи в Linux, Windows,

Android, і IOS операційних системах [4]. У роботі використовуються методи “білого” і “чорного” ящиків для виявлення вразливих місць. Головний висновок такої роботи полягає в тому, що підтвердження SSL/TLS сертифікатів повністю зламане у багатьох критично важливих додатках програмного забезпечення та бібліотек, також використовуються логічні помилки на стороні клієнта при підтвердженні SSL/TLS сертифікату. Причиною більшості з цих вразливостей є погане проектування API (програмних інтерфейсів) до основних SSL/TLS бібліотек. Розробники часто використовують програмні інтерфейси SSL/TLS API, маючи неправильне уявлення і погане розуміння їх параметрів, опцій, побічних ефектів, критичних значень. У ряді випадків можна спостерігати у роботах розробників впровадження нових вразливостей при спробі “виправити” помилки при перевірці сертифікатів. Крім того, розробники часто не розуміють, які властивості чи дані забезпечують безпечну реалізацію SSL/TLS протоколу: наприклад, вони використовують SSL/TLS бібліотеки, які не здійснюють перевірки сертифікатів, навіть якщо це необхідно (наприклад, під час здійснення процесу оплати товарів, послуг тощо). Бувають випадки, коли розробники включають в додаток проміжні шари програмного коду, що відключають перевірку сертифікатів випадково (наприклад, для тестування) або навмисно.

Незважаючи на широке практичне застосування SSL/TLS протоколу, цей протокол досить слабо досліджено за допомогою сучасних методів криптоаналізу [5].

## ЛІТЕРАТУРА

1. “Here Come The Ninjas”. Thai Duong, Juliano Rizzo May 13, 2011.

2. Juliano Rizzo, Thai Duong. “The CRIME attack”. Ekoparty. Retrieved 2012-09-21.

3. Documentation of Qualys SSL Labs: State of SSL 2010 v1.6 [Електронний ресурс] / Ivan Ristic. – Режим доступу : https://community.qualys.com/docs/DOC-1421.pdf.

4. Martin Georgiev, Subodh Iyengar, Suman Jana, Rishita Anubhai, Dan Boneh, Vitaly Shmatikov. The Most Dangerous Code in the World: Validating SSL Certificates in Non-Browser Software. Computer-Communication Networks. – 2012.

5. P.Morrissey, N.P.Smart, B.Warinschi. The TLS Handshake Protocol: A Modular Analysis. Journal of Cryptology April 2010.

*Ковальська І.О.,*
*Державний вищий навчальний заклад*
“*Національний гірничий університет*”

*Тимофєєв Д.С.,*
*Державний вищий навчальний заклад*
“*Національний гірничий університет*”

# ВИБІР МЕТРИК ЕФЕКТИВНОСТІ ПРОЦЕСІВ СУІБ

Інформаційна безпека відіграє важливу роль у формуванні процесу впровадження нових інформаційних технологій в усі сфери життя суспільства та людства в цілому. Широкомасштабне використання обчислювальної техніки й телекомунікаційних систем, збільшення обсягів інформації, що обробляється, та поширення кола користувачів приводить до якісно нових можливостей несанкціонованого отримання інформації.

Виділимо основні проблеми сфери захисту інформації [1, 2, 3]:

- неповнота організаційно-правової і нормативно-юридичної бази із захисту інформації;
- підвищення кіберзлочинності на підприємствах шляхом розвідки через розміщення на територіях, що охороняються, різних комерційних структур, підприємств і т. ін.;
- зношеність матеріально-технічної бази проведення робіт, особливо контрольно-вимірювальної апаратури, засобів обчислювальної техніки, зв’язку, оргтехніки;
- недостатній рівень фінансування створення та підтримки систем захисту і сучасних засобів захисту інформації.

Останнім часом в умовах тотального впровадження інформаційних технологій вирішити проблеми інформаційної безпеки важко через такі причини:

- інформація відносно просто копіюється дублюванням раніше створених інформаційних продуктів;
- у зв’язку з швидким розвитком інформаційних технологій значно ускладнено можливості контролю і запобігання несанкціонованому отриманню й використанню інформації з обмеженим доступом.
- різноманітність апаратних і програмних засобів формування, передачі, перетворення, відображення і зберігання інформації при впровадженні інформаційних технологій збільшує потенційні можливості формування нових каналів її витоку і порушення цілісності;

- достатнього рівня інформаційної безпеки може бути досягнуто тільки шляхом створення системи безпеки інформації, що реалізує державну політику, здійсненням управлінської, адміністративно-господарської і виробничої діяльності, підготовки кадрів відповідної кваліфікації та інших видів діяльності.

Саме через відсутність, недостатню впровадженість або старіння актуальності системи захисту інформації на підприємстві виникають різного рівня витоки інформації. Тому, на основі нормативних документів на стандарти інформаційної безпеки (ІБ), є необхідною розробка системи показників (метрик), за допомогою яких можна контролювати стан СУІБ.

Розрахунок метрик не є метою процесу оцінювання ефективності мір і процесів забезпечення інформаційної безпеки. Весь процес спрямований на те, щоб надавати інформацію, на основі якої будуть прийматися управлінські рішення в частині ІБ. Запроваджуючи процес оцінювання ефективності, необхідно продумати, як будуть аналізуватися результати його роботи, яким чином і ким будуть прийматися рішення з контролю і вдосконалення ІБ, як будуть оцінюватися результати внесених змін. Без цього цінність процесу оцінювання ефективності можна взяти під сумнів.

Під час процесу оцінювання ефективності ІБ необхідно бути готовим до прийняття управлінських рішень і їх виконання. Тільки в цьому випадку оцінювання ефективності з використанням метрик стане гнучким і зручним інструментом для оцінювання процесів і мір забезпечення ІБ. Їхнє впровадження дозволяє забезпечити роботу процесів інформаційної безпеки відповідно до очікування та цілей організації, обґрунтовано витрачаючи ресурси.

Можемо зробити висновок, що метрики необхідні для того, щоб:

- показати, яким чином діяльність із безпеки вносить безпосередній вклад у досягнення цілей безпеки;

- виміряти, як зміни в процесі відбиваються на досягненні цілей безпеки;

- виявити істотні аномалії в процесах і прийняти обґрунтовані рішення щодо їх виправлення чи поліпшення процесів [4].

Прикладом можливих для розрахунку ефективності СУІБ можуть бути метрики, відображені у таблиці 1.

Таблиця 1

Метрики розрахунку ефективності СУІБ

| № п/п | Назва метрики | Частота виміру | Одиниці виміру |
|---|---|---|---|
| 1. | Вартість системи захисту у разрахунку на одного співробітника (власного чи за контрактом) | 6 місяців | коштів на співробітника |
| 2. | Число вузлів КІС, на яких були протестовані механізми захисту | щорічно | відсоток |
| 3. | Час між виявленням уразливості та її усуненням | квартал | година |
| 4. | Число прикладних систем, для яких реалізована вимога поділу повноважень між операціями А і Б | 6 місяців | відсоток |
| 5. | Число ноутбуків із упровадженою підсистемою шифрування важливих і конфіденційних документів | квартал | відсоток |

## ЛІТЕРАТУРА

1. Правові основи охорони інформації / [В.Ф.Авраменко, Г.О.Брудний, С.І.Жлобін та ін.] ; за ред. В.О.Хорошка. – К. : ТОВ “ПоліграфКонсалтінг”, 2003. – 176 с.

2. Лазарєв Г.П. Шляхи вирішення проблем інформаційної безпеки в Україні / Г.П.Лазарєв, С.М.Кльоцкін, В.О.Хорошко // Захист інформації. – 2000. – № 2. – С. 4–9.

3. Дудикевич В.Б. Правові основи захисту інформації : конспект лекцій / В.Б.Дудикевич, В.С.Зачепило, В.В.Хома. – Львів : Вид-во Національного університету “Львівська політехніка”, 2002. – 168 с.

4. Метрики безопасности [Електронний ресурс]. – Режим доступу : http://dorlov.blogspot.com/2009/11/blog-post.html.

*Мазуркевич А.В.,*
*Національна академія СБ України*

# МЕХАНІЗМ ПРОТИДІЇ ІНТЕРНЕТ-ПРАВОПОРУШЕННЯМ: НАПРЯМИ ВДОСКОНАЛЕННЯ

Серед основних тенденцій розвитку інформатизації суспільства, що стосується практично всіх сфер життєдіяльності, включаючи економіку, державне управління, науку, мистецтво, слід відзначити стрімкий розвиток інформаційної мережі Інтернет. Започаткований у 1969 році, на сьогодні він є важливим фактором, що зумовлює успіх у бізнесі та науці, потужним засобом поширення преси, юридичних актів, місцем проведення дозвілля та спілкування людей.

Водночас, розвиток інтернету призводить до виникнення низки проблем: соціальних, організаційних, юридичних тощо, але найгострішою є активне використання мережі злочинним світом. Міжнародним суспільством кіберзлочинність (у т. ч. злочини, що вчиняються у мережі Інтернет) визнано загрозою не тільки національній безпеці окремих держав, а й людству та міжнародному порядку в цілому [1]. Зазначене зумовлює актуальність обраного напряму дослідження. Метою роботи є визначення особливостей та розкриття видів протиправного використання інтернету, аналіз негативних наслідків вказаних видів правопорушень, виявлення проблем, що впливають на ефективність боротьби з ними.

