МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ІНСТИТУТ МОДЕРНІЗАЦІЇ ЗМІСТУ ОСВІТИ

НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

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

АКТУАЛЬНІ ПРОБЛЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ

VII Науково-практична конференція

Збірник матеріалів
(Київ, 18 березня 2016 року)

У двох частинах

Частина 2

Електронна версія на CD-ROM

Київ
2016

Електронна версія друкованого видання

Актуальні проблеми управління інформаційною безпекою держави : зб. матер. наук.-практ. конф. (Київ, 18 березня 2016 року) : у 2 ч. Ч. 2. – Київ : Нац. акад. СБУ, 2016. – 164 с.

УДК 341.123(045)(0.034.2PDF)

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

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

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

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

АКТУАЛЬНІ ПИТАННЯ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ В КОНТЕКСТІ ЗАПРОВАДЖЕННЯ В УКРАЇНІ СИСТЕМ ЕЛЕКТРОННОГО УРЯДУВАННЯ

УДК 004

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

ІНФОРМАЦІЙНО-ОБЧИСЛЮВАЛЬНІ ТЕХНОЛОГІЇ В МОДЕЛЮВАННІ СОЦІОТЕХНІЧНИХ ВІДНОСИН

Моделювання соціотехнічних відносин має надзвичайно важливе значення – і перш за все – для прогнозування поведінки колективів, соціальних груп, регіонів і цілих країн, в тому числі – кількісні оцінки реакції на ті чи інші управлінські рішення керівників і влади. В кінцевому результаті використання результатів такого моделювання повинно призвести до гармонізації суспільних відносин в системах «колектив – керівник», «студенти – адміністрація університету», «народ – влада» – в першу чергу за рахунок оптимізації управлінських рішень та поглиблення знань про об'єкти управління.

Важливим джерелом достовірної інформації для такого моделювання є багаторівневе тестування та анкетування. Нехай тест (анкета) складається з N_1 задач (запитань) X_i, $i \in \{1,2,\ldots,N_1\}$ кожна з яких має по N_2 відповідей K_j, $j \in \{1,2,\ldots,N_2\}$, а кількість учасників тестування (анкетування) N_3. За результатами такого тестування (опитування) кількість отриманих параметрів буде становити:

$$P = N_{1*} N_{2*} N_3$$

Для N_1 – 100, N_2 – 10, N_3 – 1000 то маємо масив з 10^6 параметрів. Якщо ж N_3 ~10 000 або 1000 000 – наприклад, всі жителі району чи якогось містечка, то Р~100 000 000, що є практично недосяжним для обробки за «ручними» технологіями.

Сьогодні для статистичної обробки результатів опитувань використовуються сучасні досягнення інформаційно-обчислювальних технологій. Запропонований авторами комплекс обробки тестування (анкетування) забезпечує такі функції:

- автоматизоване формування тестів (анкет), що гарантує швидке народження якої завгодно кількості рівноцінних та неповторних варіантів;
- автоматизована обробка анкет (сканування, розпізнавання, дешифровка). У випадку тестування це включає співстановлення відповідей учасників тестування з ключем правильних відповідей;
- формування та зберігання бази даних по всьому масиву протестованих або опитаних;
- виявлення кореляційних зв’язків між параметрами;
- порівняння великих масивів в багатовимірних просторах;
- формування кількісних оцінок ефективності управлінських рішень тощо.

Запропонована методика апробована в Державному університеті інформаційно-комунікаційних технологій та Національному авіаційному університеті. При тестуванні студентів в період подачі документів до вступу у магістратуру була застосована інформаційно-обчислювальна технологія, яка є основою запропонованої та розробленої методи, та побудована модель самоідентифікації студентського колективу. Звичайно зросла оперативність обробки матеріалів тестування та анкетування (до 50 разів), зменшилась кількість помилок. Автоматизована система тестування та анкетування показала суттєві переваги перед традиційним (ручним) способом організації таких робіт.

УДК 355.40

Богомолов О. О.
Воєнно-дипломатична академія ім. Є. Березняка
Бойко О. В.
кандидат технічних наук, доцент
Воєнно-дипломатична академія ім. Є. Березняка

МЕТОДИКА ВИБОРУ АЛГОРИТМУ ГЕШУВАННЯ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Вибір та реалізація механізмів забезпечення цілісності та справжності інформаційних ресурсів у сучасних інформаційно-телекомунікаційних системах (ІТС) є одними з важливих етапів проектування та розробки підсистем захисту інформації. Особливе місце серед механізмів забезпечення цілісності і автентичності інформації при побудові комплексу засобів захисту із широким спектром послуг безпеки інформації займає вибір функції гешування, зокрема за стандартом ISO 7498 [1-4]. Односторонні геш-функції визначені в окремому міжнародному стандарті ISO/IEC 10118 [1, 2].

Для захисту від ймовірних загроз безпеки інформації в автоматизованих системах, як правило, використовують механізми гешування даних – ключові та без ключові геш-функції. Геш-функції також можуть використовуватись у складі електронного цифрового підпису, який є потужним механізмом забезпечення автентифікації в сучасних автоматизованих системах.

В умовах стрімкого розвитку ринку інформаційних послуг та технологій їх реалізації, питання вдосконалення програмних продуктів, що реалізують захист прав власників інформаційного ресурсу, мають достатньо динамічний характер та різноманітність підходів до їх вирішення.

Таким чином, актуальною задачею є аналіз можливості використання геш-функцій в алгоритмах криптографічних перетворень для реалізації автентичності та цілісності інформації (електронних повідомлень), в тому числі з обмеженим доступом, під час доступу до неї в ІТС закритого типу та розроблення відповідної методики.

Для обрання найбільш оптимальних варіантів криптографічних перетворень інформації в ІТС закритого типу пропонується провести всебічного дослідження алгоритмів гешування інформації, які сьогодні практично застосовуються в різних ІТС.

Геш-функція – це функція, яка відображає вхід довільної довжини в фіксоване число вихідних біт – геш-значення. Для того щоб бути корисною в криптографічних додатках, геш-функція повинна задовольняти деяким вимогам. Геш-функції можуть поділятися на односторонні геш-функції та стійкі до колізій геш-функції.

Для того, щоб геш-функція вважалася криптографічно стійкою, вона повинна задовольняти наступним вимогам: незворотність або стійкість до відновлення прообразу; стійкість до колізій першого роду або відновлення другий прообразів; стійкість до колізій другого роду.

При використанні односторонніх геш-функцій для вирішення завдань щодо вироблення ключів і псевдовипадкових чисел, вони повинні задовольняти таким вимогам: відсутність кореляції; стійкість до близьких колізій; стійкість до часткової односторонності; можливість роботи в режимі розтягування. Додатково для геш-функцій з секретним ключем висуваються вимоги: обчислювальної стійкості та стійкості ключа.

В процесі дослідження розроблена класифікація сучасних геш-функцій. В результаті аналізу основних класі геш-функцій визначено наступне:

- суттєвим недоліком безключових геш-функцій є те, що вони незахищені від можливості по підбору такого ж самого повідомлення з однаковим гешем, та мають відсутність властивості обчислювальної стійкості;
- вивчаючи результати всебічного дослідження алгоритмів гешування інформації можна стверджувати, що при використанні MAC-коду обчислити геш-код за даним вхідним повідомленням може тільки суб’єкт, що володіє секретним ключем;
- основними характеристиками алгоритмів формування MAC кодів, за якими виконується їх порівняльна оцінка відповідно до рекомендацій проекту NESSIE є: рівень захищеності MAC кодів від загальних атак; швидкодія алгоритмів формування MAC кодів; статистичні властивості розподілів MAC кодів;

- аналіз тестування швидкості роботи алгоритмів гешування показав, що найбільш перспективним алгоритмом обробки інформації є UMAC. При додатковому використанні алгоритму AES вірогідність зламу значно зменшується;

- при розгляді стандартів ISO 7498-2 і ISO/IEC 10181 визначено, що одним з найнадійніших способів вирішення завдань, пов'язаних з автентифікацією даних і джерел повідомлень, є процедури формування цифрового підпису, побудовані на основі асиметричних криптографічних алгоритмів;

- найбільш стійкою геш-функцією до різних типів атак є функція вироблення MAC-коду, яка використовується для автентифікації повідомлення.

На основі проведеного аналізу розроблена методика вибору алгоритму гешування для захисту ІТС, яка включає наступні елементи: визначення вхідних параметрів (визначення мети створення ІТС, її функцій та архітектури, розроблення моделі загроз, визначення обмежень на створення системи захисту); блок вибору геш-функції з наявних на ринку пропозицій у відповідності до функціонально-вартісного підходу; розробка практичних рекомендацій щодо вибору та експлуатації геш функцій.

Таким чином, в результаті дослідження визначено наступне:

- аналіз умов застосування функцій гешування та їх практичного використання в сучасних ІТС дозволив сформулювати вимоги, які пред'являються до застосовуваних у криптографії безключовим геш-функціям, вони полягають у стійкості до обчислення, стійкості до обчислення другого та стійкості до колізій.

- використання MAC-кодів дозволяє інтегровано вирішувати завдання гешування і забезпечення стійкості отриманих геш-кодів;

- алгоритм UMAC, заснований на універсальному сімействі геш-функцій й доказовою безпекою, є достатньо надійним та перспективним, що може дозволити його практичне використання при побудові систем захисту в перспективних ІТС з метою забезпечення автентичності та цілісності інформації;

- розроблена методика вибору алгоритму гешування для захисту ІТС на основі функціонально вартісного підходу дозволяє обрати оптимальний склад засобів захисту інформації в умовах фінансових обмежень на створення підсистеми захисту інформації.

Література

1. Кузнецов О.О. Захист інформації в інформаційних системах / О.О. Кузнецов, С.П. Євсеєв, О.Г. Король. – Х. : Вид. ХНЕУ, 2011. – 512 с.

2. Положення про проведення відкритого конкурсу криптографічних алгоритмів [Електронний ресурс] // Інститут кібернетики ім. В. М. Глушкова НАНУ. ДСТСЗІ [Електронний ресурс]. – Режим доступу : http://www.dstszi.gov.ua /dstszi/ control /ru/publish/article.

3. Поповский В. В. Защита информации в телекоммуникационных системах : учебник / В. В. Поповский, А. В. Персиков. – Х. : ООО "Компания СМИТ", 2006. – Т. 1. – 292 с.

4. Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії : навч. посібн. / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2010. – 316 с.

УДК 351.746

Величко М. В.
кандидат біологічних наук, старший науковий співробітник
Національна академія СБ України

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ – КАТАЛІЗАТОР РОЗВИТКУ БІОТЕХНОЛОГІЙ У СФЕРІ ОХОРОНИ ЗДОРОВ'Я ЛЮДИНИ

Людська спільнота не може самоізолюватися від інформаційного впливу всесвіту. Доступ до інформації екологічного чи соціального середовища є однією із умов життя людини і інших живих істот без доступу до якої вони гинуть. Перебуваючи в природному чи соціальному середовищі людина постійно генерує власну інформацію у середовище та «споживає» зовнішню як і продукти харчування. Інформація, що надходить до людини є основною потребою її життєздатності і життєдіяльності де наряду із позитивною надходить і негативна яка є шкідливою і розрушає її як психічний, духовний світ так і гармонію функціонування фізіологічних, біохімічних процесів в тілесному середовищі [1]. Тому важливо мінімізувати негативний інформаційний вплив в цілому на психічне та фізіологічне здоров'я людини. Цей напрямок є інформаційною екологією людини. На перетині інформатики і біології у XXI сторіччі виникла біоіформатика як один із провідних біотехнологій каталізатором яких послужили інформаційні

технології. Якщо інформаційні технології на часі досягли свого апогею то біотехнології тільки стрімко розвиваються і є неодмінною умовою для подальшого виживання людства. Міжнародною науковою спільнотою одностайно визначено, що людство в XXI столітті отримало завдяки сучасним біотехнологіям надзвичайні можливості щодо вирішення гострих соціальних проблем, пов'язаних з забезпеченням харчування стрімко кількісно зростаючого населення планети, підтримкою здоров'я людини та мінімізації антропогенного впливу на навколишнє середовище, поповненням джерел енергії та природних ресурсів [2]. Зокрема, стрімкий розвиток біомедицини, включаючи генну та регенераційну медицину, зумовлений перш за все двома видатними подіями в науці на межі XX та XXI століть: розшифровкою геному людини та отриманням культур ембріональних стовбурових клітин людини.

Перші доклінічні та клінічні випробування, що проводилися в США та Європі, показали надзвичайну перспективність застосування генних та клітинних технологій при таких патологіях як ішемічна хвороба серця, критична ішемія кінцівок, ішемічні та після інсультні стани головного мозку, травматичні стани, хондро- та остеопатії, нейродегенеративні хвороби, ендокринні порушення, зокрема цукровий діабет, дисфункції щитовидної залози та інше. Одним з можливих використань стовбурових клітин може стати їх застосування в реверсивній медицині, тобто, усунення за їх допомогою вад організму внаслідок його старіння або хвороби [3].

На жаль, в Україні не існує жодного центру (власної «силіконової» долини), який би мав сучасне обладнання для виконання робіт в цих напрямках з метою створення основ новітніх біотехнологій і розвитку нових напрямів медицини, включаючи діагностику і лікування. До того ж не можна уявити якісну підготовку висококваліфікованих спеціалістів з сучасних напрямків біології, медицини, ветеринарії, біотехнології без залучення до освітянського процесу досвідчених вчених, які працюють в галузі геноміки, протеоміки, генної та клітинної інженерії, аналітичних біотехнологій, біоінформатики. В той же час розвиток наукових досліджень, впровадження їх в практику, підготовка спеціалістів в цих галузях, підтримка проектів, спрямованих на поліпшення здоров’я та добробуту нації є проблемою державного рівня.

Внаслідок збігу різних обставин Україна опинилась в стані «передзникнення». Це обумовлено відсутністю в країні найваж-

ливіших для існування її населення можливостей. Україна на відміну від забезпечення власними силами потреб ветеринарної медицини, не виготовляє для вакцинації людей жодної вакцини. Вона купує готові великі фасування і розфасовує їх до готових доз. Іноді до них додають допоміжні компоненти. Така ж ситуація має місце і з антибіотиками. В результаті наявна цілковита залежність від тих країн, які поставляють в Україну вакцини та антибіотики (у повністю готовому вигляді або як „напівфабрикат"). Відсутня лабораторна база для самостійного створення вакцин та антибіотиків. Перша ж пандемія з високою летальністю, яка вичерпає на себе з країн-виробників ці найперші й найважливіші засоби профілактики і лікування, призведе до масової загибелі населення країн, що не мають власної бази створення таких засобів. І Україна буде однією з них. Така ж ситуація спіткає нашу країну у разі спалаху на її території нових (коронавірус «Мерс, вірус Зіка» та емерджентних (Ебола, Марбур, Ласо та ін.) епідемій, біоепідемічних диверсій та терористичних актів тощо. А швидкий і невпинний темп зменшення населення України за рахунок майже вдвічі більшого перевищення смертності над народжуваністю гранично загострює всю ситуацію, яка все більше наближається до загальнонаціональної катастрофи, за якої від країни залишиться тільки її назва (да й то — тільки як історичне посилання). І для того щоб протиставити цьому надійний захист, сьогодні в Україні нічого не існує.

В Україні не існує сучасних клітинних технологій (ганебним сурогатом, яких є бізнес на фетальному матеріалі), взагалі не існує тканинної інженерії, є на всю країну маленький осередок з генних технологій (в ІМБіГ, ІКБГІ НАН України), де існує білкова інженерія тощо. В той же час в світі розвинених країн саме ці технології і наукові напрямки, які їх забезпечують потужним використанням досягнень інформаційних технологій (біоінформатика, протеоміка ,функціональна геноміка тощо) розвиваються стрімко, випереджуючи по відношенню до всього іншого і абсолютно пріоритет. Це пояснюється тим, що всі ці наукові напрямки і технології направлені на біологічну реконструкцію людини на рівні дорослих індивідуумів (не в поколіннях), що практично розпочалася. Здобутком останніх десяти років з'явились напрямки, як клінічна практика, регенеративна медицина. Створена індивідуальна діагностика майбутніх захворювань на основі визначення мононуклеотидного поліморфізму. Після такого визначен-

ня створюють умови для запобігання до неминучих до останнього часу патологій (рак, інфаркти, інсульти тощо). Динамічно розвиваються напрямки сучасного лікування спадкових та масових патологій за технологією генної терапії тобто регенерації інформаційної програми розвитку людського індивідуму тощо. Світ стрімко поділяється на тих, хто в дуже близькому майбутньому складе, за американською термінологією „золотий мільярд" і тих, хто залишить на Землі для нього місце. І від того як будуть розвиватися вище зазначені біо та інформаційні технології в Україні залежить те, де вона буде.

Висновки:

1. Біоінформатика, що виникла на стиці геноміки і інформатики створила нові практичні можливості у сфері як біологічної так і інформаційної безпеки людини.

2. Розробка та реалізація новітніх біотехнологій є інструментарій науково-обґрунтованої охорони здоров'я з оптимальними економічними затратами, яка стане ефективною складовою біологічної безпеки держави.

3. Нагальна необхідність створення біотехнологічного державного науково-прикладного центру, який би мав сучасне обладнання для виконання робіт з метою створення основ новітніх біотехнологій і розвитку нових напрямів медицини, включаючи діагностику і лікування.

Література

1. Величко М.В. Біоінформатика і людина в світлі інформаційнох безпеки держави./М.В. Величко, О.В. Шамсутдінов, М. В. Наливайко//Матеріали науково-практичної конференції ННІ ІБ НА СБУ «Актуальні проблеми управління інформаційною безпекою держави», 2012, С. 127-130.

2. Інтернет-ресурс – режим доступу: www.isaaa.org .

3. Шамсутдінов О.В. Кримінально-правова охорона біологічної безпеки/О.В. Шамсутдінов, І.М. Салагор// Фахове видання НА СБУ, 2014, №50, с. 208-217.