На підставі аналізу праць науковців, таких як Л.В.Бєлкіна, Н.Л.Волкова, Р.А.Калюжний, А.М.Кузьменко, В.К.Лисиченко, С.М.Стахівський та інші, публікацій у пресі й офіційних повідомлень правоохоронних органів можемо визначити особливості правопорушень у мережі Інтернет. А саме: анонімність [2]; доступність для широкого кола осіб, широка географії скоєння; віддаленість об’єкта протиправних посягань; багатоманітність способів скоєння та приховування слідів, використання злочинцями засобів шифрування інформації; складність виявлення, фіксації та вилучення доказів протиправної діяльності.

Що стосується видів протиправних дій, вчинених за допомогою інтернету, то їх на сьогодні налічується понад тридцять видів. На підставі запропонованої ще у 2000 році класифікації ООН [3] спробуємо визначити основні види найнебезпечніших із них:

1. *Спуфинг* – за допомогою використання різноманих технічних хитрощів “зламується” захист чужих комп’ютерів та одержується доступ до інформації, що в них зберігається.

2. *Промислове шпигунство* – крадіжка промислових секретів. За даними ООН таким способом вчинюється понад 90 % таких злочинів.

3. *Вандалізм* – це зміна або знищення хакерами веб-сайтів чи баз даних за допомогою отримання протиправного доступу до них.

4. *Перехоплення паролів* – за допомогою спеціального програмного забезпечення здійснюються протиправні дії під чужим ім'ям.

5. *Шахрайство* – один із видів злочинів проти власності. Це найпоширеніше протиправне діяння. О.О.Кіпа виділив кілька найбільш поширених і небезпечних видів шахрайства: фальшиві рахунки на оплату з інтернет-магазинів; шахрайський інтернет-магазин; інтернет-кардинг [4]; емейл-шахрайство.

6. *Піратство*. Сьогодні вживаються заходи щодо охорони інтелектуальної власності в Україні з метою забезпечення конституційних прав громадян на захист інтелектуальної власності, сприятливих умов для створення об'єктів інтелектуальної власності [5].

7. *Наркозлочинність у мережі Інтернет*. Мережа Інтернет є серйозною підмогою наркозлочинності. У зв'язку з чим, на нашу думку, важливим є застосування, крім правової боротьби, також громадського контролю за поширенням наркотиків у мережі. Все більшої актуальності набуває необхідність у таких запобіжних заходах, як розробка ресурсів з профілактики наркоманії на противагу пронаркотичним сайтам, а також створення громадських груп, наприклад журналістських, для введення добровільних обмежувальних правил публікації в мережі Інтернет матеріалів, пов'язаних із пропагандою наркоманії. Також вважається доцільним запропонувати низку превентивних заходів, таких, наприклад, як адміністративні та кримінально-правові заходи впливу до юридичних осіб (комп'ютерних компаній), що надають місце під сайти з інформацією про наркотики.

До зазначених вище видів протиправного використання інтернету, вважаємо за потрібне додати такий вид, як *використання інтернету для терористичних цілей*. Члени терористичних організацій за допомогою мережі створюють та відновлюють зв'язки незалежно від кордонів держави.

На сьогоднішній день кількість правопорушень у сфері інтернету постійно збільшується, а зловмисники вдосконалюють свої старі методи і створюють нові з такою швидкістю, що законодавство просто не встигає за розвитком технологій. На нашу думку, забезпечення успішної боротьби з протиправним використанням інтернету повинно відбуватись у двох напрямах. Перший – це розбудова належної законодавчої основи (прийняття нових та удосконалення існуючих нормативно-правових актів). Другий – створення дієвого органу державної влади з протидії інтернет-правопорушенням.

В Україні кримінальну відповідальність за скоєння комп'ютерних злочинів встановлено XVI розділом КК України –

“Відповідальність за злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж” [6]. Вважаємо за доцільне запропонувати удосконалення нормативного регулювання інших видів відповідальності – адміністративної та цивільно-правової.

Що стосується другого напряму – створення дієвого органу державної влади з протидії інтернет-злочинам, – то слід розглянути досвід іноземних країн. Так, у Міністерстві внутрішніх справ Російської Федерації для боротьби з комп’ютерними злочинами (мережевий злом, поширення комп’ютерних вірусів), незаконним оборотом заборонених радіоелектронних і спеціальних технічних засобів та загрозою проникнення в міжміські та міжнародні канали зв’язку створено спеціальний підрозділ – Управління по боротьбі зі злочинами у сфері високих технологій. У США створено Національний центр захисту інфраструктури (NIPC), завданням якого є попередження та розслідування комп’ютерних злочинів і координація роботи інших центрів, таких, як National Computer Crime Squad, San Jose Resident Agency, San Francisco Division, Cyber Emergency Support Team та ін.

В Україні також здійснюється формування спеціальних підрозділів електронної розвідки та протидії комп’ютерним злочинам як у Міністерстві внутрішніх справ України, так і в Службі безпеки України. Але зважаючи на обсяги протиправного використання інтернету, зазначені підрозділи об’єктивно не мають змоги масштабно протистояти сучасним загрозам.

Враховуючи таку специфіку інтернет-злочинності, як “відсутність кордонів”, пропонується створення самостійної міжнародної організації з протидії незаконному використанню інтернету або посилення повноважень інтерполу з протидії окремим видам інтернет-правопорушень. У будь-якому випадку до повноважень цього органу потрібно віднести: координацію сил між правоохоронними органами країн-членів, моніторинг та постійний обмін досвідом, аналітичною та статистичною інформацією стосовно протидії інтернет-правопорушенням, міжнародний розшук правопорушників тощо.

## ЛІТЕРАТУРА

1. Кіпа О.О. Правопорушення в мережі інтернет / О.О.Кіпа // Часопис Київського університету права. – 2010. - № 4. – С. 346-349.

2. Оніщенко Н. Проблеми протидії правопорушенням в інформаційній сфері: реалії та перспективи [Електронний ресурс] / Н.Оніщенко, С.Сунєгін // Віче. – 2012. – № 11. – Режим доступу : http://www.viche.info/journal/3151/.

3. Виды интернет-преступлений (за классификацией ООН) – [Електронний ресурс]. – Режим доступу – http://www.crime-research.org/library/ZAK_AVPR.htm.

4. Поняття Інтернет-кардингу. [Електронний ресурс]. – Режим доступу : http://arhiv-statey.pp.ua/index.php?newsid=26123.

5. Закон України "Про авторське право і суміжні права" від 11.07.2001 р.

6. Шахрайство за допомогою інтернету // Сайт-Мережа незалежних журналістів; [Електронний ресурс]. – Режим доступу : www.vlasti.net.

*Покришко А.О.,*
*Інститут підготовки юридичних кадрів*
*для СБ України НУ "ЮАУ ім. Я.Мудрого"*

## КІБЕРТЕРОРИЗМ – СУЧАСНА ЗАГРОЗА НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ

Стрімкий розвиток інформаційних технологій сприяв виникненню нового виду злочинності – комп'ютерної, а перехід на цифрові технології, методи електронного управління технологічними процесами, конвергенція і глобалізація комп'ютерних мереж стали передумовою появи нового виду тероризму – кібернетичного. Фахівці зазначають, що загроза поширення кібертероризму за рівнем негативного впливу може бути порівняна з реальними бойовими діями, особливо якщо це стосується руйнувань інформаційних систем стратегічно важливих об'єктів. Проблема захисту кіберпростору від несанкціонованого втручання в останні роки набула колосального масштабу в усьому світі [1]. За даними Ради Європи,тільки збитки від вірусів становлять приблизно 12 мільярдів доларів кожен рік [2, с. 58].

Дослідники проблем тероризму вважають, що кібертероризм проявляється у двох формах. По-перше, це комп'ютерні злочини, які вчиняються за допомогою спеціалістів - хакерів, серед яких:

– махінації та маніпулювання системами оброблення даних (несанкціонований переказ грошей тощо);

– шпигунство (проникнення до конфіденційних каналів зв'язку державних органів для отримання "чутливої" (критичної) інформації);

– диверсія (завдання шкоди технічному та програмному забезпеченню, що порушує функціонування державних органів та інших установ);

– незаконне користування комп'ютерними послугами (програмами, купівля за рахунок інших тощо).

По-друге, це розголошення захищеної законом таємниці, незаконний доступ до комерційної та конфіденційної інформації (що нерозривно пов'язане з першою формою):

– несанкціоноване отримання інформації для її нецільового використання особами, які не мають на це відповідного права;

– незаконний збір та переховування інформації;

– порушення правил користування конфіденційною інформацією [3].

Об'єктами посягання кібертерористів можуть бути автоматизовані системи управління державою, інформаційні системи і дані в цілому, об'єкти критичної інфраструктури (системи, мережі та окремі об'єкти, вихід з ладу яких призведе до непоправних наслідків для стабільності економіки та політичних процесів у державі, соціального благополуччя та здоров'я населення).

Єдиного визначення кібертероризму, закріпленого на законодавчому рівні, поки не існує, тому, враховуючи думку відомих фахівців із питань забезпечення інформаційної безпеки, можна запропонувати такий його варіант:

кібертероризм – це суспільно небезпечна, умисна, цільова діяльність у кіберпросторі, яка полягає в навмисній комплексній атаці на комп'ютерну інформацію, включаючи захоплення, виведення з ладу й руйнування об'єктів, що створює загрозу виникнення надзвичайної ситуації в телекомунікаційних мережах, заподіяння значної майнової шкоди чи настання інших суспільно небезпечних наслідків із метою порушення громадської безпеки, залякування населення, провокацій військового конфлікту, ускладнення міжнародних відносин, здійснення впливу на органи влади або привернення уваги громадськості до певних політичних, релігійних чи інших організацій. Характерною відмінністю кібертероризму від інших форм кіберзлочинності є його відкритість, коли вимоги терориста широко сповіщаються.

З огляду на заяви високопосадовців США та експертів, задіяних у підготовці нової Стратегічної концепції НАТО, щодо необхідності розглядати кібернапади на критично важливу інфраструктуру як "акт війни", які підпадають під статтю 5 Північноатлантичного договору, варто очікувати посилення дискусії на найвищому міжнародному політичному рівні (ОБСЄ, керівні органи НАТО, Генеральна Асамблея та Рада безпеки ООН, саміти Великої вісімки) щодо можливості закріплення відповідних змін у міжнародно-правових актах та статутних документах провідних міжнародних безпекових орга-

нізацій. Це дозволить ідентифікувати кібернапади або їх сукупність як акти війни. Існує цілком реальний ризик, що спроби ототожнення кібератак з "актами війни" можуть бути реалізовані на практиці. У такому разі Україна може опинитися в двозначній ситуації і стати об'єктом додаткового впливу з боку деяких держав як потенційне джерело небезпеки для критичної інфраструктури розвинених держав світу (через активність українських хакерів, що неодноразово відзначалося на міжнародній арені) [4, с.188].

Комп'ютерна злочинність України сьогодні перебуває на рівні США початку 80-х років. Але темпи і розвиток не можуть не насторожувати. Оцінюючи загрозу кібертероризму, слід ураховувати деякі особливості нашої країни. Це, по-перше, високий потенціал і професійний рівень програмістів, послугами яких охоче користуються навіть такі флагмани програмної індустрії, як Майкрософт. По-друге, здатність молоді швидко опановувати технічні новинки, про які ще вчора вони не мали жодної уяви. Ураховуючи той факт, що обчислювальна техніка постійно дешевшає, можна очікувати, що буде зростати й кількість користувачів інтернету в нашій країні. По-третє, хоча ще слабкий, але вже помітний підйом економіки неодмінно викличе зростання комп'ютеризації і ще на один-два кроки наблизить нас до країн з розвиненою інфраструктурою, що зробить загрозу кібертероризму цілком реальною. По-четверте, високий рівень централізації органів державного управління і низький рівень кваліфікації персоналу комп'ютерних систем можуть призвести до руйнування не досить захищеної інфраструктури [5].

Аналіз сучасного стану й тенденцій розвитку вітчизняного інформаційного простору дозволяє зробити висновок, що загроза кібертероризму для України з кожним днем набуває все більшої актуалізації, стаючи однією з сучасних проблем забезпечення національної безпеки та суверенітету України. У зв'язку з цим необхідно вжити адекватних заходів щодо посилення як законодавчих, так і організаційно-інституційних гарантій інформаційної безпеки в Україні. Вбачається, що одним з них має бути перегляд компетенції і, відповідно, структури правоохоронних органів і спецслужб України, зміна підходів щодо їх кадрового і технічного забезпечення у напрямі посилення захисту від кібернетичних посягань.

## ЛІТЕРАТУРА

1. Сивкович В. Сьогодні кібертероризм – це не віртуальна загроза / В.Сивкович [Електронний ресурс]. – Режим доступу : http://www.radioera.com.ua/eranews/?idArticle=44235.

2. Довгань О.Д. Кібертероризм як загроза інформаційному суверенітету держави / О.Д.Довгань, В.Г.Хлань // Інформаційна безпека людини, суспільства, держави. – 2011. – № 3 (7). – С. 49–53.

3. Бойченко О.В. Кібертероризм у складі сучасних проблем національної безпеки /О.В.Бойченко, О.О.Ончурова // Форум права. – 2010. – № 2. – С. 57–62 [Електронний ресурс]. – Режим доступу : http://www.nbuv.gov.ua/e-journals/FP/2010-2/10bovpnb.pdf.

4. Міжнародна конференція від 26 травня 2011 року на тему: "Інформаційні технології і безпека. Проблеми правового забезпечення кібербезпеки в сучасному світі" // Інформація і право : науковий журнал. – 2011. – № 3. – С. 187–189.

5. Голубєв В. Кібертероризм – загроза національній безпеці та інтересам України / В.Голубєв [Електронний ресурс]. – Режим доступу : http://www.justinian.com.ua/article.php?id=1002.

*Рубльов А.І.,*
*Університет банківської справи*
*Національного банку України (м. Київ),*
*Львівський інститут банківської справи*

*Нємкова О.А.,*
*кандидат фізико-математичних наук, доцент,*
*Університет банківської справи*
*Національного банку України (м. Київ),*
*Львівський інститут банківської справи*

## ЗАХИСТ ВІД ВТРУЧАННЯ В СИСТЕМУ ВІДЕОСПОСТЕРЕЖЕННЯ

В останні роки невпинного розвитку одноплатних комп'ютерів і обчислювальних платформ вдалося досягти значного зменшення розмірів плат та суттєвого збільшення енергоефективності. Тепер одноплатний комп'ютер за розмірами не більший за звичайну банківську платіжну картку і має обчислювальні потужності на рівні персонального комп'ютера 2000х років, а в деяких задачах, завдяки архітектурі, справляється навіть у рази краще за тогочасні.

У зв'язку із розвитком виробництва і ростом попиту споживачів на платформи такого виду було проведено масу робіт щодо покращання зручності використання цих засобів, таких як портування операційних систем сімейства Linux. Володіння повнофункціональ-

ними системами дає користувачу можливості працювати зі звичайними пакетами програмного забезпечення, які він має при використанні звичайних персональних комп'ютерів. Завдяки низькій вартості з'явилася можливість використовувати їх в реалізації систем розумного будинку, зв'язуючи в кластери для логічної взаємодії між системами. Також можливе їх використання в аматорській робототехніці та для вирішування безлічі інших завдань, з якими тільки здатен зіткнутися користувач.

Одним із цікавих прикладів застосування одноплатних обчислювальних платформ є використання таких пристроїв для непомітного втручання в різноманітні системи через мережеві інтерфейси. Можливе використання для звичайного сніффінгу потрібних пакетів з мережі. Завдяки наявності повноцінної операційної системи на борту і можливості доступу до інтернету користувач, який встановлює такий пристрій, може контролювати роботу пристрою дистанційно, вносячи корективи у перехоплені пакети (збереження пакетів, які містять нешифровану інформацію, хеші, тільки вхідні або вихідні, тощо). Це виокремлює їх в класі пристроїв цільового призначення, які здебільшого не мають такої гнучкості в управлінні, а мають бути попередньо налаштовані перед закладкою.

Одним із найцікавіших способів застосування у сфері втручання є підключення до мереж відеоспостереження, які використовують IP-камери. Напевно кожен бачив фільми, в яких персонажі задля приховування проникнення здійснюють втручання в систему відеоспостереження. Тепер для цього достатньо всього лише одноплатного комп'ютера (Raspberry Pi, Hackberry) з одноплатною обчислювальною платформою (Arduino, TI LaunchPad), або компактного автономного маршрутизатора з підтримкою прошивок DD-WRT і OpenWRT (TP-LINK TL-MR3040).

Для моделювання ситуації втручання в систему відеоспостереження шляхом прямого підключення до витої пари та пошуку запобігання такому втручанню було використано саме маршрутизатор TP-Link з прошивкою, яка базується на ядрі Linux.

До ключових етапів під'єднання стороннього пристрою можна віднести:

- попереднє налаштування на збір сигналу і запису у файл фейкової трансляції;
- під'єднання до цільового каналу;
- запуск на запис сигналу;
- початок транслювання записаного сигналу з файла;
- розрив лінії зв'язку між камерою і системою спостереження.

Сучасне програмне забезпечення практично не захищене від такого роду втручань, їх основний функціонал направлений на опти-

мізацію отриманого потоку з камер для подальшого збереження і навіть на аналіз картинки, виділяючи рухомі об'єкти на кадрі і акцентуючи на них увагу спостерігача.