УДК 681.5.015

Козюра В. Д.
кандидат технічних наук, доцент
Національна академія СБ України
Іванченко І. С.
Національний авіаційний університет
Хорошко В. А.
доктор технічних наук, професор
Національний авіаційний університет

ОСОБЛИВОСТІ ЕКСПЛУАТАЦІЇ ТА МОДЕРНІЗАЦІЇ ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖ

Нові тенденції в сфері інформаційних та інфокомунікаційних технологій – такі, як збільшення потужності обчислювальних засобів, використання ресурсних додатків, необхідність передавання більших обсягів інформації й підтримування різних типів трафіків, суворість вимог до безпеки та інше – значно змінило підхід до побудови корпоративних мереж.

Великі корпорації, промислові підприємства та різні відомства сьогодні намагаються організувати високошвидкісну й безпечну роботу користувачів у локальних корпоративних мережах; інтегрувати передачу даних, голосову інформацію та відео зображення усередині офісу та між віддаленими філіями; забезпечити віддалений доступ різних категорій користувачів до корпоративної мережі та Інтернет; об’єднати усі компоненти мережі в загальну інфраструктуру й створити єдиний інформаційний простір так званої мультисервісної мережі.

У ході повсякденної експлуатації сучасних мультисервісних корпоративних мереж, від надійної й ефективної роботи яких найчастіше залежить успіх бізнесу, не можуть не виникнути та постійно й виникають різні проблеми оптимізації та оперативного перерозподілу наявних мережевих ресурсів. Зокрема, адміністратори мереж часто зіштовхуються з необхідністю вирішувати наступні завдання:

1. Одержати максимальну корисну віддачу від існуючої мережі й наявної смуги пропускання та забезпечити необхідний рівень безпеки й надійності для роботи конвергованих і критично важливих додатків.

2. Запобігти несанкціонованому доступу в мережу, а також доступу окремих категорій користувачів, якщо це веде до перевантаження або знижує ефективність роботи мережі в умовах недостачі ресурсів.

3. Забезпечити необхідний рівень якості мережі для роботи найбільш важливих додатків.

4. Інтегрувати в існуючу мережу постійно зростаюче число мобільних користувачів.

5. Знизити експлуатаційні та інші витрати за рахунок оптимізації роботи мережі в години найбільшого навантаження.

Для рішення перерахованих і аналогічних завдань адміністратори мережі потребують потужних засобів створення чітко визначених правил високого рівня, на основі яких буде функціонувати та керуватися корпоративна мережа. Таким чином, проведено аналіз незадовільності об'єкта, розглянуті варіанти модернізації відповідно до існуючих тенденцій розвитку корпоративних мереж, намічені основні етапи модернізації інфокомунікаційної структури.

УДК 004.057.4

Лагун А. Е.
кандидат технічних наук, доцент
Львівський державний університет безпеки життєдіяльності
Топілко В. В.
Львівський державний університет безпеки життєдіяльності

АНАЛІЗ ПРОТОКОЛІВ ЦИФРОВОГО ПІДПИСУ, ЩО ВИКОРИСТОВУЮТЬ СИМЕТРИЧНУ КРИПТОГРАФІЮ

З кожним роком в Україні все більше використовується електронний документообіг. Із запровадженням систем електронного урядування постає проблема безпеки обміну інформаційними повідомленнями, а саме забезпечення конфіденційності, достовірності і цілісності інформації, а також захисту інформації від несанкціонованого доступу і її використання.

Основу забезпечення інформаційної безпеки в інформаційно-комунікаційних системах складають криптографічні методи і засоби захисту інформації. Важливе значення в цих застосуваннях відіграють криптографічні протоколи, які описують обмін повідомленнями між двома або декількома учасниками з використанням криптографічних алгоритмів. Основною проблемою реалізації протоколів є відсутність можливості контролювати їхнє застосування. Це пов'язано з тим, що учасники протоколів можуть мати різні інтереси і тому можуть відхилятися від правил для одержання для себе більшої вигоди. Тому у всіх криптографічних протоколах передбачається наявність зловмисника.

В даній роботі проводиться дослідження криптографічних протоколів для реалізації цифрового підпису.

Цифровий підпис можна означити як рядок бітів, який приєднаний до документа. Наприклад, це може бути значення хеш-функції документа, зашифроване криптографічним ключем.

Наведемо основні характеристики цифрового підпису [1]:

– непідробність цифрового підпису гарантує те, що лише підписуючий свідомо підписав документ;

– достовірність підпису доводить, що підписуючий свідомо підписав документ;

– не можливість повторного використання визначається відсутністю можливості перенесення цифрового підпису на інший документ;

– не можливість зміни підписаного документа;

– не можливість відречення від цифрового підпису.

Протоколи цифрового підпису можна реалізувати за допомогою криптографії з відкритим ключем і симетричної криптографії. Далі будуть розглядатися протоколи цифрового підпису з використанням симетричної криптографії.

Перш за все необхідно визначитися з учасниками протоколів. Вважаємо, що в протоколах беруть участь Client1, Client2, Client3 і заслуговуючий довіри посередник Server.

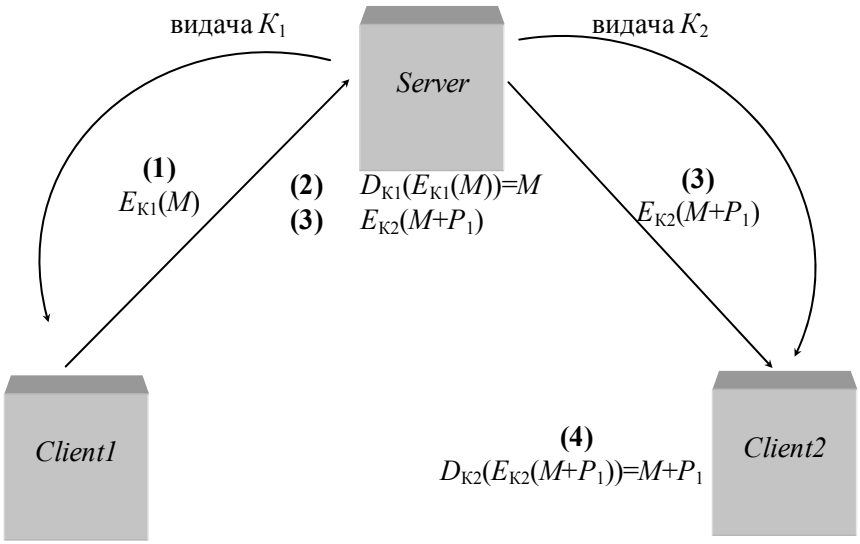

Рис. 1. Протокол підпису документа за допомогою симетричної криптосистеми і посередника

Нехай Client1 хоче підписати цифрове повідомлення і відправити його до Client2. Для забезпечення необхідних характеристик цифрового підпису можна використати заслуговуючого довіри посередника і симетричну криптосистему. Схематично роботу криптографічного протоколу зображено на рис. 1. На рисунку позначено: E – операція шифрування, D – операція розшифрування, M – повідомлення, P_1 – ім'я Client1, K_1 – секретний ключ Client1, K_2 – секретний ключо Client2.

Перед початком протоколу Server надсилає секретний ключ K_1 до Client1, а інший секретний ключ K_2 – до Client2. Протокол цифрового підпису має такий вигляд.

(1) Client1 шифрує своє повідомлення для Client2 ключем K_1 і відправляє його до Server.

(2) Server за допомогою ключа K_1 розшифровує повідомлення.

(3) Server добавляє до розшифрованого повідомлення твердження, що він отримав це повідомлення від Client1; шифрує створене повідомлення ключем K_2; відправляє нове повідомлення до Client2.

(4) Client2 розшифровує повідомлення ключем K_2; читає повідомлення від Client1 і підтвердження від Server, що повідомлення відправлене саме від Client1.

Проведемо аналіз протоколу.

Цифровий підпис не може бути підроблений, через те що лише Client1 і Server знають ключ K_1, а при спробі підміни

Client1 заслуговуючий довіри Server на другому кроці виявить підробку. Також цифровий підпис є достовірний, оскільки Server знає, що повідомлення надійшло від Client1. Від цифрового підпису неможливо відмовитися, тому що при спробі відмови Client1 підтвердження Server доведе зворотне. І, насамкінець, цифровий підпис не можна використати повторно, а підписаний документ змінити, через те що при спробі Client2, маючи підтвердження Server, приєднати його до іншого повідомлення, Server вимагатиме у Client2 його повідомлення і зашифроване повідомлення від Client1. Оскільки Client2 не знає ключа $К_1$, то він не зможе створити правильне шифроване повідомлення від Client1 і шахрайство буде виявлено.

Нехай потрібно підписати один документ двома учасниками протоколу Client1 і Client2. Це можна зробити в два етапи: Client1 підписує документ, а потім Client2 підписує вже підписаний документ. Недоліком таких підписів є подвійна величина підписаного документу і неможливість перевірити цифровий підпис Client1, не перевіривши підпис Client2.

За допомогою хеш-функцій реалізувати декілька підписів набагато простіше [2] (рис. 2).

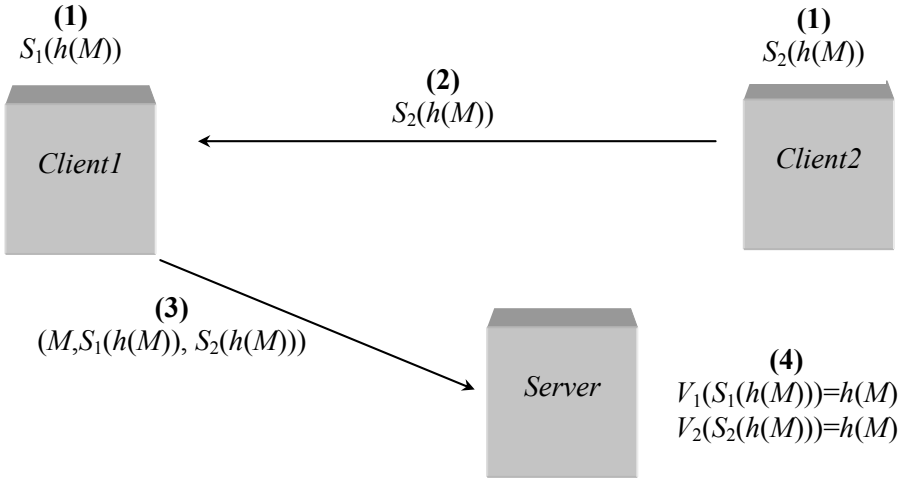

Рис. 2. Протокол реалізації декількох підписів за допомогою хеш-функцій

(1) Client1 і Client2 підписують значення хеш-функції документа S(h(M)).

(2) Client2 відправляє свій підпис до Client1.

(3) Client1 відправляє до Server документ, свій підпис і підпис Client2.

(4) Server перевіряє цифрові підписи Client1 та Client2 – V(S(h(M)))

Client1 може шахраювати з цифровим підписом, підписавши документ, а потім стверджувати, що цього не робив, заявивши що його підпис скомпрометовано і відмовившись від попередніх цифрових підписів. Єдиним захистом від такого шахрайства є зберігання закритих ключів в надійних місцях для унеможливлення доступу Client1 до свого ключа і зловживання ним.

Література

1. Лагун А.Е. Криптографічні системи та протоколи // Навч. посібник. – Львів : Вид-во Львівської політехніки, 2013. – 96 с.

2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке Си / Б. Шнайер. – М.: Триумф, 2002. – 816 с.

УДК 35:303:001

Марутян Р. Р.
кандидат історичних наук, доцент
Національна академія державного управління
при Президентові України

ЗАХИСТ ІНФОРМАЦІЙНО-АНАЛІТИЧНИХ СИСТЕМ ЯК МЕХАНІЗМ ЗАБЕЗПЕЧЕННЯ ПОЛІТИКИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Створення розвинених інформаційно-аналітичних систем підтримки управлінської діяльності є нагальною проблемою сьогодення, актуальність якої зумовлена зростаючою тенденцією до загострення методів ведення інформаційної боротьби у сфері державного та військового управління.

Розв'язання проблеми інформаційно-аналітичного забезпечення (ІАЗ) органів сектору безпеки значною мірою залежить від його важливих складових, якими є: технічна база; якісні та кількісні характеристики інформаційних ресурсів (ІР), які залучаються в процесі інформаційно-аналітичної діяльності (ІАД); стан інформаційних технологій уречевлення ІР для потреб управлінської

діяльності; стан методичного забезпечення аналітичного опрацювання джерел; професійний рівень та інтелектуальний потенціал фахівців з аналізу інформації.

Складність умов роботи аналітичних підрозділів визначається загальним станом виконання програми інформатизації в Україні. Інформаційний простір нашої держави формується в складних умовах сучасних політичних, економічних і соціальних перетворень, які створюють певні об'єктивні та суб'єктивні проблеми[1].

Один із важливих показників стану захищеності ІАД - використання розвинених інформаційних технологій, насамперед з аналітико-синтетичної обробки інформації, оскільки такі технології визначають рівень уречевлення знань у суспільстві. Теоретично є дві альтернативи розвитку інформаційних технологій: запозичення закордонних і використання власних.

Одним з недоліків запозичених технологій полягає в новій якості інформаційних ресурсів, набутій у сучасних умовах. Сьогодні інформаційні ресурси є важливим не лише стратегічним, але й тактичним об'єктом (особливо це стосується державних структур), який потрібно враховувати, приймаючи рішення у всіх сферах державного управління.

Другий негативний наслідок запозичених систем полягає в тому, що, розв'язуючи свої прикладні задачі в чужому технологічному середовищі, ми потрапляємо під «інформаційний ковпак» певної держави. Адже за таких умов легко прогнозується (якщо відомі засоби й алгоритми обробки інформації) результат опрацювання поточних інформаційних матеріалів, отже, й відповідні рішення, які можуть бути прийняті. А це спричиняє втрату інформаційного суверенітету держави та створення умов реалізації інформаційних загроз.

Реальним виходом з такого становища є розроблення власних інформаційних технологій, які містили б останні світові наукові досягнення й реально сприяли б ефективному виконанню завдань інформаційної та інформаційно-аналітичної діяльності.

З аналізу інформаційних впливів бачимо, що методи й заходи ведення інформаційної боротьби мають дуже широкий спектр. Їх активне застосування останнім часом дістало назву інформаційної зброї, від негативних впливів якої має бути розроблена система захисту інформаційно-аналітичних систем.

Таблиця 1

Узагальнена модель інформаційних загроз
інформаційно-аналітичному забезпеченню (системам)

Джерела й канали реалізації загроз	Характер прояву загроз	Заходи щодо захисту від загроз
Інформаційні технології	Занепад власних технологій обробки інформації. Імпортування запозичених інформаційних технологій	Розроблення власної інформаційної технології
Інформаційні ресурси	Перевантаження інформацією	Розроблення методів стиснення інформації
	Дезінформування	Розроблення методів виявлення дезінформації
	Приховування інформації (її неповнота). Тенденційне подання інформації	Оцінювання інформації на повноту
Свідомість людини	Суб'єктивність оцінювання інформації	Автоматизація ІАД

Вимогами, які висуваються до розроблення власної інформаційної технології, є:

випереджувальне володіння ситуацією на основі аналізу всієї доступної інформації порівняно з існуючими технологіями;

орієнтування на обробку знань (змісту інформації), а не текстів (форми інформації);

орієнтування на комплексну автоматизацію всіх етапів аналітичного опрацювання інформації.

Підсистема захисту ІАЗ органів сектору безпеки має містити розвинені методи:

1) стиснення інформаційних потоків на основі їх узагальнення з урахуванням вимог до цілісності інформації;

2) оцінка інформації на повноту;

3) виявлення суперечливої інформації, в тому числі й дезінформації.

Надмірність інформації виникає через повторення тих самих фрагментів знань у різних інформаційних джерелах, а також внаслідок "засмічування" корисної інформації зайвою. В цьому разі застосовуються такі заходи:

семантичне стиснення інформації внаслідок вилучення повторюваних фрагментів знань у різних джерелах;

прагматичне стиснення інформації через відкидання тих фрагментів знань, які не відповідають цільовій настанові розв'язання кінцевої прикладної задачі.

Як і всі етапи управління, процеси їх інформаційно-аналітичного забезпечення є цілеспрямованими й підпорядкованими певній єдиній меті. Це зумовлює потребу створення методологічної бази як взаємопов'язаної сукупності науково обґрунтованих методів організації та автоматизації інформаційно-аналітичного забезпечення всіх етапів прийняття рішень.

На кожному зазначеному етапі можуть існувати свої джерела інформаційних загроз. Основними передумовами їх прояву є некондиційність наявної інформації, неповноцінність її якості та недосконалість засобів обробки. Найнебезпечнішою є наявність дезінформації, якої, заданими фахівців, налічується близько 10 видів. Як дезінформацію розглядають не лише цілеспрямовану хибну інформацію, але й, наприклад, інформацію, що однобічно висвітлює деякі події. Для аналітика у великому обсязі інформаційних потоків виявити дезінформацію вкрай складно.

Висновок. Інформаційно-аналітичне забезпечення органів державного та військового управління значною мірою залежить від таких його важливих складових, як технічна база, якісні та кількісні характеристики інформаційних ресурсів, що залучаються в процесі інформаційно-аналітичної діяльності, стан інформаційних технологій уречевлення інформаційних ресурсів для потреб управлінської діяльності, стан методичного забезпечення аналітичного опрацювання джерел, професійний рівень та інтелектуальний потенціал фахівців з аналізу інформації.

Підсистема захисту інформаційно-аналітичного забезпечення має містити такі розвинені методи як стиснення інформаційних потоків на основі їх узагальнення з урахуванням вимог її цілісності, оцінка інформації щодо її повноти, виявлення суперечливої інформації, в т.ч. і дезінформації.