У пошуках рішення було виділено ключові способи:

- На рівні камери:

- додавання в кадр малопомітної інформації (у вигляді шуму, що додається по каналу у зворотному зв'язку з системою або відповідно до попередньо закладених правил, згідно з якими шум додається при аналізі картинки камерою з великою кількістю не послідовних комбінацій);

- використання синхронізуючого сигналу від системи до камери, який і дописується на кадр (проте такий метод може виявитися не дієвим, якщо обчислювальних потужностей апарату, що втрутився в систему і перехоплює сигнал, достатньо для обробки потоку із самостійним додаванням синхронізуючого сигналу).

- На апаратному рівні:

- деякі сучасні камери обладнані одночасно двома інтерфейсами для зв'язку із системою, одночасне використання бездротового і дротового каналу із врахуванням похибки на затримку в сигналі при порівнянні шумів на кадрі має забезпечити можливість виявлення стороннього підключення.

- На рівні системи спостереження:

- Аналіз природних шумів, отриманих на зображенні, їх комбінацій, пошук повторів у наступних кадрах порівняно з попередніми.

Таким чином, на різних рівнях можна організувати непомітну зміну справжнього зображення, яка полягає у накладанні на сигнал наперед заданих слабких шумів. Подальша обробка сигналу повинна виявляти або наявність кореляції з відомими шумами, і тоді сигнал, прийнятий по телекомунікаційній системі, прийшов від камери. Або, якщо кореляція відсутня, можна стверджувати, що сигнал був підмінений, хоча на моніторі спостерігається нормальна картина приміщення. При реалізації цього методу виникає питання генерації потрібних шумів, що в принципі не є технічною проблемою. Шум із заданим спектральним розподілом можна синтезувати апаратно з білого шуму, або синтезувати у цифровому вигляді з подальшим додаванням до сигналу. Для посилення ефекту можна динамічно змінювати спектральну щільність шуму, задаючи, наприклад, для дискретних інтервалів часу визначений спектральний розподіл шуму. На дискретний інтервал часу накладається вимога, щоб він був довшим за час кореляції шуму. В решті решт можна використати в якості шуму наперед записане зображення людини або предмета, замінюючи його час від часу на інше.

Необхідність у вдосконаленні системи відеоспостереження для запобігання втручання в її роботу на сьогодні очевидна і потребує рішення, що можна зробити одним із запропонованих вище способів.

*Щербіна В.О.,*
*Національна академія Служби безпеки України*

## УДОСКОНАЛЕННЯ ЗАХИСТУ ІНСАЙДЕРСЬКОЇ ІНФОРМАЦІЇ ЧЕРЕЗ ПРИЗМУ ІНОЗЕМНОГО ДОСВІДУ

Економічна криза 2008 року в Україні, в тому числі негативні тенденції, які мають місце у сфері розвитку фондового ринку, знаходяться у непрямому зв'язку між слабким контролем за маніпуляціями цінними паперами та незаконним використанням інформаційної інфраструктури на фондовому ринку й конфіденційної інформації суб'єктів господарювання.

Одним із важливих аспектів забезпечення інформаційної безпеки, подолання економічної кризи та створення позитивного інвестиційного клімату в Україні є вдосконалення захисту суб'єктів господарювання від незаконного використання інсайдерської інформації.

Визначення "інсайдерської інформації", "інсайдерів" для нашого законодавства є новими та мають суттєві прогалини, що може створити передумови до поширення такого явища, як інсайдерська торгівля.

Метою наукового дослідження є аналіз та порівняння з міжнародними нормами й стандартами вітчизняного законодавства щодо відповідальності за незаконне використання інсайдерської інформації, а також запропонування заходів з його вдосконалення.

Вітчизняні науковці, які займались проблематикою інсайдерської торгівлі: В.Саєнко, О.Васильченко, І.Замойський, Ю.Капіцин, Н.Кузнєцова, О.Мозговий, В.Щербина та інші правознавці.

В українському законодавстві немає чіткого визначення "інсайдерської інформації", яке б адекватно відображало це поняття та відповідало визначенню у законодавстві ЄС щодо зловживання на ринку. Так, ч. 1 ст. 44 Закону України "Про цінні папери та фондовий ринок" відносить до інсайдерської інформації: неоприлюднену інформацію про емітента, його цінні папери та похідні (деривативи), що перебувають в обігу на фондовій біржі, або правочини щодо них, у разі якщо оприлюднення такої інформації може істотно

вплинути на вартість цінних паперів та похідних (деривативів), та яка підлягає оприлюдненню відповідно до вимог, встановлених цим Законом [1]. Таке визначення порівняно із європейським є дещо вузьким, оскільки відображає обмежене коло інформації. Наприклад у пропозиціях щодо регламенту Європейського парламенту та Ради про інсайдерську торгівлю та маніпулювання ринком (махінації на ринку) до інсайдерскої інформації також може бути віднесена:

(d) … інформація, надана замовником та пов'язана з невиконаними розпорядженнями замовника щодо фінансових інструментів, котра стосується, прямо чи опосередковано, одного або кількох емітентів фінансових інструментів чи одного або кількох фінансових інструментів, і яка у випадку її оприлюднення могла б справити суттєвий вплив на ціни таких фінансових інструментів, ціни відповідних угод із наявним товаром або ціни відповідних похідних фінансових інструментів;

(e) інформація, що … стосується одного або кількох емітентів фінансових інструментів чи одного або кількох фінансових інструментів, і зазвичай не доводиться до відома громадськості, але яка, за її наявності в розумно мислячого інвестора, котрий регулярно проводить операції на ринку та з відповідним фінансовим інструментом або відповідною угодою з наявним товаром, вважалася б такою особою доречною при ухваленні рішень про умови здійснення операцій із фінансовим інструментом або відповідною угодою з наявним товаром [2].

Особливістю чинного законодавства щодо інсайдерської інформації є наявність бланкетних (відсилочних) норм, що опосередковано відносять ті чи інші дані до інсайдерської інформації та різна юридична сила цих норм (наприклад: Закон України "Про цінні папери та фондовий ринок" [1], Рішення НКЦПФР №1688 від 22 листопада 2012 року "Про затвердження Положення про функціонування фондових бірж" [3] та проект Рішення НКЦПФР "Про затвердження Порядку виявлення та подання біржами НКЦПФР інформації про операції з цінними паперами та/або похідними (деривативами) у разі підозри використання інсайдерської інформації" [4]). Така тенденція може призвести до колізій у суді під час визначення того, чи мав емітент обов'язок розкривати ту чи іншу інформацію.

До інсайдерів (суб'єктів відповідальності), які вчинили протиправні дії, передбачені ст. 232-1 Кримінального кодексу України [5] або ст. 163-9 Кодексу України про адміністративні правопорушення [6], можуть відноситись наступні особи: посадові особи емітента, у тому числі ті, які були посадовими особами емітента на момент ознайомлення з інсайдерською інформацією; особи, які мають до-

ступ до інсайдерської інформації у зв'язку з виконанням ними трудових (службових) обов'язків або договірних зобов'язань незалежно від відносин з емітентом, у тому числі співробітники професійних учасників фондового ринку; державні службовці, яким відома інсайдерська інформація внаслідок виконання ними посадових (службових) обов'язків; особи, які ознайомилися з інсайдерською інформацією неправомірним шляхом; аудитори, нотаріуси, експерти, оцінювачі, арбітражні керуючі або інші особи, які виконують надані законом публічні повноваження [5].

Аналізуючи міжнародний досвід та пропозиції щодо регламенту Європейського парламенту і Ради про інсайдерську торгівлю та маніпулювання ринком (махінації на ринку) до інсайдерскої інформації [2], необхідно зазначити, що такий перелік суб'єктів відповідальності є дещо звуженим. До цього переліку необхідно також віднести: ЗМІ, які безпосередньо здійснюють оприлюднення інсайдерської інформації; банківські та кредитні установи, що уклали договори з емітентами та професійними учасниками ринку цінних паперів та мають опосередкований доступ до інсайдерської інформації та інші особи.

Для забезпечення дієвої протидії інсайдерській торгівлі застосовується взаємодія (та моніторинг) НКЦПФР з фондовими біржами, торговцями цінними паперами, правоохоронними органами, іншими установами й організаціями з метою профілактики і спостереження, виявлення і розслідування та заходами впливу в разі вчинення інсайдерської торгівлі. Моніторинг повинен здійснюватись за певними критеріями (наприклад: історії торгівлі певним цінним папером у хронологічному порядку із зазначенням часу, обсягу, ціни і контрагентів по кожній угоді тощо), бути актуальним та максимально наближеним до реального часу.

Особливою формою взаємодії між НКЦПФР та біржами є надання звітів останніми. Процес доказування також може ускладнюватись через строки подання звітності біржами. Розділ ІІІ Рішення НКЦПФР № 279 "Про затвердження Положення про порядок складання та подання адміністративних даних щодо діяльності торговців цінними паперами" [7] дозволяє лише через п'ять днів подавати звіт у НКЦПФР про укладені (виконані) угоди. Міжнародний досвід вимагає надавати такі звіти і обліковувати дані про транзакції в режимі реального часу або максимально наближеного до реального часу [2].

Для підвищення ефективності діяльності із забезпечення інформаційної безпеки суб'єктів господарювання пропонуємо наступні заходи:

- застосовувати у Законі України "Про цінні папери та фондовий ринок" [1] більш ширше визначення "інсайдерської інформації" для запобігання колізій;

- при перерахуванні в диспозиції статті суб'єктів відповідальності за незаконне використання інсайдерської інформації в кінці переліку зазначити фразу "… та інші особи, які в будь-який спосіб отримали інсайдерську інформацію". Таке широке тлумачення інсайдерів дозволить нам притягнути до відповідальності осіб, які використали інсайдерську інформацію та мають опосередковане відношення до емітента;

- на нашу думку, важливо щоб вимоги щодо подання звітів про угоди з цінними паперами на фондовій біржі знаходились у одному нормативно-правовому акті, були наближені до реального часу та відповідали критеріям моніторингу.

## ЛІТЕРАТУРА

1. Закон України "Про цінні папери та фондовий ринок" // Відомості Верховної Ради України (ВВР). – 2006. – № 31. – Ст. 268 [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/3480-15.

2. Пропозиції до Положення Європейського Парламенту та Ради Європи щодо інсайдерської торгівлі та маніпулювання на ринку (зловживання на ринку) [Електронний ресурс]. – Режим доступу : http://www.finrep.kiev.ua/download/idmm_materials_22feb2012_ua.pdf.

3. Рішення Національної комісії з цінних паперів та фондового ринку № 1688 від 22 листопада 2012 року "Про затвердження Положення про функціонування фондових бірж". [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/z2082-12/page1.

4. Проект Рішення Національної комісії з цінних паперів та фондового ринку "Про затвердження Порядку виявлення та подання фондовими біржами Національній комісії з цінних паперів та фондового ринку інформації про операції з цінними паперами та/або похідними (деривативами) у разі підозри використання інсайдерської інформації. [Електронний ресурс]. – Режим доступу : http://www.nssmc.gov.ua/law/17060.

5. Кримінальний Кодекс України, прийнятий Верховною Радою України 05.04.2001 р. №2341-III // Відомості Верховної Ради України, 2001. – № 25–26, ст. 131) [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/2341-14.

6. Кодекс України про адміністративні правопорушення // Відомості Верховної Ради Української РСР (ВВР) 1984, додаток до № 51, ст. 1122 [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/80731-10.

7. Рішення Державної комісії з цінних паперів та фондового ринку № 279 від 08 червня 2004 року “Про затвердження Положення про порядок складання та подання адміністративних даних щодо діяльності торговців цінними паперами”. [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/z1122-04.

*Марчук О.О.,*
*ЖВІ НАУ*

## ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СПЕЦІАЛІЗОВАНИХ ЕЛЕКТРОННИХ БІБЛІОТЕК

У процесі інформатизації суспільства електронні бібліотеки посіли важливе місце у забезпеченні інформаційного розвитку суспільства. Це стосується й структурних підрозділів, які займаються спеціалізованою інформаційною діяльністю.

Електронні бібліотеки можуть забезпечувати вирішення низки завдань:

- інформаційне забезпечення навчання особового складу підрозділів;
- надання допомоги при прийнятті рішень за рахунок надавання доступу до спеціалізованої літератури;
- об’єднання багатьох інформаційних ресурсів під єдиним керуванням;
- автоматизація пошуку електронних ресурсів;
- каталогізація електронних ресурсів.

Це визначає завдання створення спеціалізованих електронних бібліотек, які забезпечать зручний доступ до електронних ресурсів, розмежування доступу, безпеку електронних ресурсів, зручну каталогізацію ресурсів та їх автоматизований пошук.

Для вирішення цього завдання проведений аналіз існуючих електронних бібліотек та визначені їх основні переваги й недоліки. Також розглянуті основні підходи до побудови електронних бібліотек, на основі чого розроблений власний алгоритм для побудови спеціалізованої електронної бібліотеки та здійснена його програмна реалізація.

Слід сказати, що найбільш поширеними та зручними підходами до побудови електронних бібліотек є використання технологій систем управління базами даних (СУБД) та технологій семантичного

Web. Це дозволяє створювати зручні за інтерфейсом, з гнучким пошуком даних електронні бібліотеки.

Важливим питанням виступає забезпечення безпеки даних. Це можливо здійснювати за рахунок розмежування доступу, жорсткої авторизації доступу, використання захищених комп'ютерних мереж із обмеженням об'єднання з іншими комп'ютерними мережами.

*Мельничук А.Ю.,*
*Національна академія СБ України*

## ЗАХИСТ ПРАВ ЛЮДИНИ ПІД ЧАС ЗДІЙСНЕННЯ ДОСТУПУ ДО ПУБЛІЧНОЇ ІНФОРМАЦІЇ

У цій роботі будуть розглядатися проблеми доступу до публічної інформації, судова практика адміністративних судів України щодо застосування законодавства про доступ до інформації. Метою роботи є висвітлення проблем правового регулювання у сфері доступу до публічної інформації, а також розробка шляхів удосконалення законодавства.

Судова практика виявила певні складнощі реалізації положень законодавства про доступ до публічної інформації в Україні, які аналізуються нижче. Узагальнення, які наводяться, звичайно, не претендують на всеосяжність, а емпірична база охоплюється відкритими даними Єдиного державного реєстру судових рішень. Масив проаналізованих судових рішень складають рішення адміністративних судів України, винесені в 2011-2013 роках, які безпосередньо посилаються на Закон України "Про доступ до публічної інформації" [1]. Ми проаналізували 24 судових рішення [2].

Найбільша категорія справ, розглянутих судами, стосується випадків, коли *відповіді на інформаційний запит органом державної влади просто не було надано.* Таких справ серед дослідженого масиву було 12, що становить 50 % від усього масиву.

У більшості цих справ запитувачі не отримали жодної відповіді на свій запит. Хоча стаття 20 Закону України "Про доступ до публічної інформації" чітко встановлює обов'язок розпорядника інформації надати її особі за її запитом. А якщо запит не підлягає задоволенню, стаття 22 Закону України "Про доступ до публічної інформації" зобов'язує у письмовій формі надіслати відмову. Суд у цих випадках підійшов до всіх справ однозначно і визнавав протиправною бездіяльність розпорядників інформації.

Аналізуючи резолютивні частини судових рішень, хочемо звернути увагу на таке. У цих справах суд зобов'язував розпорядників інформації, по-перше, невідкладно надати відповідь на інформаційний запит, і, по-друге, повідомити суд про результати виконання постанови суду. З формальної точки зору адміністративний суд не може перебирати на себе повноваження органу виконавчої влади і приймати рішення, які належать до компетенції саме відповідача.

Наступна категорія справ – це суперечки із суб'єктами власних повноважень, в яких *відповідачами було порушено строки розгляду інформаційного запиту*. Таких справ знайдено 7, що становить 30 % від всього опрацьованого масиву. Ці справи цікаві тим, що відповідь на запит була отримана, проте пізніше, ніж встановлено.

Відповідно до статті 20 Закону України "Про доступ до публічної інформації", розпорядник інформації має надати відповідь на запит на інформацію не пізніше *п'яти робочих днів* з дня отримання запиту. А у разі, якщо запит стосується надання великого обсягу інформації або потребує пошуку інформації серед значної кількості даних, – до 20 робочих днів з обґрунтуванням такого продовження. У цих випадках суд ґрунтувався і обчислював строк із дати реєстрації інформаційного запиту у розпорядника.

У частині справ відповідачі не могли надати доказів того, коли надсилалися відповіді на запит. На таку практику суди реагували досить просто, визнаючи такі дії і бездіяльність розпорядників публічної інформації такими, що порушують вимоги закону.

Наступною є категорія спорів про *належність інформації до кола публічної*. У 3 справах (що складає 12 % від дослідженого масиву справ) суд визнавав інформацію публічною і такою, що підлягає наданню запитувачу. Відмовляючи у наданні інформації розпорядники мотивували це, як правило, тим, що вона є службовою, таємною або конфіденційною.

Стаття 21 Закону України "Про інформацію" [3] та стаття 6 Закону України "Про доступ до публічної інформації" дійсно визначають, що інформацією з обмеженим доступом є: конфіденційна інформація, таємна інформація, службова інформація.

Проте, як мотивував свої рішення суд, у цих адміністративних справах обов'язок доведення правомірності свого рішення, дії чи бездіяльності покладається на відповідача – суб'єкта влади. Саме він повинен довести, чому він прийняв таке рішення. А також повинен довести, з посиланням на конкретні норми законодавства, що інформація та документи, які просив надати позивач, не входить до зазначеного вище переліку.

Також вважаємо достатніми підстави виділити категорію справ, в яких адміністративний суд задовольняв вимоги про надання пуб-

лічної інформації, коли надана своєчасно відповідь на інформаційний запит була неповною. Слід відзначити, що в Законі України ,“Про доступ до публічної інформації” про повноту інформації згадується лише один раз. Відповідно до статті 23 Закону України “Про доступ до публічної інформації” запитувач публічної інформації має право оскаржити надання недостовірної або неповної інформації. Самого визначення “повна інформація”, або критеріїв “повноти інформації” закон не дає.