Література

1. Пампуха І.В. Обґрунтування необхідності розробки власних інформаційних технологій для рішення завдань інформаційної та інформаційно-аналітичної діяльності [Електронний ресурс]. – Режим доступу: http://vuzlib.com/content/view/1102/23/.

УДК 343.983.25

Орлов Ю. Ю.
доктор юридичних наук, старший науковий співробітник
Національна академія внутрішніх справ

ФУНКЦІОНАЛЬНІ МОЖЛИВОСТІ ПРОГРАМИ SYSTEM KEEPER

У серпні 2014 року на новинному порталі http://www.liga.net з'явилася інформація про виявлення управлінням Служби безпеки України в Харківській області «телефонної програми-шпигуна». Програма дозволяла негласно отримувати інформацію з мобільного телефону, зокрема прослуховувати акустичний фон оточення у реальному часі, перехоплювати й зберігати телефонні переговори, мати доступ до фото- й відеофайлів, SMS-листування й електронної пошти, що зберігаються на мобільному телефоні, а також визначати місце знаходження абонента.

Для здійснення контролю мобільного пристрою зловмиснику було необхідно на декілька хвилин отримати фізичний доступ до нього й інсталювати програму. Після цього інформація, знята з мобільного терміналу негласно від його власника, надходила до певного сервера в мережі інтернет, де й накопичувалася для несанкціонованого перегляду. «Програма-шпигун» запускалась автоматично при включенні мобільного терміналу й жодним чином не проявляла ознак своєї активності [1].

Слід визнати, що останнім часом суспільство стикнулося з інноваційними технологіями негласного отримання інформації, які використовують величезні можливості сучасної комунікаційної інфраструктури й здатні підняти проблему незаконного втручання в бізнес та особисте життя громадян на якісно новий рівень. Доведеним фактом є наявність у приватному користуванні спеціального програмного забезпечення, що дозволяє отримувати з терміналів мобільного зв'язку інформацію конфіденційного характеру без відома користувача й здатне до необмеженого безконтрольного поширення.

Метою цієї доповіді є ознайомлення читача з основними функціональними можливостями спеціальної програми System Keeper й ознаками її несанкціонованої інсталяції у мобільних терміналах задля запобігання її протиправному розповсюдженню.

Зауважимо, що програма System Keeper офіційно не поширюється, зокрема, інформація про неї відсутня в пропозиціях спеціалізованого інтернет-магазину Google Play Маркет. За результатами дослідження, проведеного наприкінці 2015 року спеціалістами Національної академії внутрішніх справ, програму System Keeper віднесено до категорії спеціальних технічних засобів негласного отримання інформації [2].

Ця програма створена під платформу Android. Вона не входить до комплекту програм, що офіційно постачаються із цією операційною системою. Разом з тим, в її ярлику присутні елементи бренду Android, що очевидно є засобом камуфлювання й порушує правила використання товарного знаку.

Операційна система Android у стандартній формі відображає інформацію про інстальовану програму System Keeper. Тіло програми System Keeper займає 236 kb пам'яті мобільного телефону, ще деякий обсяг пам'яті займають дані.

Після інсталяції програми операційна система Android декларує (з поясненнями) на панелі програми System Keeper її можливості щодо отримання таких доступів: «переадресація та блокування вхідних викликів; отримання статусу та ідентифікаційної інформації телефону; надсилання SMS-повідомлень (з попередженням, щодо можливості надсилання «шкідливими програмами» без підтвердження користувача); отримання текстових SMS-повідомлень (з попередженням щодо відстеження та видалення вхідних SMS-повідомлень без повідомлення користувачу); читання текстових SMS- та MMS-повідомлень, збережених на мобільному терміналі та SIM-карті незалежно від конфіденційності; записування аудіо (з використанням штатного мікрофону); визначення приблизного місцезнаходження (на основі стільникової мережі та Wi-Fi) та точного місцезнаходження (на основі GPS, стільникової мережі та Wi-Fi); читання журналу викликів (з попередженням щодо можливості надсилання даних журналу без відома користувача «шкідливими програмами»); читання контактів, що зберігаються в мобільному терміналі (з попередженням, що «шкідливі програми» можуть надсилати контактні дані без відома користувача); змінювання чи видалення вмісту на карті SD; повний доступ до мережі (з використанням програмних інтерфейсів та мережевих протоколів та можливістю надсилання даних до мережі); виконання під час запуску (автоматичний запуск

програми при включенні мобільного терміналу); недопущення переходу мобільного терміналу в режим сну; тестування доступу до захищеної SD-пам'яті». Очевидно, зазначена попереджувальна інформація операційної системи Android сформульована недостатньо чітко й не дає користувачу правильного й повного уявлення про процеси, що їх реалізує програма.

Дослідження функціонування програми System Keeper дозволило встановити низку її функціональних можливостей.

Мобільний термінал з інстальованою на ньому програмою System Keeper (надалі – КМТ, контрольований мобільний термінал) в автоматичному режимі підтримує зв'язок з електронною поштовою скринькою в мережі інтернет (надалі – ЕПС). На електрону адресу надходить весь обсяг знятої з терміналу інформації. Адресу ЕПС (логін) встановлюють в ході інсталяції програми.

При здійсненні користувачем вихідного виклику або надходженні вхідного виклику з відповіддю чи без відповіді абонента КМТ відправляє на ЕПС текстове повідомлення про модель та IMEI-код КМТ, напрямок виклику (вхідний/вихідний), номер «мобільника», на який (з якого) здійснено виклик, час і дату виклику, тривалість контакту, а також вкладення («attachments») у вигляді аудіофайлу звукозапису телефонної розмови у форматі .3gp.

В ході прослуховування телефонних переговорів КМТ додатково відправляє на електронну поштову скриньку власні службові стільникові ідентифікатори, зокрема: код мобільного зв'язку країни (Country code), найменування мережі, в якій функціонує КМТ (Network name), ідентифікатор мережі (Network ID); код місцезнаходження (Location Area Code, LAC); глобальний ідентифікатор чарунки (базової станції) (Cell ID). За цими ідентифікаторами підготовлений фахівець може встановити географічне місце розташування абонента КМТ з точністю до стільникової чарунки.

Подібним чином КМТ негласно отримує інформацію щодо відправлених (отриманих) SMS-повідомлень. При надсиланні (надходженні) SMS-повідомлення КМТ негайно відправляє на зазначену ЕПС текстову інформацію про модель та IMEI-код КМТ, напрямок надсилання (вхідне/вихідне), номер «мобільника», на який (з якого) надіслано повідомлення, час і дату надсилання, а також зміст SMS-повідомлення.

При здійснені фотознімків за допомогою вбудованої фотовідеокамери КМТ негайно відправляє на зазначену ЕПС текстову

інформацію про модель та IMEI-код КМТ, повідомлення про тип інформації («camera»), час і дату фотозйомки, а також вкладення у вигляді файлу фотозображення в форматі .jpg.

Для активації режиму прослуховування оточення на КМТ з іншого мобільного пристрою надсилають кодове керуюче SMS-повідомлення, яке містить вказівку щодо тривалості прослуховування (в межах до 180 хвилин). КМТ негайно починає прослуховувати оточення, після завершення якого відправляє на ЕПС текстове повідомлення про модель та IMEI-код КМТ, про тип інформації («environment records»), час і дату, тривалість прослуховування, а також вкладення у вигляді файлу аудіозапису в форматі .3gp.

Зв'язок КМТ з ЕПС, на яку передається знята інформація, підтримується без повідомлення користувачу мобільного терміналу.

Програма System Keeper активується автоматично щоразу після включення КМТ. Користувач не має доступу до панелі інструментів програми й позбавлений можливості її відключити або видалити.

Разом з тим, користувач може тимчасово призупинити роботу програми та її окремих служб, натискаючи відповідні віртуальні клавіші «Зупин.» у вікні «Налаштування»/»Програми»/«Запущена програма System Keeper» на КМТ. Проте, здійснення ним в подальшому будь-якої активної дії на КМТ призводить до автоматичного відновлення роботи програми без повідомлення користувача.

Література

1. СБУ обнаружила телефонную программу-шпион российских спецслужб [Електронний ресурс]. – Режим доступу: http://news.liga.net/news/politics/2995768-sbu_obnaruzhila_telefonnuyu_programmu_shpion_rossiyskikh_spetssluzhb.htm

2. Висновок спеціалістів № 171 за результатами дослідження смартфону від 30 листопада 2015 року. – К.: Нац. акад-я внутр. справ, 2015. – 16 с.

УДК 323.28

Прозоров А. Ю.
Національна академія СБ України

РОЛЬ ІНФОРМАЦІЙНИХ ЦІННОСТЕЙ В ЗАБЕЗПЕЧЕННІ БЕЗПЕКИ ДЕРЖАВИ

Національні цінності є наріжним каменем основ національної безпеки. Їхня деградація та втрата фактично означає втрату національної ідентичності та державності. Національні цінності визначають ціннісні орієнтації суспільства, політичне, культурологічне та філософське світосприйняття, моральні та етичні принципи поведінки кожного члена суспільства. Національні цінності – фундаментальні норми, які дозволяють окремій людині повсякчас здійснювати вибір життєвої позиції, суспільству визначатися із стратегічним баченням свого майбутнього та лінії поведінки в кризових ситуаціях, а державі визначати пріоритети внутрішньої та зовнішньої політики. Вони є найбільш стабільним та найменш динамічним елементом системи забезпечення національної безпеки, визначають сутність, цілісність, стійкість, конфігурацію та направленість формування та функціонування вказаної системи.

Виконуючи регулятивну функцію в інформаційної сфері життєдіяльності суспільства, в тому числі і в сфері інформаційної безпеки, цінності виступають соціально-вагомими орієнтирами організації діяльності соціальних суб'єктів (індивідів, груп, спільнот), професійних колективів, соціальних і державних інститутів та формують систему відносин в інформаційній сфері в цілому, та області забезпечення інформаційної безпеки.

Інформаційні цінності суспільства, є більш усталеними та первісними по відношенню до інтересів, тому що ґрунтуються на інформаційних потребах людини, суспільства і держави, на відміну від інтересів, що залежать від політичної кон'юнктури, мають суб'єктивний та рухливий характер. Тому, саме цінності є методологічним підґрунтям для визначення національних інформаційних інтересів.

Класифікація цінностей на термінальні та інструментальні, яку запропонував Мілтон Рокич та деякі інші дослідники, дає можливість, з одного боку, дослідити найважливіші цільові, або

термінальні цінності інформаційного суспільства, однією з яких, є перш за все інформація, що визначається як суспільним благом, користю, необхідністю, значущість та актуалізація якої сприяє безпечному і сталому розвитку суспільства. З іншого боку, цей підхід допомагає визначити засіб досягнення визначеної мети – інструментальні цінності як систему інституцій інформаційної сфери, що обумовлюють оптимізацію стану національної безпеки України.

Як бачимо, ключове місце в розумінні проблеми інформаційної безпеки займає саме інформація, що набуває статусу провідної цінності сучасного суспільства.

Таким чином, можна виділити декілька груп інструментальних цінностей інформаційної сфери суспільства, що розглядаються як засоби досягнення термінальних, або фундаментальних цінностей. До інструментальних цінностей першої групи доцільно віднести властивості, що визначають позитивну значущість саме інформації – її істинність, достовірність, актуальність, своєчасність, точність, достатність, репрезентативність, обґрунтованість, доступність, стійкість, повноту. [1, с. 188]

Серед ціннісних пріоритетів другої групи, доцільно виокремити захищеність інформаційного ресурсу, інформаційно-телекомунікаційних систем, інфраструктури та інформаційних послуг, інформаційних прав і свобод, інформаційного ринку та в цілому інформаційного простору; інформаційну безпеку людини, суспільства, Української держави та міжнародної спільноти, правову захищеність інформації від маніпулювання, перекручення, обмеження та використання із злочинним напрямом. Окремі групи інструментальних цінностей, складають освітні, професійно-кадрові та інформаційно-технологічні ресурси інформаційної сфери.

Постає питання про місце цінностей інформаційної сфери в загальній системі цінностей суспільства. Воно повинно визначатися, перш за все, провідною роллю інформації в суспільному розвитку, а також, термінальними, фундаментальними цінностями суспільства, по відношенню до яких інформація виступає як інструментальна, допоміжна цінність. Інформація сама по собі є нейтральною, але вона набуває статусу загальнолюдської і цивілізаційної цінності лише за умов наявності й оцінці її етичної складової, що дозволяє отримати відповідь на запитання – в ім'я

чого використовується інформація. В контексті інформаційної безпеки це запитання трансформується у проблему пріоритетності цінностей свободи доступу до інформації і необхідності її обмеження в інтересах людини суспільства і держави.

Негативні, побічні прояви використання інформаційних технологій накладають значні обмеження на їх застосування, вимагають відповідної морально-психологічної підготовки людини, особливих заходів протидії негативному психологічному впливу на свідомість, виховання високих моральних якостей особистості.

Урахування можливих негативних наслідків використання нових інформаційних технологій дозволяє визначити особистісні якості людини в інформаційній сфері діяльності, які поступово набувають характеру професійних і етичних цінностей цієї сфери. Це комунікабельність, мобільність, толерантність, активність, постійний пошук нових знань, готовність їх засвоєння і застосування, варіативність мислення, передбачення наслідків діяльності, етичність використання інформації, комп'ютерна грамотність, самоконтроль, морально-психологічна стійкість. Найважливішою умовою виключення негативних наслідків застосування новітніх інформаційних технологій є моральна складова особистості, її ціннісні орієнтації, що базуються на загальнолюдських гуманістичних цінностях, поряд з ефективною системою соціального контролю. "Здатність до повноцінної комунікації є важливою умовою міцності суспільства, подолання конфліктних ситуацій і напруженості", підкреслює Б. Новіков [2, с. 14].

Таким чином, в умовах сьогодення ефективний захист національної інформаційної сфери держави може бути забезпечений за умов прийняття та проведення відповідних програм з розвитку інформаційних цінностей особи, суспільства та держави.

Поряд з цим, в основу державної політики забезпечення інформаційної безпеки, повинна бути покладена системна, превентивна діяльність органів державної влади, у тому числі СБ України, щодо надання гарантій інформаційної безпеки особі, суспільству, державі.

Література

1. Актуальні проблеми національної безпеки суспільства : монографія / В.О. Ананьїн, В.А, Галєєв, В.В, Горлинський, та ін. за ред. В.О. Ананьїна. Ін-т спец.зв'язку та захисту інформації НУТУ "КПІ". – К. : НВФ "Славутич - Дельфін", 2008. – 246 с.

2. Новіков Б.В. Гуманізм, духовність в сучасному інформаційному суспільстві / Б.В. Новіков // Вісник Національного технічного університету України "КПІ". Філософія. Психологія. Педагогіка. : Зб. Наук. Праць. – К. : ІВЦ "Політехніка", 2001. № 1. – С. 7-14.

УДК 343.32

Фролов Р. А.
Національна академія СБ України

ВРАХУВАННЯ МОЖЛИВОСТЕЙ РОЗВІДКИ З ВІДКРИТИХ ДЖЕРЕЛ ІНФОРМАЦІЇ ПРИ ЗАПРОВАДЖЕННІ СИСТЕМ ЕЛЕКТРОННОГО УРЯДУВАННЯ

Розвиток сучасних технологій, насамперед комп'ютерних, зумовив значне зростання інформаційних потоків у світі. Такі хвилі інформації, що обраховуються в мережі Інтернет такими одиницями як терабайти, петабайти, ексабайти, зеттабайти і т.п. окрім різного роду інформаційного сміття містять в собі безліч даних, поширення яких може нанести значної шкоди інтересам фізичних і юридичних осіб, а в окремих випадках, навіть інтересам держави.

Майже кожного дня в мережі Інтернет можна знайти інформацію (у формі інтерв'ю, телепередачі, наукової статті і т.п.) щодо політичної чи економічної обстановки в тій чи іншій країні світу, сучасних досягнень у підготовці військовослужбовців збройних сил, правоохоронних органів або спецслужб тієї чи іншої країни, надходження нових одиниць озброєння тощо. Така інформація, ґрунтовно проаналізована та уміло реалізована зацікавленою стороною, може завдати шкоди державі в політичній, економічній, оборонній та інших сферах.

Найбільшої ефективності розвідки з відкритих джерел (Open-Source Intelligence, OSINT) для отримання розвідувальної інформації досягли американські фахівці. За їх визначенням, OSINT – це широкий пошук і аналіз інформації, отриманої з загальнодоступних джерел. У розвідувальному співтоваристві термін «відкритий» вказує на загальнодоступність джерела (на відміну від секретних джерел і джерел з обмеженим використанням), він

не пов'язаний з поняттями «відкриті джерела» або «публічна розвідка» [1].

ФБР США взагалі розглядає OSINT як один із основних методів збору інформації. OSINT входить до системи так званих «дисциплін зі збору розвідувальної інформації» (intelligence collection disciplines, INTs) [2].

ФБР розглядає OSINT як збирання великого обсягу інформації з джерел, що загальнодоступні, а саме мас-медіа (газети, радіо, телебачення тощо), професійні та академічні праці (документи, конференції, симпозіуми) та суспільну інформацію (урядові звіти, демографічні дані, слухання, промови тощо). Окремо зазначається, що інформація, яка отримана з відкритих джерел, має бути перевірена та проаналізована для того, щоб бути корисною для політичного істеблішменту [2].

Доповідь спеціаліста Служби досліджень Конгресу (Congressional Research Service, CRS) Річарда А. Беста в Конгресі США у 2007 році розкриває необмежені можливості застосування такого виду розвідки [3].

За його інформацією, «розвідка з відкритих джерел» має справу з інформацією, що не є таємною (хоча в деяких випадках з відкритих джерел вдається отримати й таємні дані – авт.).

На даний час перед Україною, як перед європейською державою, що розвивається в демократичному напрямку, стоїть завдання запровадження систем електронного урядування як моделі управління, у якій всю сукупність внутрішніх і зовнішніх зв’язків та процесів підтримують та забезпечують відповідні інформаційно-комп’ютерні технології .