Вивчені справи свідчать, що судова практика певною мірою заповнила цю правову прогалину. Судді самі визначали і вказували у своїх постановах критерії “повноти інформації”. Так, у одній справі орган реєстрації прав на нерухоме майно не надав товариству дані про реєстрацію певного нерухомого майна та його власників. Товариство звернулось до адміністративного суду, просило в позові визнати відмову незаконною. Суд встановив, що відповідно до змісту Закону України “Про доступ до публічної інформації” відповідь на інформаційний запит має бути повною. Під “повнотою” в цьому випадку необхідно розуміти обґрунтовану, вичерпну та зрозумілу інформацію на кожне питання, яке викладене в інформаційному запиті.

На нашу думку, інформація про власників нерухомого майна завжди є персональними даними, а отже підпадає під особливий режим правової охорони. Однак не завжди така інформація підлягає зарахуванню до конфіденційної інформації. Адже відповідно до статті 6 частини 5 Закону “Про доступ до публічної інформації” не може бути обмежено доступ до інформації про розпорядження бюджетними коштами, володіння, користування чи розпорядження державним, комунальним майном, у тому числі до копій відповідних документів, умови отримання цих коштів чи майна, прізвища, імена, по батькові фізичних осіб та найменування юридичних осіб, які отримали ці кошти або майно. Отже, можна констатувати, що зазначені вище дані, хоч і є персональними, однак мають надаватись на запит будь-якій особі. При цьому випадки передачі земельних ділянок, об’єктів нерухомості (як житлового, так і нежитлового фонду) в порядку приватизації є актами розпорядження державним чи комунальним майном, і тому, на нашу думку, прізвища, імена, по батькові фізичних осіб та найменування юридичних осіб, які приватизували чи викупали земельні ділянки, квартири, приміщення нежитлового призначення, мають розкриватись за запитом про надання публічної інформації.

Інша категорія справ стосується *дотримання заявником процедури доступу до публічної інформації* (дві справи, 8 % від всього масиву). В одній із справ, мешканці села подали до сільської ради

колективний інформаційний запит щодо доступу до офіційних документів і щодо надання письмової інформації. У задоволенні запиту було відмовлено, оскільки він не відповідав встановленій формі для подання запитів, яка встановлена радою. Як визначив суд, відмова відповідача в наданні інформації позивачу з підстав невідповідності запиту формі є надуманою, адже статтею 6 Закону України "Про доступ до публічної інформації" не передбачено такої підстави для обмеження права громадян на отримання інформації, як невідповідність форми запиту будь-якому Закону.

## ЛІТЕРАТУРА

1. Судові рішення (результати пошуку). – [Електронний ресурс]. – Режим доступу : Єдиний державний реєстр судових рішень www.reyestr.court.gov.ua/searh83502480_adm%%%%%#%#%l%l%24%.

2. Закон України "Про інформацію" від 02.10.1992 № 2657-XII // Відомості Верховної Ради України 1992, № 48 від 01.12.1992.

3. Закон України "Про доступ до публічної інформації" від 13.01.2011, № 2939-VI // Голос України 2011, № 24 від 09.02.2011.

*Морозюк С.П.,*
*Національна академія СБ України*

## ШЛЯХИ ПІДВИЩЕННЯ РІВНЯ БЕЗПЕКИ КІБЕРНЕТИЧНОГО ПРОСТОРУ УКРАЇНИ

Важливість кібербезпеки стрімко зростає у сучасному світі. Із поширенням застосування інформаційних та комунікаційних технологій, їхнім впровадженням у найважливіші сфери життя країн, використанням як державними, так і комерційними структурами в управлінських процесах актуалізується питання безпеки кіберпростору.

Спостерігається висока вразливість кібернетичного простору перед кібератаками, діяльністю злочинних угруповань, хакерів, промислово-фінансових груп та осіб, допущених до роботи з системами в порядку здійснення службової діяльності (інсайдерів). Випадки негативного кібервпливу стають частішими, організованішими, більш легкими та дешевими в підготовці і реалізації.

Серйозне занепокоєння у світі викликає потенційна можливість прихованого кібервпливу на об'єкти критичних інфраструктур, ключових секторів економіки, від стану яких залежить безпека дер-

жави і суспільства (енергетика, водопостачання, транспортні системи та інші). Так як управління ними здійснюється в основному за допомогою автоматизованих систем, результатом такого впливу може стати дезорганізація роботи цих життєво важливих галузей.

Збільшується активність спецслужб держав щодо розвідувальної діяльності в комп'ютерних мережах. Кібершпигунство стає майже непомітним та безперешкодним.

У зв'язку із все частішим застосуванням кібернетичної зброї у воєнних та політичних конфліктах виникла тенденція мілітаризації кібернетичного простору, який став новою ареною протистояння держав.

Із впевненістю можна сказати, що і в майбутньому кіберпростір буде невід'ємною складовою у міждержавних конфліктах, але лише допоміжним елементом протистоянь. Незважаючи на високу оцінку ризиків кібератак, мілітаризовані контрзаходи будуть не завжди ефективними у забезпеченні кібербезпеки.

Більшість провідних держав світу вже розробили та реалізують власні стратегії кібербезпеки, зокрема:

- *США*: – Стратегія діяльності в кіберпросторі (Strategy for Operating in Cyberspace) Міністерства оборони США;

- Міжнародна стратегія кіберпростору: розвиток, безпека та відкритість у мережевому світі (International Strategy for Cyberspace: Prosperity, Security,and Openness in a Networked World) Білого дому;

- Концепція безпечного кібернетичного майбутнього: Стратегія кібернетичної діяльності в забезпеченні національної безпеки (Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise) Департаменту національної безпеки.

- *Велика Британія:* Стратегія кібербезпеки Великої Британії: захист і сприяння в цифровому світі (Cyber Security Strategy: Protecting and Promoting the UK in a Digital World).

- *Франція:* Захист і безпека інформаційних систем: французька стратегія (D?fense et s?curit? des syst?mes d'information: Strat?giede la France) прем'єр-міністра Франції.

- *Німеччина:* Стратегія кібербезпеки Німеччини (Cyber Security Strategy for Germany) федерального Міністерства внутрішніх справ.

- *Голландія:* Національна стратегія кібербезпеки: успіх через співпрацю (The National Cyber Security Strategy (NCSS): Success through cooperation).

У цих документах на державному рівні визначено основні засади, шляхи та об'єкти забезпечення кібернетичної безпеки, яка визначається одним із пріоритетних напрямів розвитку.

Проаналізувавши вказані вище стратегії, можна виділити найбільш поширені шляхи підвищення рівня безпеки кібернетичного простору, які визнають всі держави:

- формування законодавчої бази регулювання відносин у всесвітньому кібернетичному просторі (обумовлене відсутністю чітких меж кіберпростору окремої держави);

- міждержавний обмін інформацією про кібератаки та можливі шляхи протидії ( в Європі здійснюється у рамках реалізації Європейської конвенції про кіберзлочинність);

- спільні дії з виявлення та припинення діяльності шкідливих програм, осіб, злочинних та терористичних угруповань, які спрямовані на нанесення шкоди світовому кіберпростору;

- усестороннє забезпечення державами органів та відомств, до функціональних обов'язків яких входить забезпечення безпеки у відповідній сфері (наприклад, тільки по відкритих програмах МО США витрачає щорічно близько 3 млрд. доларів на забезпечення кібербезпеки);

- створення нових державних і приватних автоматизованих систем управління, мереж обміну й обробки інформації, методик навчання службового персоналу;

- тісна співпраця із приватним сектором (у більшості країн йому належить близько 85-90% усіх критичних інфраструктур) щодо забезпечення безпеки інформаційних та управлінських систем;

- використання кращих комерційних виробів у сфері забезпечення комп'ютерної, мережевої та інформаційної безпеки;

- контроль за імпортованим апаратно-програмним та програмно-технічним обладнанням, яке буде експлуатуватися, їх перевірка на наявність апаратно-програмних закладок;

- забезпечення високого рівня індивідуального захисту (кібергігієни) шляхом підтримання в робочому стані та своєчасного оновлення спеціального захисного програмного забезпечення;

- створення умов для залучення професійного і талановитого кадрового складу;

- визначення безпеки як основного критерію здійснення діяльності у кіберпросторі.

Беручи до уваги викладене вище, слід зауважити, що хоча український кіберпростір давно є складовою світового, держава ще недостатньо долучилася до міжнародної співпраці у галузі досягнення його безпеки. Контролюючи проведення організаційних та технічних заходів забезпечення кібербезпеки, пріоритетним завданням держави все ж має стати створення законодавчої бази як основи здійснення такої діяльності. Неодноразово наголошувалося на необ-

хідності створення власної Стратегії кібербезпеки, основою якої повинна стати Доктрина інформаційної безпеки України, та закону "Про кібернетичну безпеку". Така нормотворча діяльність стане першим кроком для досягнення належного рівня кібербезпеки Україною у світі інформаційних і комунікаційних технологій.