Така система суттєво збільшить ефективність управлінської та адміністративної діяльності, зменшить державні матеріальні і часові витрати на комунікації, упорядкує дані в єдиних інформаційних системах, підвищить якість надання послуг, полегшить життя пересічним громадянам тощо.

Однак, запровадження цієї системи має враховуючи можливості застосування розвідки з відкритих джерел, а отже передбачати розробку і впровадження дієвої системи захисту даних при електронному документообігу, розмежовувати циркуляцію закритої та відкритої інформації, забезпечити конфіденційність та безпеку баз даних.

Література

1. Розвідка з відкритих джерел [Електронний ресурс] Open-source intelligence. – Режим доступу : http://en.wikipedia.org/wiki/Open-source_intelligence.

2. Дисципліни по збиранню розвідувальних даних [Електронний ресурс] Intelligence Collection Disciplines (INTs). – Режим доступу : www.fbi.gov/about-us/intelligence/disciplines.

3. Розвідка з відкритих джерел (OSINT): Доповідь для Конгресу [Електронний ресурс] Open Source Intelligence (OSINT): Issues for Congress. – Режим доступу : https://opencrs.com/document/RL34270/2008-01-28/.

УДК 681.5.015

Юрх Н. Г.
Національна академія СБ України
Тимченко М. П.
Національний авіаційний університет
Скоробогатько О. А.
Національний авіаційний університет

СИНТЕЗ ПАРАМЕТРІВ СИСТЕМ УПРАВЛІННЯ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ

Однією з основних характеристик сучасного суспільства є інформатизація телекомунікаційних послуг. Їх сукупність постійно ускладнюється, розширяється та удосконалюється. Основою технічного комплексу, що забезпечує доступ до різноманітної інформації, є телекомунікаційна мережа. Для досягнення глобальної доступності, реалізації вимог ринку інформаційних послуг потрібна така архітектура мережі, яка компромісно оптимізувала б діюче устаткування з новими технологіями.

Проблема управління телекомунікаційними мережами є однією з найважливіших у практиці експлуатації мереж Загально визнаною концепцією управління є концепція TMN, яка передбачає наступні рівні управління: елементами мережі, мережею, послугами, бізнесом.

Мережею управління телекомунікаціями TMN може забезпечувати функції управління та зв'язок як між різними операційними системами, так і між операційною системою і різними час-

тинами мереж телекомунікацій. При цьому структура мережі управління телекомунікаціями може змінюватися від дуже простого з'єднання між операційною системою і єдиним елементом обладнання зв'язку до складної мережі, що поєднує багато різноманітних типів операційних систем і обладнання телекомунікацій.

При проектування систем управління (СУ) доцільно зупинитися на виборі кількох показників якості, що враховуються при синтезі. Як зазначалось, кількість показників, які характеризують якість реальної системи, може бути дуже великою. Це означає, що чим більша кількість показників якості враховується при синтезі системи, тим більше досконалою буде синтезована система. В той час, коли більше врахованих показників якості, тим складніше провести синтез без введення деяких обмежень. Тому на практиці існує оптимальна кількість показників якості, яку необхідно враховувати. Введення додаткових показників якості призводить не до покращення, а до погіршення результатів синтезу.

При проектування системи управління необхідно враховувати такі показники:

1. Кількість керуючої інформації (а отже, і необхідну пропускну спроможність каналів), що забезпечує задану точність параметрів об'єктів мережі. При цьому визначається мінімальна кількість керуючої інформації, яка дає змогу СУ мати як властивість адаптивності до плинно прогнозованих збурень, так і інваріантність до заздалегідь не прогнозованих факторів.
2. Затримка керуючої інформації, при якій час передавання команд управління до контрольованих об'єктів не перевищує заданого.
3. Достовірність (вірогідність помилки) при передаванні керуючої інформації.
4. Вартість системи управління.

ПРОБЛЕМНІ ПИТАННЯ ПІДГОТОВКИ ФАХІВЦІВ У ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

УДК: 004.04:00.65+004.056

Бровко В. Д.
кандидат технічних наук
Національна академія СБ України
Воскобойніков С. О.
Національна академія СБ України

АКТУАЛЬНІ ПИТАННЯ ПРОФЕСІЙНОЇ ПІДГОТОВКИ МАЙБУТНІХ ФАХІВЦІВ ГАЛУЗІ «КІБЕРБЕЗПЕКА»

Інформація є одним із основних ресурсів розвитку інформаційного суспільства, інформаційне середовище, морально-етичні норми його формування та правові норми регулювання мають спрямовувати розвиток на благо людства.

Водночас зі стрімким розвитком науки і техніки на шляху до інформаційного суспільства постають морально-етичні проблеми відповідальності людини за науково-технічну діяльність. Ноосферна свідомість людини спрямовує її життєдіяльність, в тому числі й інформаційну діяльність на реалізацію гуманістичної, антропологічної і культурологічної парадигм розвитку суспільства і освіти.

Стрімкий науково-технічний прогрес, розвиток інформаційних і комунікаційних технологій спричинює глибокі системні перетворення в інформаційному та кібернетичному просторах. Кібернетичний простір має відповідну специфіку, що породжує нові загрози й виклики фахівцям з інформаційної безпеки. Фахівці з інформаційної безпеки повинні розв’язувати нові специфічні завдання, які вимагають від них нових знань і вмінь, інноваційних підходів до їх вирішення. З огляду на це, для забезпечення потреб кібербезпеки фахівцями, спроможними виявляти комп’ютерні інциденти й ознаки ризиків кібернетичної безпеки та активно протидіяти сторонньому кібернетичному впливу, пропонується запровадження в системі вищої освіти України профілю навчання

«Кібернетична безпека». За направленістю своєї професійної діяльності такі фахівці входять в систему інформаційної безпеки суб'єкта інформаційної діяльності.

Аналіз зовнішніх ризиків, починаючи з ризиків кліматичних і погодних умов, техногенних ризиків, інформаційних ризиків і внутрішніх ризиків інформаційної безпеки, ризиків кіберпростору визначає рівень захисту інформації суб'єкта інформаційної діяльності. Новітні програмні і технічні засоби на основі впровадження й використання інформаційних технологій для забезпечення технічних ресурсів і комунікацій, інноваційних засобів обробки інформації надають можливість удосконалення системного аналізу ризиків та професійної компетентності майбутніх фахівців інформаційної безпеки.

Формування професійної компетентності майбутніх фахівців інформаційної безпеки – дворівневий неперервний педагогічний процес, який включає послідовну й неперервну фахову підготовку відповідно до Галузевих стандартів вищої освіти освітньо-кваліфікаційного рівня (ОКР) «бакалавр» та освітньо-кваліфікаційного рівня «магістр» у вищих навчальних закладах III – IV рівнів акредитації, спеціалізованих структурних підрозділах – навчально-наукових інститутах.

Формування спеціальних професійних якостей, необхідних для реалізації фахових компетенцій майбутніх фахівців інформаційної безпеки, здійснюється у процесі професійної підготовки – вивчення спеціальних навчальних дисциплін нормативної і варіативної частин навчальних планів відповідно до освітньо-професійної програми та освітньо-кваліфікаційної характеристики Галузевих стандартів вищої освіти нового покоління на основі компетентнісного підходу.

У відповідності із Постановою КМУ №266 від 29 квітня 2015 року «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти» затверджено галузі знань і спеціальності: 12 «Інформаційні технології», 125 «Кібербезпека»; 25 «Воєнні науки, національна безпека, безпека державного кордону», 251 «Державна безпека».

Література

1. Бурячок В.Л. Основи формування державної системи кібернетичної безпеки: Монографія. / В.Л. Бурячок. – К.: НАУ, 2013. – 432 с.

2. Касперський І.П. Класифікація інформації з обмеженим доступом в Україні / І.П Касперський // Науковий вісник херсонського державного Університету. Серія Юридичні науки. – 2013. – №1. – С. 26-29.

3. Постанова КМ України від 29.04.2015 № 266 «Про затвердження переліку спеціальностей, за якими здійснюється підготовка фахівців у вищих навчальних закладах за освітньо-кваліфікаційними рівнями спеціаліста і магістра». [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi.

4. Управление безопасностью информационной инфраструктуры / Евсеев С.П., Хорошко В.А. и др. Раздел 20.// Информационные системы в управлении, образовании, промышленности: Монография. – Харьков : Вид. ТОВ «Щедра садиба плюс», 2014. – 498 с.

5. Шеломенцев В.П. Правове забезпечення кібернетичної безпеки України та основні напрями її удосконалення / Володимир Петрович Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика, 2012. – №1 (27) 2010 – С. 312–320.

УДК 371.124:51: 378.22: 004.032.6

Іванова О. С.
кандидат фізико-математичних наук
Національна академія СБ України

ВИКОРИСТАННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ФОРМУВАННЯ ЛОГІЧНОГО МИСЛЕННЯ ПРИ ВИКЛАДАННІ ФІЗИКО-МАТЕМАТИЧНИХ ДИСЦИПЛІН ДЛЯ СТУДЕНТІВ ТА КУРСАНТІВ

Ми прекрасно знаємо, що освіта нації – запорука її майбутнього. Адже система освіти дає суттєвий вплив на формування духовних, моральних, естетичних та культурних цінностей людини.

В сучасних умовах навчальний процес вимагає постійного вдосконалення, адже сучасний ринок праці вимагає 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, що можуть швидко адаптуватись до нових умов на світовому ринку праці і які можуть вносити нові ідеї та розробки, тобто бути джерелом розвитку тієї галузі науки та виробництва у якій вони задіяні.

Саме фізико-математичні науки є унікальним засобом формування таких якостей сучасного фахівця, як професійна компетентність, творче мислення, навички до самостійної наукової роботи. Адже фізико-математичні методи та математичне моделювання широко використовується для розв'язку практичних задач із різних галузей науки, техніки, економіки, виробництва. Зокрема методи теорії ймовірності широко використовуються у різноманітних галузях природничих та технічних наук: у теорії надійності, теорії масового обслуговування, у теоретичній фізиці, геодезії, астрономії, теорії стрільби, теорії помилок спостереження, теорії автоматичного управління, загальної теорії зв'язку, і т. д.

У зв'язку із цим постають проблеми пошуку та винайдення засобів ефективного розвитку фізико-математичного мислення студентів та курсантів. Адже саме належний рівень розвитку логічного математичного мислення відіграє велику роль у формуванні таких якостей. Першим на що необхідно звернути увагу у навчальному процесі, на мою думку, не тільки на те, що засвоюється (зміст навчання) студентами та курсантами, але й і якості засвоєння матеріалу. Переважно у більшості випадків однією із особливостей викладання фізико-математичних дисциплін є бажання викладачів дати їх матеріал у повному обсязі, при цьому не ставлячи перед собою завдання формування у студентів та курсантів логічного мислення.

На мою думку, при викладанні фізико-математичних дисциплін слід звертати увагу на:

Умови доведення до студентів матеріалу. Важко не погодитись, що успішність у засвоєнні матеріалу залежить від того, чи це здійснюється індивідуально чи колективно, в авторитарних чи гуманістичних умовах, з огляду на сприйняття та пам'ять чи на весь особистісний потенціал людини, за допомогою репродуктивних чи активних методів навчання (особливу увагу приділяючи мультимедійним) [3].

Максимальне використання наочного матеріалу з використанням комп'ютерних технологій. Дійсно, на заняттях працює

принцип: «краще один раз побачити, ніж багато раз почути». Робота з предметами навколишньої дійсності вирішує завдання розвитку наочно – дійового, наочно – образного, а потім і словесно – логічного, абстрактного мислення студентів [2]. Таким чином здійснюється корекція таких процесів мислення, як аналіз, синтез, узагальнення, абстрагування, формуються умови для розвитку пам'яті, уваги, тощо.

Введення нетрадиційних дослідних робіт та робіт з використанням віртуальної лабораторії. До такого типу робіт можна віднести наприклад, момент виконання роботи на природі, де можна приділити увагу екологічному вихованню та здійснити принцип міжпредметних зв'язків із іншими дисциплінами [5].

Можна також, розбити групу на команди по два – три чоловіки, поставивши перед кожною із них якусь конкретну фізико-математичну задачу та запропонувати самостійно знайти її вирішення та порівняти методи вирішення даної проблеми між собою. Таким чином кожен із студентів та курсантів, в рамках своєї команди, може стати і експериментатором, і перевіряючим, і ведучим розрахунки, що формує в свою чергу не лише практичні навички, а й дає можливість встановити логічний зв'язок теорії та практики, виховує відповідальність, працелюбство та колективізм [3].

Віртуальна лабораторія, за допомогою засобів моделювання, дає можливість не тільки демонструвати об'єкти й процеси, що вивчаються, а й досліджувати їх величини, особливо в умовах відсутності діючої лабораторії. Особливе значення фізичні й математичні моделі мають для вивчення динамічних систем і процесів [1].

Правильну організацію самостійної роботи, та розробка спеціального навчально – методичного матеріалу, зокрема з використанням інформаційно-комунікаційних технологій, що сприяє ефективнішій самосійній роботі студентів та курсантів. Організація самостійної роботи повинна активно впливати на характер навчального процесу, систематизувати роботу студентів та курсантів протягом усього навчального процесу [6]. 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, створення мультимедійних презентацій та практичних завдань [4].

Отже, вивчення фізико-математичних дисциплін вносить невичерпний виховний і розвиваючий потенціал, і прихований він не в готових алгоритмах, теоремах і 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.

Використання інформаційно-комунікаційних технологій забезпечує, з одного боку, актуалізацію, коригування, збагачення й розширення спектру наявного суб'єктного досвіду студентів зі здійснення різних видів методичної діяльності, а з іншого – інтеграцію його із суспільно-історичним досвідом шляхом наповнення відповідним науковим змістом, є важливим засобом для формування методичної компетентності майбутнього фахівця під час навчання у вищому навчальному закладі.

Література

1. Акуленко І. А. Відеолабораторія майбутнього вчителя математики профільної школи : електрон. посібник для студ. педагог. ВНЗ [Електронний ресурс] / І. А. Акуленко. – 1,48 Гб. – Черкаси, ЧНУ, 2014. – 1 електрон. опт. диск (DVD–ROM) ; 12 см. – Систем. вимоги : Autoplay Menu Designer 3.6, Microsoft Office PowerPoint 2007, Adobe Flash Player. – Назва з контейнера.

2. Білоконна Н. І. До проблеми використання інформаційних технологій у навчальному процесі / Н. І. Білоконна, С. П. Білоконний // II Славянские педагогические чтения: Тез. докл. междунар. конф., 16 – 18 окт. 2003. – Тирасполь, 2003. – С. 49-53.

3. Демиденко В.К. Психологія вищої освіти. [Навч. посібн.] / В.К. Демиденко – Бердянськ, 2003.

4. Основи нових інформаційних технологій навчання: [Посібник для вчителів] / Авторська колегія за ред. Ю. І. Машбиця. – К. : ІЗМН, 2010. – 217с.

5. Основи нових інформаційних технологій навчання. [Посібник для вчителів] / Авторська колегія за ред. Ю. І. Машбиця. – К. : ІЗМН, 2010. – 217с.

6. Слєпкань З.І. Методика навчання математики: [Підруч. для студ. мат. спеціальностей пед. навч. закладів] / З.І. Слєпкань. – К. : Зодіак-ЕКО, 2000. - 512 с.: іл.

УДК 005.3

Коншин О. В.
Служба безпеки України

АКТУАЛЬНІ ПИТАННЯ ПІДГОТОВКИ ФАХІВЦІВ У ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Є чотири складові сили будь-якої держави – політична, економічна, дипломатична та інформаційна. Зміцнення інформаційної безпеки держави на сучасному етапі з урахуванням новочасних загроз національним інтересам України слід розглядати в двох аспектах: підготовка, перепідготовка фахівців в галузі інформаційної безпеки та усунення недоліків, перешкод та створення новітніх системних підходів у функціонуванні діючої системи державної інформаційної політики.

В умовах збільшення інформаційного простору України і входження в світовий інформаційний простір вагомої гостроти та актуальності набувають питання забезпечення інформаційної безпеки в інформаційно-комунікаційних системах України як однієї зі складових інформаційної безпеки держави і в першу чергу підготовка фахівців за напрямами «Безпека інформаційно-комунікаційних технологій», «Системи технічного захисту інформації».

Важливу роль інформаційній безпеці відведено з розумінням того, що: інформаційна безпека є не тільки однією із головних складових національної безпеки України, але й невід'ємним компонентом усіх інших її складових. Інформаційні стратегії в сучасних умовах набирають важливе значення у випадку реалізації різних стратегій співробітництва або відіграють роль своєрідної «інформаційної зброї» при реалізації стратегії суперництва - ведення так званих «інформаційних війн»; можливість цілеспрямованого інформаційного впливу на думку людей може привести до політичних, соціальних, військових та інших конфліктів, дезорганізувати державне управління, фінансову систему, роботу наукових центрів, обумовити інші деструктивні процеси в суспільстві, руйнування та дезорганізацію інформаційної інфраструктури держави можна порівняти до наслідків застосування зброї масового ураження.

Окрему стурбованість викликає практично стихійний та некерований розвиток та використання мережі Internet, що створює

передумови для використання її можливостей терористичними формуваннями та іноземними спецслужбами. Підготовка фахівців у цій сфері повинна вестися в державі за напрямом «Управління інформаційною безпекою».

Слід зазначити, що на сьогодні в Україні функціонує понад 5 тисяч режимно-секретних органів на підприємствах та установах різної форми власності. З огляду на потреби державного і приватного сектору України у фахівцях з більш широкого кола питань інформаційної безпеки, включаючи інформаційно-психологічну безпеку з 2010 року у Навчально-науковому інституті інформаційної безпеки НА СБ України розпочата підготовка кадрів за спеціальністю "Управління інформаційною безпекою" (галузь знань "Інформаційна безпека). За названими спеціальностями вищі навчальні заклади України здійснювали підготовку випускників відповідно до Постанови Кабінету міністрів України № 1719-2006 р. "Про перелік напрямів, за якими здійснюється підготовка фахівців у вищих навчальних закладах за освітньо-кваліфікаційним рівнем бакалавра".

У той же час у минулому році, не приймаючи до уваги пропозиції СБ України, що надавались на етапі формування переліку, Постановою Кабінету Міністрів України № 266-2015 р. затверджено новий перелік галузей знань та спеціальностей вищої освіти, у якому відсутні спеціальності "Організація захисту інформації з обмеженим доступом" та "Управління інформаційною безпекою", що стало підставою з 1 вересня 2015 року для припинення Національною академією СБ України набору студентів за вказаними спеціальностями та фактично унеможливлює підготовку фахівців для сфери інформаційної безпеки та охорони інформації з обмеженим доступом, у тому числі і для потреб СБ України, у будь-яких вітчизняних вишах.

Ситуація, коли замість галузі знань "Інформаційна безпека" та відповідних напрямів підготовки "Безпека інформаційно-комунікаційних технологій", "Системи технічного захисту інформації" та "Управління інформаційною безпекою" залишено лише одну спеціальність "Безпека інформаційно-комунікаційних технологій" у новій галузі знань "Інформаційно-комунікаційні технології" обмежує підготовку фахівців до вузького напряму оперативно-службової діяльності та усуває важливі на сьогоднішній день базові аспекти підготовки з управління інформаційною без-

пекою та системи технічного захисту інформації, які є найбільш важливі для нашої держави, що в свою чергу негативно вплине на інформаційну безпеку України загалом.

Адже, на сьогодні в умовах інформаційної агресії Російської Федерації проти України, ведення міждержавного протиборства провідних країн світу у кіберпросторі, підготовка фахівців у сфері інформаційної безпеки набуває широкої актуальності. Про це свідчить і затверджена Указом Президента України Стратегія національної безпеки України, у якій пріоритетами забезпечення національної безпеки визначено, зокрема, удосконалення професійної підготовки у сфері інформаційної безпеки та створення системи підготовки кадрів у сфері кібербезпеки для потреб органів сектору безпеки і оборони.

Враховуючі специфіку діяльності СБ України та наявність відомчих ВНЗ, достатнього рівня науково-педагогічного потенціалу, залишається не вирішеним питання щодо створення на їх базі технічного факультету з підготовки, перепідготовки та підвищення кваліфікації фахівців у галузі інформаційної безпеки виключно в інтересах СБ України.

Актуальність цього питання підтверджується тим, що з урахуванням існуючого дифіциту фахівців достатнього рівня, слухачі потоку підвищення кваліфікації оперативного складу профільних підрозділів у сфері інформаційної безпеки СБ України вимушені висловити пропозиції щодо збільшення кількості занять за участю представників практичних підрозділів Центрального управління Служби безпеки України та кількості годин на проведення стажування в підрозділах СБ України, додати семінари-дискусії, практичні заняття за тематикою реалізованих справ.

Такими що потребують уваги можна також назвати наступні питання, а саме: недостатня адаптація змісту підготовки фахівців у ВНЗ до сучасних і перспективних потреб інформаційної безпеки за умов стрімкого розвитку науково-технічних засад інформаційного суспільства та суттєвого оновлення спеціалізованих програмно-апаратних засобів захисту інформації протягом періоду навчання (несвоєчасне оновлення стандартів освіти); відставання навчально-матеріальної бази ВНЗ від новітніх програмно-апаратних засобів захисту інформації, що застосовуються у органах державної влади, силових структурах, корпораціях, компаніях та підприємствах (у зв’язку з їх вартістю); низький рівень вза-

ємодії з ВНЗ провідних країн світу (обмін інформацією, досвідом, науково-методичним забезпеченням, стажування, тощо) з питань вдосконалення підготовки фахівців у галузі інформаційної безпеки; низький рівень володіння іноземною мовою (технічною мовою оригінале країн сучасних технологій та наукових розробок в галузі інформаційної безпеки), особливо англійською.

На думку багатьох фахівців, незважаючи на різноманіття та тонкощі спеціальної техніки для отримання та передачі інформації, людина залишається одним з найбільш вірогідних джерел витоку інформації. Сама людина в багатьох випадках носій інформації з обмеженим доступом. Тому не менш важливо приділяти достатньої уваги підбору кандидатів, які будуть працювати з інформацією з обмеженим доступом, необхідно враховувати їх ділові, професійні, моральні якості і психологічні особливості. Вкрай важливо організувати відповідний підбір та відбір, формувати у студентів (курсантів) низку необхідних якостей.

УДК 378

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

АКТУАЛЬНІ ПРОБЛЕМИ ПІДГОТОВКИ ФАХІВЦІВ У СФЕРІ БЕЗПЕКИ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

На сьогодні інформаційно-комунікаційні технології (ІКТ) стали потужною силою перетворення суспільного життя та інноваційного розвитку. Фактично саме вони змінили за останні роки всі галузі економіки світу.

В Україні інформаційні та телекомунікаційні послуги складають п'яту частину вітчизняного ринку послуг. При цьому частка ІКТ у ВВП країни становить понад три відсотки. Ця галузь одна з небагатьох в Україні зберегла тенденції зростання.

Але, нажаль, Україна не досягла бажаного рівня розвитку сфери ІКТ, зокрема, у перетворенні національної економіки у

цифрову. Попри позитивні тенденції, сфера ІКТ інших країн розвивається значно швидше, ніж України.

Перелік проблемних питань, що стримують розвиток ІКТ в Україні надзвичайно широкий і докладно розглядався під час парламентських слухань, які відбулись 3 лютого цього року.

Слід відзначити, що на важливості освіти, як одного з компонентів реформи галузі ІКТ, наголошували в свої доповідях третина доповідачів на зазначених слуханнях. Крім того, чверть доповідачів звернули увагу на потребу вдосконалення в Україні сфери інформаційної безпеки та на важливості підготовки відповідних фахівців.

Перша частина доповіді присвячена досвіду Інституту спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут" в сфері підготовки висококваліфікованих офіцерських кадрів в сфері безпеки державних інформаційних ресурсів.

Друга частина доповіді присвячена проблемним питанням, що виникли внаслідок прийняття Кабінетом Міністрів України постанови "Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти", яка фактично ліквідувала галузь знань 1701 "Інформаційна безпека". В умовах ведення неприкритої гібридної війни та збройної агресії РФ проти України, яка спрямована в першу чергу на руйнування основ національної безпеки, на порушення системи державного управління, внесення розбрату між громадянами держави через засоби масової інформації та соціальні мережі, знищення галузі знань вбачається, м'яко кажучи, недоречним.

Замість цілої ГАЛУЗІ ЗНАНЬ, Міністерство освіти і науки України пропонує в рамках спеціальності 125 «Кібербезпека» галузі знань 12 «Інформаційні технології», запровадити спеціалізації «Безпека інформаційно-комунікаційних технологій», «Технічний захист інформації», «Управління інформаційною безпекою».

Фахівці ІСЗЗІ НТУУ "КПІ" визнають актуальність підготовки за спеціальністю "Кібербезпека", але як важливої складової в межах галузі "Інформаційна безпека". На наш погляд, міжнародний стандарт ISO/IEC 27032:2012(E) виражає погляд на це питання міжнародного експертного середовища. Згідно з ним, кібербезпека є окремим доменом безпеки і забезпечує конфіденційність, цілісність та доступність інформації у кіберпросторі, що має прояви лише у взаємодії людей та організацій в Інтернет.

На даний час триває конструктивний діалог з МОН щодо зазначеного питання і, сподіваюсь, що в недалекому майбутньому наша спільна робота дозволить врахувати позицію експертів з інформаційної безпеки і не тільки зберегти національну освітню та наукову школу, але і продовжити активний розвиток освітньої підготовки з інформаційної безпеки.

УДК 372.8:004

Коркач І. В.
Національна академія СБ України

АКТУАЛЬНІ ПИТАННЯ ВИКЛАДАННЯ НОВІТНІХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ВИЩИХ НАВЧАЛЬНИХ ЗАКЛАДАХ УКРАЇНИ

У наш час, коли стрімко розвиваються інформаційні технології, не можна отримати повноцінну вищу освіту без вивчення інформатики. Сьогодні ця дисципліна викладається щонайменше у 163 вищих навчальних закладах України [1]. Поверховий аналіз показує, що основними темами при вивченні інформаційних технологій насамперед є такі:

- будова й архітектура комп'ютера;
- операційні системи;
- безпечне використання комп'ютера;
- основи телекомунікації;
- офісні програми;
- комп'ютерна графіка;
- основи програмування.

Схожі рекомендації надавав раніше Інститут інноваційних технологій і змісту освіти, реорганізований нині у дві окремі структури – Інститут модернізації змісту освіти та Інститут освітньої аналітики [2].

Основне направлення освітньої діяльності при вивченні інформатики сконцентроване на засвоєнні будови комп'ютерної техніки та методах використання основних програмних пакетів для підготовки документів, звітів, наукових досліджень тощо.

На погляд фахівців, зміст вивчення основ інформаційних технологій дещо відстає від розвитку предметної галузі інформа-

тики, у зв'язку з чим фактичний рівень підготовки не завжди відповідає вимогам сьогодення [3]. Стрімкий розвиток засобів інформатизації, інформаційних й особливо телекомунікаційних технологій вимагає нового наповнення дисципліни та кардинального переосмислення цілей, змісту, засобів, методів і форм підготовки з інформатики на сучасному рівні і повинен знайти відображення в системі загальної освіти. Для того, щоб іти «в ногу» з технологіями, треба не просто вдосконалювати навчальний матеріал у зв'язку з появою нових версій програмного забезпечення, а концептуально переглянути перелік компетенцій, які ми маємо формувати у майбутніх фахівців. На це впливає багато чинників, найголовнішими з яких є:

Інформатика активно вивчається в загальноосвітній школі. Молодь, котра вступає на навчання до вищих навчальних закладів, уже знайома з азами комп'ютерної техніки, різновидами операційних систем і має навички роботи з основними офісними пакетами.

Уже не тільки в кожній оселі є комп'ютер, а кожен член родини має свій вихід до Інтернету за допомогою власного ПК, планшета чи мобільного телефону, який у наш час мало відрізняється від комп'ютера.

Різноманітність операційних систем, що використовує пересічна людина. В однієї людини домашній комп'ютер може працювати під MS Windows, ноутбук під Linux, а мобільний пристрій – під iOS чи Android. Відпадає необхідність їх вивчати, бо зробити це якісно просто неможливо. До того ж, розробники системного програмного забезпечення прикладають чимало зусиль, щоб кінцевому користувачу і не знадобилися ці знання.

Стрімкий прогрес новітніх мережевих технологій, таких, як пошукові системи і хмарні обчислення, доступні й інтуїтивно зрозумілі навіть людям похилого віку, що дають змогу працювати з інформацією, не замислюючись, де вона знаходиться, де зберігається і звідки береться.

Інформаційний вибух сьогодення, коли кількість доступної інформації подвоюється кожні вісімнадцять місяців. Здебільшого (до 95%) цей потік складається з неструктурованих даних і лише 5% складають різні бази даних [4]. Сучасний фахівець має орієнтуватись у цих потоках, швидко знаходити і вміло сортувати необхідну інформацію.

Нові виклики у сфері інформаційної безпеки, перед якими опинилася Україна майже непідготовленою. Насамперед це інформаційне протиборство з використанням глобального медіапростору, соціальних мереж, фейкових ЗМІ та ін. А також кібернетичні атаки, що не є теоретичними, а вже проводяться проти нашої держави та її критичної інфраструктури. І якщо цей аспект не є таким важливим при підготовці студентів в інших ВНЗ, то для майбутніх випускників освітніх установ правоохоронних органів є необхідним.

Тому, на наш погляд, при викладанні інформатики акцент має зміщуватися від вивчення інструментів підготовки документів, до вмілого та ефективного управління інформаційними потоками, пошуку корисної інформації в глобальному інформаційному просторі, ефективному її аналізі та використанні.

Кафедрою інформаційних систем і технологій та захисту інтересів держави у сфері інформаційної безпеки був повністю перероблений зміст навчального матеріалу й розроблена якісно нова дисципліна «Сучасні інформаційні технології», яка з минулого (2015) року викладається в НА СБ України.

Для формування компетентності управління інформацією у майбутніх фахівців були обрані такі основні напрями розвитку дисципліни:

- сучасні інформаційні відносини, та їхнє нормативне регулювання;
- захист інформації при роботі з мережею Інтернет;
- хмарні обчислення;
- методи несанкціонованого доступу до інформації в ІТС;
- методи відбору й аналізу інформації з відкритих джерел (OSINT).

Із метою переходу до нового наповнення матеріалу проводиться поступове введення нових тем та проведення ретельного аналізу результатів навчання.

Зрозуміло, що для досягнення поставленої мети необхідно удосконалювати не лише навчальний матеріал, а й модернізувати технічну базу, використовувати нову методику викладання, включаючи дистанційне навчання, широко застосовувати досягнення інформаційної інфраструктури.

Література

1. Перелік ВНЗ, у яких викладається дисципліна «Інформатика та комп'ютерна техніка» [Електронний ресурс]. – Режим доступу : http://www.osvita.com.ua/ua/universities/?page=1&directions=45&desc=2.
2. Основи інформатики для ВНЗ [Електронний ресурс]. – Режим доступу : http://vzvo.gov.ua/navchalni-prohramy/95-computer-basics-for-universities.html.
3. Електронний навчально-методичний комплекс з дисципліни «Методика викладання основ інформаційних технологій» [Електронний ресурс]. – Режим доступу : http://ito.vspu.net/ENK/MVOIT/index.html.
4. Информационной взрыв // Википедия [Электронный ресурс]. – Режим доступа : https://ru.wikipedia.org/wiki/Информационный_взрыв.

УДК 005.3

Мельник С. В.
кандидат технічних наук, доцент
Національна академія СБ України

АКТУАЛЬНІ ПИТАННЯ ЗАПРОВАДЖЕННЯ В УКРАЇНІ СПЕЦІАЛЬНОСТІ «КІБЕРБЕЗПЕКА»

У зв'язку із прийняттям постанови Кабінету Міністрів України від 29 квітня 2015 р. № 266 «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти» в українській освіті зникла галузь знань 1701 «Інформаційна безпека» зі спеціальностями 170101 «Безпека інформаційних і комунікаційних систем», 170102 «Системи технічного захисту інформації» та 170103 «Управління інформаційною безпекою». Відповідно до таблиці переходів для галузі знань «Інформаційна безпека» визначено одну спеціальність «Кібербезпека» галузі знань «Інформаційні технології», в яку ще входять спеціальності «Інженерія програмного забезпечення», «Комп'ютерні науки та інформаційні технології», «Комп'ютерна інженерія», «Системний аналіз».

Тому виходячи із вимог Закону України «Про вищу освіту» стають актуальними питання щодо змісту (переліку компетентностей), обсягу та оцінювання якості змісту і результатів освітньої діяльності вищих навчальних закладів за спеціальністю «Кібербезпека» (розроблення стандарту вищої освіти), запроваджен-

ня спеціалізацій, що відповідають спеціальностям колишньої галузі знань «Інформаційна безпека», розроблення освітніх програм та проведення їх акредитації.

Як наслідок, розпочалась активна дискусія щодо співвідношення понять «Інформаційна безпека» та «Кібернетична безпека», методологічних основ діяльності із забезпечення інформаційної та кібернетичної безпеки.

На сьогодні більша частина фахівців все ж таки вважає, що поняття кібернетичної безпеки є складовою частиною поняття інформаційної безпеки, оскільки розглядаються ті ж самі загрози, методи, засоби і заходи захисту, але лише в кіберпросторі.

Вочевидь не поглиблюючись у деталізацію відомих визначень поняття «Кіберпростір», під ним можна розуміти віртуальне середовище, яке є по суті програмним забезпеченням комп'ютерної техніки, мережевого та телекомунікаційного обладнання, а також людський фактор (в термінах технічного захисту інформації – це автоматизовані системи класів 1, 2 та 3). Відповідно, основними загрозами кібербезпеки можна вважати наміри застосування шкідливого програмного забезпечення (порушення безпеки інформації та регламенту роботи технічних засобів), шкідливого контенту (реалізація негативних інформаційно-психологічних впливів), порушення авторських прав, використання технологічних можливостей кіберпростору для підготовки та скоєння правопорушень.

Таким чином, є логічним, що в спеціальності «Кібербезпека» по за увагою залишаються заходи захисту об'єктів інформаційної діяльності від витоку акустичної інформації (яка не обробляється в інформаційно-комунікаційних системах – ІКС), побічних електромагнітних випромінювань та наведень ІКТ, силових впливів на технічні засоби тощо. Тобто, фактично, не враховується предмет колишньої спеціальності 170102 «Системи технічного захисту інформації», який визначається реальними потребами практики у захисті державних і приватних інформаційних ресурсів.

Далі звернемо увагу на питання формалізації діяльності із забезпечення кібернетичної безпеки, яку можна розглянути як комплекс заходів із профілактики, захисту, виявлення та реагування на інциденти кібербезпеки, протидії кіберзлочинності зокрема. Недарма в стратегії кібербезпеки України визначено у яко-

сті одного із принципів забезпечення кібернетичної безпеки особи, суспільства та держави комплексний підхід до впровадження правових, організаційних, технічних та інформаційних заходів, оскільки кібербезпека – це технічна, правова і соціальна проблема.

Виходячи зі сказаного стає зрозумілим, що завдання забезпечення безпеки інформаційних і комунікаційних систем (технічний захист інформації від несанкціонованого доступу та криптографічний захист інформації), а також управління інформаційною безпекою (відповідно до стандартів серії ISO/IEC 2700X) є лише складовими частинами системи кіберзахисту.