*Олексієнко А.В.,*
*Національна академія СБ України*

## ЗАГРОЗИ БЕЗПЕЦІ ОСОБИ В УМОВАХ СОЦІАЛІЗАЦІЇ ІНТЕРНЕТ-СЕРВІСІВ

Популярність соціальних мереж серед українських користувачів за останні роки значно збільшилась. Більше того, існує тенденція до подальшого росту цієї популярності. За даними статистики, найбільш популярними соціальними мережами в Україні є "Вконтакте" та "Одноклассники" [1]. Також необхідно відмітити зростаючу популярність соціальних мереж "Dassmates" та "Facebook".

Зростання інтересу до таких інтернет-сервісів створює нові можливості для спілкування, дружби, бізнесу у всьому світі, але ці обставини не залишились не поміченими творцями шкідливого програмного забезпечення та різного роду інтернет-злочинцями.

Так, користувачі соціальних мереж проводять багато часу спілкуючись, однак не тільки вдома, але й на роботі. При цьому більшість з них не дотримуються звичайної обережності, відкриваючи прямий доступ у свої системи великій кількості шкідливих програм. Спам – атаки, фальшиві антивіруси, трояни, шпигунські та рекламні модулі, віруси – все це головні загрози, які чекають на кожного користувача соціальної мережі. Навіть популярні в мережах ігри, тести та інші розваги, можуть бути використані для проникнення шкідливого коду на комп'ютер. Але поряд із зазначеними "традиційними" для всього інтернету загрозами, з'явились й інші, пов'язані з безтурботною поведінкою користувача соціальної мережі. Вони можуть виявитися більш шкідливими і мати більш тяжкі наслідки, ніж заражений вірусом комп'ютер.

До таких загроз, зокрема, належать фішингові атаки. Сутність фішингової атаки полягає у нападі на організацію або окремого користувача для отримання важливих даних. Для цього застосовують-

ся різні методи шахрайства з використанням справжніх даних користувача або компанії. Така атака вимагає доброго знання адресата, але вона, як правило, виявляється найбільш успішною. Проведення фішингових атак у соціальній мережі спрощується завдяки довірливості користувачів, які відкривають свої особисті дані співрозмовникам-“друзям”. Шахраї створюють правдоподібні профілі, які зовні мають цілком нормальний для користувача вигляд. Причини популярності такого виду шахрайства зрозумілі: користувачі не думають, як може бути використана та чи інша особиста інформація, опублікована ними в мережі.

Інший вид обману в соціальних мережах – підміна особи. Мета шахраїв – представитися знайомим і отримати особисту інформацію.

Величезна кількість користувачів захоплюються іграми в соціальних мережах, в яких використовується своя віртуальна валюта, що допомагає підвищити ігровий статус. Причому її купують, розплачуючись справжніми грошима, але існують і “безкоштовні” способи збільшення ігрового капіталу, які приносять ще більше прибутку компаніям. Суть в тому, що користувачам пропонують пройти тест на IQ або завантажити пробну версію якоїсь програми, отримавши натомість деяку кількість віртуальних грошей. Ніде не згадується, що користувач у будь–якому випадку витратить реальні гроші. Наприклад, гроші можуть зніматися з мобільного телефону або стягуватися за доставку “безкоштовного” DVD з програмою. Також, розробники ігор отримують доступ до персональних даних користувачів, що дозволяє розсилати персональні спам-повідомлення.

Незважаючи на спроби антивірусних компаній та виробників браузерів протидіяти таким загрозам шляхом розробки антивірусного та антифішингового програмного забезпечення, атак стає все більше і вони робляться все більш витонченими.

Отже, завжди необхідно пам’ятати, що користування соціальними мережами не тільки надає переваги для спілкування з друзями, але може завдати істотної шкоди фінансам і сприяти крадіжці особистої інформації.

## ЛІТЕРАТУРА

1. Десятка самих популярних соцсетей [Електронний ресурс]. – Режим доступу : http://avietast.livejournal.com/18046.html.

*Пирогова Ю.І.,*
*Навчально-науковий інститут інформаційної безпеки*
*Національної академії СБ України*

## СУЧАСНІ ПІДХОДИ ДО ОБГРУНТУВАННЯ СКЛАДУ КОМПЛЕКСУ ТЗІ

Комплекси ТЗІ – комплекси захисту інформації з обмеженим доступом від витоку через технічні канали, які створюються на об'єктах інформаційної діяльності. Процес розробки рішень щодо захисту інформації включає вибір і обґрунтування складу та структури комплексу ТЗІ відповідно до вимог нормативних документів та доцільності задіяння певних засобів.

На нашу думку, щоб створити ефективний комплекс ТЗІ необхідно визначити підходи до обґрунтування складу комплексу ТЗІ та додержуватись їх при побудові комплексу та при його експлуатації.

Підходами до обґрунтування складу комплексу ТЗІ є:

1) інженерно-технічний;

2) правовий;

3) економічний.

Розглянемо роль кожної складової з підходів у комплексі ТЗІ.

Система інженерно-технічного захисту інформації включає підсистему фізичного захисту інформації та підсистему захисту інформації від витоку технічними каналами.

Підсистема фізичного захисту інформації створюється для протидії навмисним загрозам впливу зловмисника і стихійним лихам. Засоби цієї підсистеми реалізують методи фізичного захисту за допомогою інженерних конструкцій і технічних засобів охорони. Необхідність та ефективність інженерного захисту й технічної охорони об'єктів підтверджується статистикою, відповідно до якої більше 50 % вторгнень вчиняється на комерційні об'єкти з вільним доступом персоналу і клієнтів і тільки 5 % – на об'єкти з посиленим режимом охорони, із застосуванням спеціально підготовленого персоналу і складних технічних систем охорони.

Основу інженерного захисту та технічної охорони складають засоби, що перешкоджають фізичному проникненню зловмисника в контрольовану зону, технічні засоби, які інформують співробітників служби безпеки про інцидент, а також засоби і люди, що усувають загрози.

Підсистема інженерно-технічного захисту інформації від витоку технічними каналами призначена для зниження до допустимих значень величини ризику (ймовірності) несанкціонованого розповсюдження ін-

формації від її джерела, розташованого всередині контрольованої зони, до зловмисника. Для досягнення цієї мети система повинна мати механізми (сили та засоби) виявлення і нейтралізації загроз підслуховування, спостереження, перехоплення і витоку інформації по речовинному каналу [1, с. 529–561].

Правовий захист – це закони, інші нормативні акти, правила, процедури та заходи, що забезпечують захист інформації на правовій основі (міждержавний захист; захист на рівні держави; на рівні підприємства).

Захист інформації регулюється нормативними актами різного рівня. Це міжнародні договори, які стали частиною законодавства України, закони України, постанови Кабінету Міністрів, розпорядження та укази Президента, а також нормативні документи технічного захисту інформації, внутрівідомчі документи та інструкції.

Економічний підхід до захисту інформації можна сформулювати наступним чином: "Якщо розмір витрат на одержання будь-якої інформації перевищує її вартість або збиток в результаті витоку, то система захисту вигідна". Для ринку ця ідея очевидна - потрібно, щоб вартість системи захисту інформації не перевищувала вартості самої інформації.

Основні економічні принципи:

- технологія захисту інформації повинна вибиратися таким чином, щоб при мінімальних витратах, забезпечувати максимальний захист;
- надійність захисту повинна визначатися з міркувань оптимізації ставлення "функціональність системи без захисту" /"функціональність системи із захистом".

Вартість системи захисту складається з початкових вкладень і вартості експлуатації, що включає витрати на навчання персоналу та на підтримку систем [2].

## ЛІТЕРАТУРА

1. Торокин А.А. Инженерно-техническая защита информации : учеб. пособ. для студентов, обучающихся по специальностям в обл. информ. безопасности / А.А.Торокин. – М. : Гели-ос АРВ, 2005.

2. Волчков А. "Экономический подход к защите информации" [Електронний ресурс] / А.Волчков. – Режим доступу : http://directorinfo.ru.

*Свідзінський О.Ф.,*
*Національна академія СБ України*

# ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОСОБИ: СОЦІАЛІЗАЦІЯ ІНТЕРНЕТ-СЕРВІСІВ

Сучасне суспільство розвивається за рахунок інформації – будь-яких відомостей та даних, збережених на матеріальних носіях або у електронному вигляді. Світовий соціальний прогрес з-поміж інших держав торкнувся і України, активний розвиток науки зробили інформацію більш доступною для українців. Зокрема, за даними аналізу інтернет-аудиторії України, в березні 2012 року доступ до інтернету мало 48% мешканців України віком 15 років і старше. Користуються інтернетом 42% (16,9 млн) раз на місяць і частіше, 39% (15,7 млн) раз на тиждень і частіше та 31% (12,4 млн) щодня, або майже щодня.