Загалом же сфера кібернетичної безпеки охоплює проблеми: захисту інформації особи, суспільства та держави (включаючи завдання управління інформаційною безпекою); інформаційного протиборства у військовій сфері; попередження, виявлення, припинення та розкриття кіберзлочинів; протидії розвідувально-підривній діяльності іноземних спеціальних служб та іншим протиправним діям. Тому національна система кібербезпеки передбачає координацію дій Держспецзв'язку, Міністерства оборони та Генерального штабу, Міністерства внутрішніх справ (Національної поліції), Служби безпеки та розвідувальних органів України, а також бізнесу та громадськості. В свою чергу відповідно до сфер компетенції формується потреба державного і приватного сектору у фахівцях з кібербезпеки.

Виходячи зі сказаного зрозуміло, що сформувати в рамках спеціальності «кібербезпека» єдині вимоги до знань, вмінь, практичних навичок, способів мислення, світоглядних і громадських якостей та морально-етичних цінностей (компетентностей) фахівців та професіоналів з кібернетичної і інформаційної безпеки достатньо проблематично, тому що мова йде не про формування окремих спеціалізацій, а спеціальностей, які обумовлені сучасною практикою забезпечення інформаційної безпеки.

Враховуючи непохитність позиції Міністерства освіти і науки України щодо імплементації галузі знань «Інформаційна безпека» у спеціальність «Кібербезпека» можливо розглянути два варіанти вирішення питання із започаткування спеціалізацій «Безпека інформаційних і комунікаційних систем», «Системи технічного захисту інформації», «Управління інформаційною без-

пекою» та можливо «Кібербезпека» для відповідних сфер відомчих компетенцій.

Перший. Започаткування зазначених спеціалізацій в рамках різних спеціальностей, які найбільш близькі з точки зору нормативної частини освітніх програм.

Другий. Формування нормативної частини освітніх програм за спеціальністю «Кібербезпека» виходячи зі спільної частини компетентностей спеціалізацій у цій професійній сфері, що можуть стосуватись основ програмної і комп'ютерної інженерії, методів, засобів та заходів захисту інформації та управління інформаційною безпекою. При цьому доцільно передбачити необхідну деталізацію у варіативних частинах освітніх програм відповідних спеціалізацій.

Перший підхід можна вважати менш прийнятним, оскільки у цьому випадку втрачається зв'язок між розглядом методів забезпечення інформаційної і кібернетичної безпеки, який лежить в основі комплексного підходу до захисту, і є необхідною умовою для гарантованого забезпечення визначеного достатнього рівня захисту.

Література

1. О. Орлов Державне управління підготовкою фахівців у сфері кібербезпеки. Режим доступу: http://www.kbuapa.kharkov.ua/e-book/db/2013-2/doc/3/01.pdf

2. В. Бурячок, В. Богуш Рекомендації щодо розробки та запровадження профілю навчання «Кібернетична безпека» в Україні. Режим доступу: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/bezin_2014_20_2_5.pdf

УДК 159.923.5

Паливода О. О.
Національна академії СБ України

ПІЗНАВАЛЬНА АКТИВНІСТЬ ФАХІВЦІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК ПЕРЕДУМОВА ЇХ УСПІШНОГО ПРОФЕСІЙНОГО СТАНОВЛЕННЯ

Сучасний стан розвитку людства визначають як епоху інформаційного суспільства. Наша держава включена у процес загальної інформатизації і формування єдиного світового інформаційного простору. Науковці зазначають, що застосування новітніх технологій, інформаційний «вибух» та швидке «зістарення» інформації, різке ускладнення, автоматизація та комп'ютеризація виробничих процесів, висока вірогідність виникнення «нестандартних» ситуацій у виробничій та соціальній сферах висувають все нові вимоги до фахівців [1]. Адже вони, окрім професійних знань, вмінь та навичок, повинні мати ще й спеціальні компетентності та особистісні властивості, що забезпечують гнучкість та мобільність професійної поведінки, самостійність у пошуку та засвоєнні нової інформації, формування нового професійного досвіду.

Особливо такі вимоги актуальні у сферах, що характеризуються динамічними змінами умов та змісту праці, до яких належить інформаційна безпека. Успішність професійного становлення фахівців цієї сфери визначається постійним розвитком їх психологічних характеристик відповідно до вимог професійної діяльності, оскільки професіогенез є досить динамічним, індивідуальним і неповторним для кожного з них.

З метою попередження можливого негативного впливу професійної діяльності на психіку фахівця та прогнозування успішності виконання ним професійних завдань проводяться професіографічні й психографічні дослідження. Останні мають на меті визначити перелік професійно важливих та професійно небажаних якостей. Однією із найважливіших характеристик фахівця інформаційної безпеки є високий рівень пізнавальної активності. Вона ґрунтується на пізнавальних інтересах, ініціативі, активності, інтегрує пізнавальну мотивацію, вольове прагнення до пізнання, комплекс знань, умінь, навичок і здібностей та забезпечує ефективну самостійну пізнавальну діяльність у професійних ситуаціях

інформаційної невизначеності, дефіциту часу та в умовах психофізичного навантаження.

Пізнавальну активність фахівця визначають як характеристику особистості, яка виявляється у її ставленні до пізнавальної діяльності, що передбачає стан готовності, прагнення до самостійної діяльності, спрямованої на засвоєння індивідом соціального досвіду, накопичених людством знань і способів діяльності, а також знаходить вияв у пізнавальній діяльності [2].

Щоб об'єктивно охарактеризувати пізнавальну активність, необхідно виокремити її основні структурні компоненти. Так до структури пізнавальної активності включають такі три основні компоненти [3]: мотиваційний, операційно-дійовий і особистісний. Мотиваційний компонент містить емоційно-спонукальні чинники пізнавальної активності фахівців, їхнє ставлення до підвищення свого професійного рівня, прагнення до засвоєння нових знань і способів пізнавальної діяльності. Операційно-дійовий компонент відображає процесуально-інструментальний аспект пізнавальної активності і включає такі складові: навчальні уміння, способи і прийоми пізнання, властивості мислення та зовнішні прояви пізнавальної діяльності. Особистісний компонент відображає сформованість особистісних рис фахівців, які проявляються і розвиваються в пізнавальній активності: допитливість, вдумливість, рефлексивність, наполегливість, самокритичність, пізнавальна ініціативність тощо.

До того ж, науковці [2; 4] характеризують розвиток пізнавальної активності як процес переходу від можливостей, схильностей, прагнення особистості реалізувати свої сили, потреби в їх саморозвитку до перетворення особистості в суб'єкта діяльності, активного й творчого, що самореалізується. Зазначають, що її розвиток відбувається переважно на трьох рівнях (залежно від характеру діяльності, ступеня самостійності та творчості). Перший, репродуктивний, виявляється в діяльності виконавського відтворювального характеру. Репродуктивна активність характеризується усвідомленим заучуванням та відтворенням зразка розумової чи практичної дії. Другий рівень – реконструктивний, або продуктивний, на якому передбачається не тільки копіювання, але і вибір способів діяльності, використання здобутих знань, їх перенос в інші ситуації, їх певну інтерпретацію, репродуктивна активність характеризує особистість з боку готовності оволодіва-

ти готовими знаннями, енергійності пізнавальної діяльності. Третій, творчий рівень, характеризується ініціативою, самостійністю особистості у визнанні цілей та постановці проблем, завдань пізнавальної діяльності, способів її здійснення, потребою оволодіння знаннями, інтересом, новизною, оригінальністю та оптимальністю.

Слід відзначити, що творча складова професійного розвитку завжди нерозривно пов'язана з його репродуктивною складовою. При цьому основним змістом творчого компонента професійної діяльності є знаходження нових ідей, професійних смислів, нових цілей професійної самореалізації. У репродуктивному же компоненті переважають процеси засвоєння і вітворення, припускають роботу з масивами інформації. Взаємодія творчого та репродуктивного компонентів забезпечується аналітичними і рефлексивними процесами. Оскільки процес професійного розвитку представляє собою ряд послідовних етапів, на кожному з яких може бути актуалізований більшою мірою творчий, або репродуктивний компонент, то управління професійним розвитком доцільно розглядати як процес регулювання їх взаємодії в цілісній професійній діяльності.

Із вище викладеного слідує, що успішність професійного становлення фахівця визначається ступенем відповідності індивідуально-психологічних особливостей, особистісних якостей, здібностей, спрямованості вимогам діяльності. Саме тому, при підготовці фахівців слід не тільки формувати у них необхідні професійні знання, уміння та навички, але й звертати увагу на розвиток в них професійно важливих якостей, які б зумовлювали успішність професійної діяльності. Для фахівців інформаційної безпеки однією із найважливіших якостей є висока пізнавальна активність – складна психологічна характеристика особистості, що виявляється у рисах характеру (допитливість, вдумливість, схильність до участі в дискусіях і відстоюванні власних поглядів, рефлексивність, схильність до інтелектуального самовдосконалення, самокритичність, впевненість у собі, пізнавальна сміливість, схильність до пізнавальної самореалізації, пізнавальна ініціативність) та реалізовується на трьох рівнях (репродуктивному, реконструктивному і творчому). Підвищенню пізнавальної активності сприятиме розвиток інтелектуального потенціалу фахівців, напрацю-

вання разом із ними гностичних механізмів роботи з великою кількістю інформації та комплекс сформованих професійно важливих якостей.

Література

1. Кокун О.М. Психологія професійного становлення сучасного фахівця: монографія / О.М. Кокун – К. : ДП «Інформ.-аналіт. агенство», 2012. – 200 с.

2. Лозова В.І. Цілісний підхід до формування пізнавальної активності школярів / В.І. Лозова. – 2-е вид., доп. – Харків : «ОВС», 2000. – 164 с.

3. Горохівський О.Є. Формування пізнавальної активності курсантів вищих навчальних закладів міністерства надзвичайних ситуацій у процесі вивчення спеціальних дисциплін : автореф. дис. на здобуття наук. ступ. канд. пед. наук : спец. 13.00.04 «Теорія і методика професійної освіти» / О.Є. Горохівський. – Вінниця, 2006. – 20 с.

4. Лузан П.Г. Цілеспрямоване формування навчально-пізнавальної активності студентів / П.Г. Лузан // Науковий вісник Національного аграрного університету : зб. наук. пр. – Вип 1. – Київ, 1997. – С. 154-163.

УДК 316.32:165.63

Поперечнюк В. М.

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

СУЧАСНІ РИЗИКИ ФОРМУВАННЯ ТА РОЗВИТКУ ОСОБИСТОСТІ В УМОВАХ СТАНОВЛЕННЯ ІНФОРМАЦІЙНОГО ПРОСТОРУ

Нині, людина весь час знаходиться у безперервних потоках інформації (ЗМІ, комп'ютери, канцелярська робота, факси, телефони, кіно, плакати, реклама, законопроекти, рахунки та тисячі інших джерел) які проникають в її свідомість, впливають на людину та її життя, змінюють парадигму сприйняття і розуміння навколишньої дійсності. У принципі, умови тотального панування інформації, на думку Е. Тоффлера, є досить комфортними для людини, але захаращеність інформаційного простору, негативно впливає на формування та розвиток людини і її потреб (у першу чергу інформаційних та когнітивних), адже вона буде споживати

весь запропонований їх медійний продукт не будучи вибагливою до його якості та змісту [1, с. 133].

Люди настільки починають залежати від інформації, що без блоку новин вже не можуть усвідомити свого життя, весь час намагаються та хочуть бути поінформованим про останні події. Залежність суспільства від інформації пояснюється, як когнітивними здібностями особистості, так і прагнення держави та ЗМІ показати свою значимість, дати більше новин, тим самим розширити аудиторію. Як влучно зауважив представник Об'єднаного комітету керівників штабів США (1993-1997 рр.), генерал Дж. Шалікашвілі: «Ми не перемагаємо, поки CNN не повідомляє, що ми перемагаємо» [2, с. 104].

При цьому, ЗМІ стають не лише головним джерелом одержання інформації, а й переймають функції головного засобу формування національної та міжнародної думки, є невід'ємним компонентом зовнішньої та внутрішньої політики кожної держави [3, с. 488], а відтак стають ареною для більшості політичних зіткнень та суперечок [4, с. 67].

Використання ЗМІ для маніпулювання суспільною думкою має системний характер та низку фактів такого прояву. За даними ГО «Телекритика», щодо умов дотримання професійних стандартів у роботі вітчизняних інформаційних служб провідних телеканалів за грудень 2013 р. було виявлено недостатній рівень дотримання журналістських стандартів, при висвітленні протестних подій у Києві та всій Україні в наслідок силового розгону Євромайдану. Водночас провідні канали подавали інші новин із порушенням балансу думок, без належної повноти інформації, без відокремлення фактів від думок, а також із наявними журналістськими оцінками [5].

Зокрема, сучасний медіапростір характеризується О.В. Полікарповою наступними ознаками: надлишком непотрібно (зайвої) інформації, за допомогою якої приховується конкретна інформація; відсутність адекватно структурованої інформації; значна кількість та хаотичність великої кількості різних «інформаційних фантомів» (снігова людина, чупакабра, НЛО тощо) та ін. [6]. Зазначені прояви агресивності інформаційного простору негативно впливають на людину. «Перенасичення» людини інформацією виснажує її моральний, духовний та інтелектуальний потенціал, втомлюючи та перевантажуючи не потрібною інформацією, що

спричиняє зниження когнітивних й інтелектуальних здібностей особистості, зменшення здатності до критичного сприйняття та осмислення інформації [7, с. 134-135], або навіть кризи ідентичності [8]. Такі умови породжують загрози інформаційній безпеці та безкарного маніпулятивного впливу на людину, її психіку і свідомість, у результаті чого, суспільство ризикує бути керованим.

Тобто, якщо говорити про прийдешню соціально-економічну формацію, з тотальними об'ємами різного характеру та сутності інформації, то сучасна людина, просто не готова до цього, її мозок ще не в змозі адекватно реагувати та опановувати такі масиви інформації. З цього приводу влучним є висловлювання наведене у Всесвітній доповіді ЮНЕСКО «До суспільства знань»: «В сучасних інформаційних потоках, знайти необхідну інформацію, аналогічно до спроби напитись із пожежного крану – води виставить, але треба примудритись не захлинутися». Звісно, ІКТ фільтрують інформацію, проте, вони не можуть так само ефективно «відсіяти» непотрібну інформацію як людський мозок [9, с. 52].

Тому, варто підготувати людину та суспільство до належного сприйняття й обробки інформації, щоб кожен міг опанувати елементарні навики інформаційної культури і кіберсоціалізації, що сприятиме адекватному, ефективному використанню ІКТ та задоволенню інформаційних потреб населення. Адже, остання в інформаційному суспільстві, є основою розвитку людини та сприяє задоволенню інших потреб.

Отже, виходячи із аналізу нинішніх соціально-політичних реалій життя України та світу, виявляється необхідність гармонійного розвитку високоінтелектуальної людини, з високим рівнем соціальної відповідальності зданої ефективно використовувати інформацію та ІКТ для задоволення власних інформаційних потреб. Адже, лише за таких умов суспільство може диктувати свої умови та самостійно формувати якісний інформаційний простір.

Література

1. A.Toffler, Future shock the third wave [Електроннний ресурс]: BantamBooks, 1980. – 448p. – Режим доступу: http://www.crossroadscounsellinggroup.com/resources/ebook/Toffler-ThirdWave-complimentsofCRTI.pdf.

2. Бондаренко В. О. Інформаційні впливи та інформаційні операції [Електронний ресурс] / В. О. Бондаренко, О. В. Литвиненко // Стратегічна

панорама. – № 4. – 1999. – Режим доступу : http://www.niurr.gov.ua/ukr/publishing/panorama4_2000/bo_21.htm

3. Международное право : ученик / [отв. Ред. Ю.М. Колосов, Э.С. Кривчикова]. – М. : Международные отношения, 2000. – 720 с.

4. Протидія інформаційному тероризму та його фінансуванню в сучасних умовах : монографія / В.В. Крутов, М.П. Стрельбицький, О.А. Шевченко (за аг. ред.. В.В. Крутова) – К.: Вид-во НАПрН У; Ужгород: ТОВ «ІВА», 2014. – 309 с.

5. Про що мовчали новини новини у грудні - 2013 [Електронний ресурс] // MediaSapiens/ Режим доступу: http://osvita.mediasapiens.ua/material/26525.

6. Поликарпова Е.В. Медиавоздействия на жизнедеятельность человека: аксиологические аспекты: Дис.... канд. филос. наук: 09.00.13. — Р-н-Д, 2005. — 124 с.

7. Золотар О. О. Особливості правової соціалізації особистості в інформаційному суспільстві: формування "інформаційного щита" // Філософські та суспільно-правові проблеми становлення і розвитку інформаційного суспільства: Матеріали круглого столу / 20 березня 2013 р., м. Київ / Упорядн.: Андрусишин Б. І., Майстренко І. А., Пилипчук В. Г., Фурашев В. М. – Ужгород. – ТОВ "ІВА". – 2013. – С. 133-136.

8. Див. Соціологія особистісної ідентичності в просторі права: Монографія / Богомаз К.Ю., Конох М.С., Кравцов Ю.С. та ін. – Дніпродзержинськ: ДДТУ, 2009. – 184 с; Козловець М.А. Феномен національної ідентичності: виклики глобалізації: Монографія. – Житомир: Вид-во ЖДУ ім. І. Франка, 2009. – 558 с; Пелагеша Н. Україна у смислових війнах постмодерну: трансформація української національної ідентичності в умовах глобалізації: Монографія. – К.: НІСД, 2008. — 287 с.

9. К обществам знания : Всемирный доклад ЮНЕСКО. – Париж: Издательство ЮНЕСКО, 2005. – 240 с.