При збережені наведеної вище тенденції, з урахуванням того що Україна вже переступила поріг соціалізації інтернету у суспільстві (33%), надалі кожний четвертий українець буде користуватися інтернетом мало не щодня. Проте соціалізація інтернет-сервісів містить і певні небезпеки, зокрема, збільшення кількості правопорушень, предметом яких є інформація, що обробляється за допомогою інтернет-сервісів. Більше того, при отриманні певної інформації з мережі Інтернет та використанні інтернет-сервісів ми не тільки отримуємо “щось”, але і віддаємо, або можемо віддати, “щось ще більш цінніше”. У зазначеному контексті це певна конфіденційна інформація, за допомогою якої можна ідентифікувати особу-користувача, і надалі використати її на шкоду правам та інтересам цієї особи або інших членів суспільства, можливо й держави в цілому.

Головним соціальним процесом, через який здійснюється взаємодія між особистістю та суспільством, є процес соціалізації, що має досить багато різних інтерпретацій, однією із яких є соціалізація особи через інтернет, і в зворотному напрямку соціалізація інтернету здійснюється через осіб-користувачів.

Ми вважаємо, що у цій сфері існують такі проблеми:

1. Переважна частина національних веб-ресурсів ігнорують вимоги нормативно-правових актів у сфері захисту конфіденційної інформації особи.

2. У нормативно-правових актах не визначено чіткого переліку персональних даних особи і можливих джерел їхнього отримання.

3. Наявність у нормативно-правових актах оціночних понять, які встановлюють винятки для дії норми права.

4. Наявність колізій у правовому регулюванні сфери конфіденційних відомостей особи (Закони України “Про інформацію”, “Про захист персональних даних”, Конституція України).

5. У Законі України “Про захист персональних даних” випущено такий важливий статус інформації, як персональні дані, отримані із мережі інтернет.

6. Наші законодавці хоча і посилаються на Директиву ЄС про особливості використання персональних даних у сфері телекомунікацій, але фактично жодне з її положень не використане (у частині, що стосується інтернету та інтернет-сервісів), не враховуються особливості обробки персональних даних у сфері телекомунікацій, зокрема у мережі Інтернет.

7. Адміністративна діяльність спрямована на забезпечення порядку доступу, організації роботи з персональними даними з позицій уповноваженого державного органу у цій сфері та його повноважень, але не на захист прав особи від неправомірного використання цих даних, особливо коли йде мова про інформацію, одержану із інтернет-ресурсів.

Крім зазначених вище проблем варто застерегти, що за умови стрімкої соціалізації інтернет-сервісів особливої важливості набуває боротьба з такими адміністративними правопорушеннями, як ст. 188-39 КУпАП, ст. 188-40 КУпАП та ст. 212-6 КУпАП. Для створення логічно завершеного, ефективного правового регламентування адміністративної відповідальності за вчинення зазначених правопорушень, насамперед, необхідно передбачити у чинному КУпАП розділ, який би містив правопорушення у сфері обігу інформації, а також закріпити у чинному КУпАП норму, яка б передбачала адміністративну відповідальності юридичних осіб за вчинення правопорушень в інформаційній сфері.

За вчинення адміністративного правопорушення у сфері інформаційної безпеки на фізичних осіб найчастіше накладається штраф. На нашу думку, цей вид адміністративного стягнення також варто застосовувати і до юридичних осіб – порушників законодавства про інформацію.

## ЛІТЕРАТУРА

1. Закон України “Про інформацію” від 2 жовтня 1992 року № 2657-XII //Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650.

2. В Україні 12,2 мільйони активних інтернет-користувачів Інтернет // [Електронний ресурс] : Сайт “Українська правда”. – Режим доступу : http://www.pravda.com.ua/news/2012/07/18/6969059/.

3. Мережа Internet. Види сервісів Internet // [Електронний ресурс] : Інтернет сайт “Знання”. – Режим доступу : http://www.znannya.org/?view=web_tech_basic%20_article.

4. Перший моніторинг відкритості та прозорості обробки персональних даних в Інтернеті // [Електронний ресурс] : Сайт Української асоціація захисту персональних даних. – Режим доступу : http://uapdp.org/index.php/podiji/khronika-podij/144-pershiy-monitoring.

5. Європейська конвенції з прав людини (ETS No. 5), ратифікована Законом України N 475/97-ВР від 17.07.97.

6. Обговорення в Асамблеї 7 жовтня 2011 (36-е засідання). Доповідь Комісії з культури, науки та освіти, доповідач: пан Саллес Рихтер. Захист конфіденційності і персональних даних в Інтернет і онлайн засобах масової інформації // [Електронний ресурс]: Інформаційний портал Харківської правозахисної групи. – Режим доступу: http://khpg.org.index.php?id=1329990005.

7. Конституція України: Прийнята на п’ятій сесії Верховної Ради України 28 червня 1996 року // Відомості Верховної Ради України. – 1996. – № 30. – Ст. 141.

8. Благодарний А.М. Особливості адміністративної відповідальності за правопорушення в інформаційній сфері / А.М.Благодарний. – К. : Підприємництво, господарство і право. – № 11(167). – 2009. – Ст. 123.

9. Кодекс України про адміністративні правопорушення // Відомості Верховної Ради Української РСР України. – 1984. – додаток до № 51. – Ст. 1122.

10. Юрченко И.А. Понятие и виды информационных преступлений / И.А.Юрченко // Российское право в Интернете. – № 2003 (01). Інтернет ресурс. Режим доступу : http: rli.consultant.ru/magazine/2003/01.

11. Адміністративне право України : підруч. / [Ю.П.Битяк, В.М.Паращук, О.В.Дьяченко та ін. ] ; за ред. Ю.П.Битяка. – К. : Юрінком Інтер, 2005. – 544 с. – Ст. 175.

12. Блажівська Н.Т. Діяльність провайдерів. Практичний погляд на питання / Н.Т.Блажівська, Т.В.Береза // [Електронний ресурс] : Сайт “Юрист”. – Режим доступу : http://www.lawyer.org.ua/?w=r&i=5&d=267.

13. Агапов А.Б. Основы государственного управления в сфере информатизации в Российской Федерации / А.Б.Агапов. – М. : Юристъ, 1997. – 343 с.

14. Інтернет в Україні // [Електронний ресурс] : Відкрита інтернет-енциклопедія “Вікіпедія”. – Режим доступу : http://uk.wikipedia.org/wiki/Інтернет_в_Україні#cite_note-12.

# РЕКОМЕНДАЦІЇ

НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ
“Інформаційна безпека: виклики і загрози сучасності”

5 квітня 2013 року в Національній академії Служби безпеки України проведено щорічну науково-практичну конференцію *“Інформаційна безпека: виклики і загрози сучасності”*.

У роботі конференції брали участь понад 150 учасників, у тому числі науковці та викладачі вищих навчальних закладів України, фахівці Служби безпеки України, інших міністерств та відомств, представники вітчизняного ІТ-бізнесу.

На конференції обговорено комплекс загальнотеоретичних, правових, технічних та організаційних питань, пов’язаних із проблемами визначення та протидії загрозам інформаційній безпеці держави.

За результатами обговорення питань конференція

РЕКОМЕНДУЄ:

1. Враховуючи те, що видозміна існуючих та виникнення нових загроз інформаційній безпеці особи, суспільства та держави потребує постійного удосконалення й уточнення понятійно-категорійного апарату, підходів і методик визначення (моделювання, виявлення, оцінювання) загроз та розроблення заходів з попередження і мінімізації їх наслідків, проведення науково-практичних досліджень з цих питань за гуманітарними і технічними напрямами вважати пріоритетними.

2. Виходячи з актуальності завдань протидії злочинам у сфері використання комп'ютерної техніки, інформаційних систем та мереж, а також мереж електрозв'язку, – поглиблювати міжвідомчу співпрацю з питань удосконалення методичного й технологічного забезпечення кібернетичної безпеки.

3. Беручи до уваги міжгалузевий характер проблематики визначення загроз інформаційній безпеці держави, рекомендувати зацікавленим міністерствам і відомствам проводити спільні дослідження з цих напрямів та формувати на основі їх результатів комплексні, узгоджені пропозиції щодо удосконалення законодавства в інформаційній сфері.

4. Активно розвивати систему правового захисту інтелектуальної власності у вищих навчальних закладах та науково-дослідних підрозділах правоохоронних органів й інших силових відомств.

# ЗМІСТ

Науково-практичне видання

# ІНФОРМАЦІЙНА БЕЗПЕКА: ВИКЛИКИ І ЗАГРОЗИ СУЧАСНОСТІ

*ЗБІРНИК МАТЕРІАЛІВ*
*НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ*
*5 квітня 2013 р., м. Київ*

Редактори *Н.М.Мармоленко*, *О.П.Власенко,*
*С.В.Ангелуца, Н.М.Лашкет*
Комп'ютерне макетування *Т.О.Коркач*
Технічне редагування *О.С.Вишневська*

Підписано до друку 30.08.2013. Формат 60х84/16.
Папір офсетний № 1. Гарнітура Times New Roman.
Друк офсетний. Ум. друк. арк. 24,36
Обл.-вид. арк. 22,59. Тираж пр. Зам. №

Реєстр. № 29/20-6139 від 26.07.2013 р.

Копіювально-розмножувальний сектор
науково-видавничого відділу
центру навчально-наукових та науково-практичних видань
Національної академії Служби безпеки України,
03022, Київ, вул. Трутенка, 22.