УДК 342:316.4

Радзієвська О. Г.
Науково-дослідний інститут інформатики і права
Національної академії правових наук України

ІНФОРМАЦІЙНА БЕЗПЕКА ДИТИНИ В УМОВАХ ГІБРИДНИХ ВІЙН

Уже другий рік поспіль Україна перебуває в стані неоголошеної війни нового типу, яку у світі прийнято називати гібридною. Особливістю такої війни є широке застосування інформа-

ційного та інформаційно-психологічного протиборства поряд із збройним протистоянням. Беззаперечним є той факт, що у стані інформаційно-психологічної війни, що веде сьогодні країна–агресор проти нашої держави, свідомість будь-якого громадянина є об'єктом посягань і потребує посиленого захисту. Забезпечення інформаційної безпеки будь-якого громадянина гарантується ст. 17 Конституції України [1] та відповідно до Закону України «Про основи національної безпеки України» відноситься до сфери національної безпеки і є пріоритетним напрямом державної політики [2].

Особливо вразливою до негативних інформаційних впливів є свідомість дитини. Дитина ще не володіє сталими принципами та нормами. Отримана нею інформація не піддається логічному осмисленню, практично відсутня критика та аналіз, зате, емоційність сприйняття – найвища. Дитина – це ідеальний об'єкт для маніпулювання. Закладені у дитинстві посили стають основою існування та поведінки індивідуума у дорослому житті. Вкладаючи певні змісти у дитячу свідомість можна створити підконтрольну особистість, або направити її розвиток у бажаному напрямку, необхідному для досягнення поставленої мети. Тому дитяча свідомість одночасно є ще й елементом протистояння на середньо- та довготривалу перспективу. Саме свідомість дітей є об'єктом прискіпливої уваги агентів впливу.

У світлі прийняття Росією нової військової доктрини, підписаної президентом 24.12.2014 р., це твердження набуває нових змістів. Серед основних зовнішніх та внутрішніх військових небезпек у ній визначено «діяльність, пов'язану з інформаційним впливом на населення, в першу чергу на молодих громадян, що має на меті підрив історичних, духовних, патріотичних традицій в сфері захисту батьківщини.» (п. 13). [3] Відповідно, протидіяти таким загрозам пропонується комплексом військових, політичних, економічних та інформаційних заходів з широким використанням протестних настроїв населення на території противника та у глобальному інформаційному просторі (п. 15). Це дає можливість стверджувати, що найближчим часом важливість питання забезпечення інформаційної безпеки особи, а особливо дитини, в Україні буде лише зростати, потребуючи нових напрацювань на довготривалу перспективу.

Уже сьогодні є певне розуміння проблеми та спостерігаються окремі кроки у її вирішенні. Проте залишається й певна хаоти-

чність та безсистемність цього процесу. Наприклад, відповідно до Закону України «Про внесення змін до деяких законів про захист інформаційного телерадіопростору України» [4] створено перелік продуктів російського кінематографу, що заборонені для транслювання на національних каналах. Цей список постійно доповнюється. Проте у політичних ток-шоу та інтерв'ю, як і раніше, деякі політики слово-в-слово цитують ідеї країни-агресора. Непоодинокими залишаються факти цілеспрямованого запрошення російських журналістів з відвертими антиукраїнськими поглядами для роботи на телеканалах України їх власниками. Для прикладу можна згадати про шеф-редактора М. Столярову. Це також елемент інформаційної війни Росії проти України. Адже залучення проросійськи налаштованих, чи взагалі громадян РФ, тобто громадян країни-агресора, до топ-менеджменту провідних каналів України дозволяє опосередковано корегувати редакційну політику, маніпулюючи як з новинами інформаційних блоків, так і з використанням російської пропагандистської продукції в ефірі. На цьому ж прикладі видно ще одну слабкість української держави у забезпеченні інформаційної безпеки – це відсутність превентивних заходів протидії виникненню такої ситуації. Адже лише прикра випадковість завадила пані Столяровій і надалі виконувати свої функціональні обов'язки та продовжувати формувати інформаційну політику у новинних блоках загальноукраїнського телеканалу «Інтер».

Елементами інформаційної агресії Росії проти України є також неявні ознаки дискримінації представників української нації у російській кіно- та телепродукції. У будь-якому з проаналізованих серіалів чи фільмів російського виробництва обов'язково присутній персонаж українського походження в образі негативного героя: чи то злочинця, чи зрадника, чи повії. Цей персонаж, як правило, не є головним, проте формує в підсвідомості російського телеглядача негативний образ українця, а в українського – почуття сорому, вини за представника свого народу та комплекс низьковартості. Замовлення матеріалів з подібним змістом для великих медійних компаній Росії сьогодні виконують й українські виробники медіапродукції, що є недопустимим. В умовах такого прихованого інформаційно-психологічного впливу на свідомість та підсвідомість дитини складно виховати високодуховну та патріотичну особистість з високими національними та загаль-

нолюдськими цінностями. Тому при наданні дозволу на трансляцію російського медійного продукту на українському ринку необхідно більш ретельно перевіряти останній на наявність прихованого інформаційного впливу на свідомість.

Переважну більшість ефірного часу на нашому телебаченні займає продукція російського виробництва. За існуючими даними, у 2014 році топ-шістка українських телеканалів показала 29 тис. годин художнього контенту, включно з повторами, з них 55 %, тобто 15,6 тис. годин – російського художнього контенту [5]. Зважаючи на це, створюється загроза формування у дітей хибної національної світоглядної позиції.

Іншим аспектом інформаційно-психологічного впливу на свідомість дітей в умовах протистояння між Україною та Росією є друкована продукція. Нещодавно в окупованому Луганську було представлено новий ілюстрований дитячий пізнавально-розважальний журнал «Вежливые человечки». Продукція розрахована на дошкільнят та дітей молодшого шкільного віку. Головними героями оповіді є героїчні дітлахи в образах так званих «бійців Малоросії», а в негативних героях цієї оповіді не складно упізнати президента України, Прем'єр-міністра та Секретаря РНБО. Таке перекручування фактів, паплюження та зневага до перших осіб держави формує у дитячій свідомості викривлену картину сприйняття сьогодення, змінює їх цінності та життєві орієнтири і навряд чи зможе виховати з них гідну особистість з високим рівнем правосвідомості та громадянською позицією. В даному випадку цей журнал є інструментом інформаційного впливу та елементом повномасштабної інформаційної війни Росії проти України.

У підсумку хотілося б зазначити, що в умовах війни державна інформаційна політика повинна бути більш конструктивною, поєднувати зусилля на різних рівнях, базуватися на пріоритетах національної безпеки та працювати на перспективу. Вироблення концептуальних засад інформаційної безпеки, стратегій протидії негативним інформаційним впливам на дітей та комплексних програм їх впровадження дозволило б не лише виграти бій за свідомість дітей сьогодні, але й отримати перемогу у боротьбі за майбутнє процвітання нашої держави.

Література

1. Конституція України : Закон від 28.06.1996 № 254к/96-ВР – Режим доступу : // http://zakon4.rada.gov.ua/laws/show/254%D0%BA/96-D0%B2%D1%80
2. Про основи національної безпеки України : Закон України від 19.06.2003 № 964-IV. – Режим доступу : // http://zakon4.rada.gov.ua/laws/show/964-15
3. Военная доктрина Российской Федерации - Електронний ресурс. – Режим доступу : http://static.kremlin.ru/ media/events /files/ 41d527556bec8deb3530.pdf
4. Про внесення змін до деяких законів про захист інформаційного телерадіопростору України : Закон України від 05.02.2015 № 159-VIII. - Електронний ресурс. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/159-19.
5. Петренко Г. Державна інформаційна безпека: чому віз і нині там? [Електронний ресурс] : Media Sapiens – Режим доступу : http://osvita.mediasapiens.ua/media_law/government/derzhavna_informatsiyna_bezpeka_chomu_viz_i_nini_tam/ – Назва з титул. екрана. – (Дата звернення: 12.02.2016).

УДК 378.046:004

Самойленко О. О.
кандидат педагогічних наук
Національна академія СБ України
Кащук В. І.
Національна академія СБ України

ОСОБЛИВОСТІ ВИКОРИСТАННЯ ПЕРСОНАЛЬНОГО ВЕБ-РЕСУРСУ ВИКЛАДАЧА У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Актуальність теми дослідження зумовлена оновленням нормативно-правового забезпечення щодо впровадження інформаційно-комунікаційних технологій в систему вищої освіти (Закон України «Про вищу освіту», Закон України «Про Національну програму інформатизації», Указ Президента України «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні», накази Міністерства освіти і науки України).

Вивчення науково-педагогічних джерел з досліджуваної проблеми та аналіз стану технічного забезпечення системи вищої освіти дозволили окреслити такі суперечності між: вимогами, зумовленими розвитком інформаційного суспільства, і реальним станом розвитку системи вищої освіти; інтенсивним темпом розвитку інформаційних технологій в освіті та недостатнім рівнем оновлення змісту вищої освіти.

Персональний веб-ресурс викладача складається з дисциплін, які за ним закріплено. Головною метою функціонування веб-ресурсу є надання доступу студента до навчальних матеріалів з метою забезпечення якості освітнього процесу. Основною структурною одиницею веб-ресурсу є електронний навчально-методичний комплекс. Електронний навчально-методичний комплекс для наповнення персонального веб-ресурсу викладача включає: методичні рекомендації для студентів щодо сценарію самостійної роботи з даним ресурсом, послідовності виконання завдань, особливостей моніторингу; документи планування освітнього процесу (навчальні програми модулів, графік консультацій, потижневі завдання); змістовне, дидактичне та методичне наповнення модулів; лекційні матеріали з використанням мультимедійних засобів; практичні завдання із методичними рекомендаціями щодо їх виконання; електронні бібліотеки (підбір електронних книг, наукових видань, публікацій, монографій, методичних рекомендацій, інструкцій для завантаження; перелік рекомендованих джерел, наявних у бібліотеці навчального закладу і т.п.); термінологічні словники; тестові завдання для поточного контролю якості знань, самоконтролю; пакети питань для анкетування та інтерв'ювання; інші ресурси навчально-інформаційного призначення.

Окрім освітнього матеріалу персональний веб-ресурс викладача містить засоби для зворотного зв'язку у вигляді тематичних форумів та індивідуальних повідомлень. Форуми призначені для обговорення питань, які виникають у процесі опанування дисципліни. Індивідуальні повідомлення використовуються викладачем у якості нагадування про необхідність завершення певної теми студентом і здачі практичних робіт. Також передбачено спілкування студентів між собою.

Персональний веб-ресурс є системою з обмеженим рівнем доступу. Викладач самостійно надає доступ до нього. Зв'язок між

веб-ресурсом і системою відбувається по захищеному каналу зв'язку. Система розроблена на основі відкритого програмного забезпечення та поширюється за ліцензією GNU Public License.

Література

1. Биков В. Ю. Теоретико-методологічні засади моделювання навчального середовища сучасних педагогічних систем / В. Ю. Биков // Інформаційні технології і засоби навчання. [Електронний ресурс]. – Режим доступу : http://core.ac.uk/download/pdf/11083990.pdf

2. Гуревич Р. С. Сучасні інформаційні технології та їхнє використання: методичний посібник / [Гуревич Р. С., Шестопалюк О. В., Кадемія М. Ю., Кобися А. П., Кобися В. М.]. – Вінниця: ТОВ ПЦ «Енозіс», 2006. – 131 с.

3. Дубасенюк О. А. Професійна педагогічна освіта: інноваційні технології та методики [Монографія] / О. А. Дубасенюк [та ін.] ; ред. О. А. Дубасенюк ; Житомирський держ. ун-т ім. Івана Франка. – Житомир : ЖДУ ім. І. Франка, 2009. – 564 с.

4. Самойленко О. О. Засоби спілкування в мережі Інтернет: метод. посіб. / О. О. Самойленко. – К. : УМО НАПН України, 2014. – 88 с.

УДК 355.232 : [355.23:355.40] (477) (091)

Супрунов Ю. М.
Заслужений працівник освіти України
Національний університет оборони України
імені Івана Черняховського

СТАНОВЛЕННЯ СИСТЕМИ ПІДГОТОВКИ ВІЙСЬКОВИХ ФАХІВЦІВ У ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ (1991-2012 роки)

Складність воєнно-політичної обстановки у світі і, в першу чергу навкруги України, визначає необхідність удосконалення системи забезпечення інформаційної безпеки України. Важливим компонентом такої системи є її кадрове забезпечення. Фахівців у галузі інформаційної безпеки готують в загальній системі підготовки фахівців розвідувально-інформаційних систем (РІС).

Пропонується наступне визначення РІС: розвідувально-інформаційні системи – це складні інформаційні системи, основною чи допоміжною функцією яких є функція моніторингу (роз-

відки) для потреб сектору безпеки і оборони держави. При цьому слід зазначити, що функція розвідки РІС включає складові: добування, збору, обробки та аналізу розвідувальних даних (формування розвідувальної інформації), що визначає рівень складності та можливості інформаційної системи.

Важливість удосконалення системи підготовки фахівців РІС визначається і завданнями Воєнної доктрини України (нова редакція від 24.09.2015):

«…модернізація системи воєнної розвідки на стратегічному та оперативно-тактичному рівнях;

створення єдиної системи видової розвідки;

посилення розвідувальної діяльності в інтересах підготовки та проведення Україною стратегічних комунікацій, контрпропагандистських заходів та інформаційно-психологічних операцій;

попередження та ефективна протидія інформаційно-психологічним впливам іноземних держав, спрямованим на підрив обороноздатності, порушення суверенітету і територіальної цілісності України, дестабілізацію внутрішньої соціально-політичної обстановки, провокування міжетнічних та міжконфесійних конфліктів в Україні…»

Стан єдиної системи військової освіти України в світлі сучасних воєнно-політичних викликів і загроз вже не повною мірою відповідає вимогам до підготовки військових фахівців. Для своєчасного та ефективного удосконалення підготовки фахівців, уникнення помилок, необхідне врахування актуального історичного досвіду підготовки військових фахівців РІС. До цього часу системний аналіз історії розвитку підготовки військових фахівців РІС (у тому числі фахівців у галузі інформаційної безпеки) для ЗС України та інших відомств не проводився.

На основі пошуку, аналізу і узагальнення історіографії, історичних джерел та наукової літератури у галузі військової освіти проведено дослідження становлення та розвиток системи підготовки військових фахівців РІС тактичного рівня для Збройних Сил України (1991-2012 рр.), виявлення передумов, тенденцій, характерних рис та особливостей цього процесу, узагальнено актуальний досвід підготовки фахівців РІС.

В доповіді пропонується основні результати систематизації історії розвитку підготовки фахівців РІС на основі прийнятої періодизації реформування та розвитку єдиної системи військової

освіти в Україні, в контексті порівняльного аналізу з системами підготовки фахівців у провідних країнах світу. Зокрема пропонується наступна періодизація:

- створення системи підготовки військових фахівців РІС тактичного рівня (ТР) в ході першого періоду реформи системи військової освіти (СВО) в Україні (1991-1996 рр.);

- становлення системи підготовки військових фахівців РІС ТР в ході другого періоду реформи СВО в Україні (1997-2001 рр.);

- розвиток системи підготовки військових фахівців РІС у базових вищих військових навчальних закладах (ВВНЗ) Міністерства оборони України та інших відомств (2002-2012 рр.).

В ході проведеного аналіз розвитку традицій комплексної системи підготовки військових фахівців у визначених ВВНЗ, як вирішальної умови забезпечення кваліфікаційних вимог фахівців РІС, визначена сутність комплексування підготовки військових фахівців у ВВНЗ на організаційному рівні та рівні змісту навчання в контексті удосконалення їх підготовки.

При проведенні аналізу комплексування підготовки військових фахівців РІС розглядалось:

а) на організаційному рівні шляхом:

- формування безперервної системи підготовки фахівців РІС на тактичному і оперативно-тактичному рівнях (визначення раціональної мережі ВВНЗ єдиної системи військової освіти (Міністерства оборони України та інших військових формувань (ІВФ);

- формування системи безперервної підготовки фахівців РІС для Міністерства оборони України та ІВФ, іноземних військових фахівців (за спільними спеціальностями) в окремих ВВНЗ (утворення навчального комплексу з підготовки, перепідготовки та підвищення кваліфікації військових фахівців, у т.ч. з активним використанням навчально-матеріальної бази (НМБ) бойової підготовки військ);

- поєднання підготовки на спільній базі окремого ВВНЗ військових фахівців кадру і запасу (за спільними військово-обліковими спеціальностями) та цивільних фахівців (за спільними напрямами та спорідненими спеціальностями).

б) на рівні змісту навчання шляхом:

- зосередження в окремому ВВНЗ спеціальностей та спеціалізацій підготовки військових фахівців певної спрямованості, зокрема РІС (оптимізації замовлення на їх підготовку);

- узгодження нормативних складових змісту освіти споріднених напрямів (спеціальностей) та відповідних навчальних планів за змістом і часом для оптимізації лекційних потоків курсантів (слухачів, студентів), диференціації лабораторних та практичних занять для окремих спеціалізацій в межах спільного лекційного потоку спеціальності (споріднених спеціальностей);

- диференціацію підготовки фахівців для Міністерства оборони України та ІВФ в межах спеціалізації шляхом індивідуалізації навчання, наукової роботи, системи курсових, кваліфікаційних робіт та ін.;

- узгодження окремих елементів практичної підготовки на спільній НМБ різних категорій навчаємих, у т.ч. проведення з ними спільних комплексних практичних занять (тренувань, навчань) з відповідним розподілом функціональних завдань для економії ресурсу ОіВТ, інших витрат;

- формування системи комплексних навчальних курсів, удосконалення структури і змісту нормативних дисциплін і використання їх для спеціальної підготовки військових фахівців тощо.

Література

1. Нещадим М. І. Військова освіта України: історія, теорія, методологія, практика : монографія / М. І. Нещадим. – К. : Видавничо-поліграфічний центр "Київський університет", 2003. – 852 с.

2. Супрунов Ю. М. Історичні передумови розвитку комплексної системи підготовки військових фахівців у Житомирському військовому інституті імені С. П. Корольова. / Ю. М. Супрунов – Труди університету : зб. наук. праць. – К. : НУОУ. – №4 (131). – 2015. – 240 с. С. 226 – 237.

3. Директива Міністра оборони України від 22.01.92 № Д-5 “Про розвиток військової освіти в умовах реформування Збройних Сил України”. ГДАМО України: Фонд Адміністрації Міністерства оборони України.

4. Наказ Міністра оборони України від 25.07.92 № 133 “Про реформування системи військової освіти в Україні” // Галузевий державний архів Міністерства оборони України (ГДА МОУ), м. Київ.

5. Про створення єдиної системи військової освіти: постанова Кабінету Міністрів України від 15.12.97 № 1410 [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/1410-97-п.

УДК 791.44.02

Фриз В. П.
кандидат технічних наук, доцент
Житомирський військовий інститут імені С.П. Корольова

ПІДГОТОВКА ФАХІВЦІВ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ОСНОВІ ІГРОВИХ МЕТОДІВ НАВЧАННЯ

Постійний розвиток інформаційних технологій, вимагає здійснювати ефективну підготовку фахівців які використовують інформаційно-комп'ютерні системи для ведення спеціальних дій. Тому якісна підготовка таких військових фахівців є актуальною задачею.

Як показує досвід проведення занять на випускний кафедрі, традиційні форми навчання такі як лекції, семінари, практичні та лабораторні заняття, для курсантів 4-5 курсів виявляються малоефективними. Тому одним із перспективних шляхів для вирішення цього питання є використання ігрового методу навчання.

По своєму змісту ігровий метод навчання це моделювання ситуації яка виникає в реальності при виконанні функціональних завдань за призначенням, причому ситуації як правило проблемній. Гра являє собою сукупність заходів, в ході яких групі курсантів пропонується вирішить певну ігрову задачу, яка відображає реальні ситуації в застосуванні підрозділу за функціональним призначенням.

Методика проведення заняття полягає у поділі навчальної групи на дві команди, в кожній з яких призначається старший, а особовий склад розподіляється за умовними посадами. Сценарій проведення заняття розробляється заздалегідь, в ньому визначаються правила та умови гри, критерії оцінювання.

Перевагами проведення ігрового заняття є активізація діяльності кожного військовослужбовця, його зацікавлення в умовній перемозі своєї команди, спонукання до прояву не шаблонного, а творчого підходу у вирішенні поставлених завдань. Під час гри відбувається швидке поповнення знань до необхідного рівня, практичне засвоєння навичок та прийняття рішення в умовах реальної взаємодії з партнерами.

Література

1. Гра як метод навчання. Значення педагогічної гри. [Електронний ресурс]. – Режим доступу : http://geografica.net.ua/publ/metodichni_materiali/metodichni_materiali/gra_jak_metod_navchannja_znachennja_pedagogichnoji_gri/8-1-0-239.

2. Ягупов В.В. Педагогіка – Ігрові методи навчання. Ділові ігри. [Електронний ресурс]. – Режим доступу : http://eduknigi.com/ped_view.php?id=198.

ІНФОРМАЦІЙНА БЕЗПЕКА ОЧИМА МОЛОДИХ ВЧЕНИХ

УДК 342.95

Бондар І. Г.
Національна академія СБ України

ДЕЯКІ ПИТАННЯ УДОСКОНАЛЕННЯ ПРАВОВОЇ РЕГЛАМЕНТАЦІЇ ЕЛЕКТРОННОГО УРЯДУВАННЯ В УКРАЇНІ

З часу Євромайдану та зміни влади в 2014 році політики та офіційні особи часто наголошують на пріоритетності розбудови в Україні електронного урядування. Спробуємо зрозуміти, чому ж виник такий ажіотаж навколо інноваційного способу державного управління.

Розвиток молодої української держави, особливо в умовах політичної, економічної та воєнної нестабільності, вимагає використання нових форм державного управління, які б з однієї сторони задовольняли потреби випереджаючого розвитку суспільства, а з іншої – могли бути реалізовані за сучасних реалій. Необхідність змін зумовлена нагальною потребою реформування державного управління у зв’язку із наявністю таких проблем:

Непрозорість, закритість діяльності органів державної влади;

Відсутність довіри громадян до інститутів та посадовців державної влади та місцевого самоврядування;

Високий рівень корупції;

Надмірний бюрократизм;

Низька якість державних послуг;

Відірваність суспільства від державних рішень;

Відсутність контролю суспільства, популізм влади.

Досвід розвинених країн світу свідчить, що одним з ефективних засобів боротьби із переліченими суспільними явищами є запровадження електронного урядування – форми організації державного управління, за якої відбувається активна взаємодія органів державної влади та органів місцевого самоврядування між собою, з суспільством, людиною та бізнесом за допомогою інформаційно-комунікаційних технологій [1].

Дійсно, запровадження функціонування електронного урядування є запорукою нормального функціонування державного апарату сьогодення. Воно здатне змінити саму природу влади, забезпечуючи прозорість її діяльності. Запровадження та використання технологій електронного урядування є вагомим фактором підвищення національної конкурентоспроможності сучасної держави, що сприяє прискореним темпам економічного зростання та поліпшує структуру національної економіки. Крім того, ця система забезпечить реальну участь громадян у політичних процесах держави, зробить владу підконтрольною громадськості. Враховуючи результати реалізації пілотних проектів електронного урядування в окремих відомствах, можемо говорити про позитивні показники щодо взаємозв'язку та двосторонньої взаємодії між громадянином та державою, що є основою в формуванні громадянського суспільства. Проте, Україна посідає лише 87 місце серед 193 країн-членів Організації Об'єднаних Націй за результатами міжнародної оцінки розвитку електронного урядування «United Nations E-Government Survey 2014. E-Government For The Future We Want» (станом на 2014 рік, оцінка проводиться раз на два роки) [2].

Такий низький показник зумовлений низкою різних причин серед яких звісно ж ще кілька років тому першість займало недостатнє фінансування зазначеного сегменту. Попри це, на сьогодні існує ряд волонтерських організацій та інвесторських фондів (iGov, e-progress та ін.), які успішно займаються розвитком електронного урядування в Україні та надають відповідну інтелектуальну та фінансову допомогу. У контексті сьогодення, на нашу думку, на перший план серед проблем розбудови електронного урядування в Україні вийшла правова площина даного питання.

Вітчизняна нормативно-правова база електронного урядування включає в себе низку законів, Укази Президента України, розпорядження та постанови Кабінету Міністрів України, а також галузеві нормативні документи, підготовлені Адміністрацією Державної служби спеціального зв'язку та захисту інформації України, Державним комітетом України з питань технічного регулювання та споживчої політики.

Але на законодавчому рівні чітко не визначено режими функціонування електронного урядування, критерії переходу електронного урядування з одного режиму в інший, не визначені стандарти, яким повинна відповідати національна електронна систе-

ма. Тому значна кількість чинних законодавчих і нормативно-правових актів, що регулюють відносини у сфері інформаційних технологій, потребують внесення відповідних змін та доповнень.

Насьогодні усі ці питання залишаються складними, певною мірою корупційними та вимагають багато часу, зусиль і ресурсів. Це зменшує ефективність, результативність та гнучкість управління державними електронними ресурсами. Як результат, в органах влади та державних установах впроваджена значна кількість комплексних інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, у тому числі державних реєстрів, систем відомчого електронного документообігу, автоматизації типової діяльності та систем підтримки прийняття управлінських рішень, які не сумісні між собою, використовують різні технології, стандарти та формати. Відповідні явища не приноситимуть очікуваної ефективності роботи електронного урядування [3].

Проаналізувавши стан нормативно-правової бази України з питань електронного урядування можемо виділити такі рекомендації щодо її поліпшення:

Законодавче закріплення алгоритма отримання громадянами державних послуг в електронному режимі.

Розробка та прийняття проекту Закону України «Про електронну ідентифікацію».

Затвердження програми "Електронна Україна" та Положення про Національний реєстр електронних інформаційних ресурсів.

Нормативне закріплення залучення громадськості до ухвалення публічно-правових рішень на рівні органів державної влади і місцевого самоврядування у досліджуваній сфері.

Визначення на законодавчому рівні питання фінансування реалізації національного Плану дій та заходів, а також регіональних програм впровадження ініціативи «Відкритий уряд».

Забезпечення виконання положень нормативно-правової бази щодо інструментів електронної персоналізації та застосування «електронного підпису».

Визначення ієрархії державних органів у сфері електронного урядування та визначення єдиного координаційного центру.

В подальшому, основним напрямом наукових досліджень електронного урядування в Україні повинно стати удосконалення правової регламентації алгоритму отримання громадянами державних послуг електронно у реальному масштабі часу, регламен-

тації порядку звернення, стандартизації форм документів, запитів і відповідей такого режиму. Також законодавчо треба визначити права й обов'язки користувачів єдиного порталу, характер інформації в інформаційній базі системи, відповідальність сторін стосовно роботи з інформацією, а також правовий статус документів у системі.

Література

1. Розпорядження Кабінету Міністрів України від 13 грудня 2010 року № 2250-р «Про схвалення Концепції розвитку електронного урядування в Україні» [Електронний ресурс]. - Режим доступу : http://zakon3.rada.gov.ua/laws/show/2250-2010-р.

2. Hongbo W. United Nations E-Government Survey 2014. E-Government For The Future We Want / W.Hongbo. – Нью-Йорк : United Nations, 2014. – 284 с.

3. Концептуальні засади розвитку електронного урядування в Україні : навч. посібн. / [О.А. Баранов, М.С. Демкова, С.В. Дзюба та ін.]. – 2009. – 82 с.

УДК 341.1:342.6 (043)

Бондаренко І .Д.
Національна академія СБ України

КРИМІНАЛЬНО-ПРАВОВА ХАРАКТЕРИСТИКА ДІЯНЬ ІЗ НЕСАНКЦІОНОВАНОГО ЗБУТУ ТА РОЗПОВСЮДЖЕННЯ «КОМП'ЮТЕРНОЇ» ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ (СТ. 361-2 КК УКРАЇНИ)

Кримінально-правові засоби є важливою складовою системи захисту інформації з обмеженим доступом. Однією із статей КК України, що встановлює відповідальність за порушення конфіденційності такої інформації є ст. 361-2, в якій криміналізовано несанкціонований збут або розповсюдження інформації з обмеженим доступом, яка зберігається в формі комп'ютерних даних та є захищеною. Водночас, питання встановлення сутності цих діянь, їх співвідношення між собою, а так само – визначення моменту закінчення аналізованого злочину є ускладненими з огляду на неоднозначне розуміння кримінально-правового значення понять

«інформація» та «комп'ютерні дані», що зумовлене розбіжністю моментів отримання електронного носія/файлу та сприйняття інформації, неможливістю такого сприйняття без використання посередника, – засобів комп'ютерної техніки. Крім того, на сучасному етапі розвитку технологій та глобалізації інформаційного простору стрімко набувають поширення нові форми діянь, які посягають на конфіденційність інформації з обмеженим доступом, зокрема, її анонімне пересилання з використанням комунікаційних сервісів мережі Інтернет, а також розміщення в публічному доступі, що призводить до швидкого та неконтрольованого розповсюдження інформації. Все це свідчить про необхідність переосмислення традиційного кримінально-правового розуміння діянь, що посягають на конфіденційність інформації, зокрема і злочину, передбаченого ст. 361-2 КК України.

Використовуючи в диспозиції ст. 361-2 КК України для позначення суспільно-небезпечного діяння два терміни «збут» та «розповсюдження», законодавець фактично протиставляє їх, але вивчення існуючих наукових дефініцій зазначених понять відображає проблематичність їх розмежування. Так, можна виділити три критерії, за якими ці терміни відповідно до окремих тлумачень повністю корелюють. Перший критерій – оплатність: і збут, і розповсюдження науковці часто розглядають як такі, що можуть здійснюватися в оплатній або безоплатній формі. Крім того, поняття «незаконний збут» розкривається в Постанові Пленуму Верховного суду України від 26.04.2002р. № 4, де зазначено, що ним є «...будь-які оплатні чи безоплатні форми їх реалізації…» [1]. Другий критерій – кількість отримувачів інформації: і збут, і розповсюдження як правило розглядають як такі, що можуть передбачати передачу інформації як одній, так і багатьом особам. Третій критерій – спосіб поширення інформації: і збут, і розповсюдження переважно розглядаються як такі, що можуть передбачати особисту передачу інформації «із рук в руки» на матеріальному носії або її передачу шляхом надання доступу, зокрема, через мережу Інтернет. З наведеного можна зробити висновок, що проблематичність чіткого розмежування несанкціонованого «збуту» та «розповсюдження» обумовлена тим, що ці поняття не позначають два окремі, самостійні діяння, а співвідносяться між собою як частина та ціле. Аналогічного висновку дійшов і О.О. Кирбят'єв, зазначаючи «збут охоплюється розповсюдженням», та

В.І. Тарабановська, яка вказувала на «факт розповсюдження, зокрема, продажу…» [2, с. 8; 3, с. 77]. Розповсюдження є поняттям найширшим за змістом. Аналіз судової практики за ст. 361-2 КК України дозволяє виділити дві окремі форми такого розповсюдження, які суттєво відрізняються, зокрема, щодо моменту закінчення злочину. Їх пропонується викласти в тексті статті наступним чином: 1) адресна передача інформації сторонній особі (оплатно і безоплатно) 2) розміщення інформації в публічному доступі, за якого такий доступ до неї може отримати абстрактне, невизначене коло осіб. Спільним для обох форм є те, що стороння особа (особи) може як очікувати отримання інформації, так і набути її без попередньої домовленості. У випадку розміщення в публічному доступі очікуваність може мати місце, коли таке розміщення анонсується заздалегідь. При адресній передачі інформації з обмеженим доступом умисел злочинця (адресанта) направлений на її надання конкретній, заздалегідь визначеній сторонній особі (адресату) або групі осіб (адресатам), кількісний склад якої контрольований та чітко сприйнятий адресантом. Факт знайомства адресанта з адресатом на кваліфікацію не впливають: передача, інформації, її оплата можуть взагалі здійснюватися безконтактно та анонімно. Розповсюдження інформації шляхом її розміщення в публічному доступі передбачає неможливість оплатності, адресантом не створюється застережень для її отримання. Відсутня ознака адресності – умисел винного направлений не на передачу інформації конкретній, наперед визначеній особі, а абстрактному, неконтрольованому адресантом колу осіб – внаслідок такого розміщення отримати доступ до інформації може будь-хто. Винний усвідомлює, що розміщувана ним інформаціє не є загальнодоступною та бажає передати її особам, яким вона раніше не була відома. Інформація могла бути попередньо отримана адресантом як з «непублічного» джерела (наприклад, від спеціального суб’єкта) або з «публічного» та загальнодоступного. Аналіз судової практики за ст. 361-2 КК України свідчить, що навіть якщо таке джерело інформації було «публічним» (наприклад, «встановлений досудовим слідством сайт») суд так само визнавав діяння із її розповсюдження злочином [4]. Але в цьому контексті видається правильною думка, що розміщення інформації в публічному доступі, яка попередньо вже була отримана з «публічного джерела», має вважатися злочинним лише якщо спосіб її розмі-

щення із абсолютною очевидністю передбачає суттєве збільшення кількості потенційних адресатів. Так, наприклад, видається правильним кваліфікувати за ст. 361-2 КК України дії журналіста, який під час сюжету, що транслювався по одному із провідних національних телеканалів у прайм-тайм, продемонстрував та зачитав текст документів, що мають гриф «таємно», які попередньо були розміщені на сайті так-званого «файлообмінника» невстановленою особою. З іншої сторони, видається помилковим розглядати як «розміщення» в публічному доступі, дії особи, яка побачивши у стрічці новин соціальної мережі репост (посилання) на вже неодноразово переглянутий та коментований запис іншого користувача, до якого було прикріплено фотографію документа з грифом «таємно», робить посилання на цей запис на своїй персональній сторінці соціальної мережі, тим самим надаючи до запису доступ додатковому колу осіб.

Тлумачення моменту закінчення злочину, передбаченого ст. 361-2 КК України, за аналогією з розголошенням державної таємниці, тобто з моменту усвідомлення змісту інформації сторонньою особою, видається помилковим, оскільки, в такому випадку, залишається поза увагою важливий аспект – адресат може відкласти ознайомлення зі змістом інформації у файлі (власне як і на некомп'ютерному носії) на невизначений строк, взагалі не ознайомлюватись з інформацією, але передати носій чи сам файл іншій сторонній особі або розмістити його в публічному доступі. Таку ситуацію, коли адресат отримав носій/файл або інформацію було розміщено в публічному доступі, але ознайомлення зі змістом інформації ще не відбулося, пропонується позначати як «стан перманентної загрози конфіденційності», який є аномальним для встановленого режиму обігу такої інформації, а отже вже є свідченням порушення режиму її захищеності. Саме із виникненням цього стану необхідно пов'язувати момент закінчення аналізованого злочину. У випадку адресної передачі інформації він виникає в результаті надання носія/файлу, коли адресат отримує реальну можливість його передачі третій особі та/або ознайомлення з інформацією. Можливість є реальною, якщо активні дії, які мають бути вжиті з боку адресата щоб розпорядитись отриманою інформацією, є звичайними для відповідних способів її надання, наприклад, такими є завантаження через під'єднаний до Інтернету комп'ютер з сайту електронної пошти надісланого файлу та

його відкриття стандартною офісною програмою. Коли ж інформація передається шляхом розповіді або демонстрації – момент закінчення злочину обумовлюється можливістю відтворення сприйнятої адресатом інформації незалежно від усвідомлення її змісту, оскільки сам факт запам’ятовування дозволяє в подальшому її передати третім особам. Момент закінчення аналізованого злочину у формі розміщення інформації в публічному доступі пов'язаний із виникненням потенційної можливості ознайомлення з нею, копіювання, запам’ятовування (із здатністю до подальшого відтворення) невизначеним, неконтрольованим колом осіб в результаті її публічної розповіді/демонстрації чи передачі умовному посереднику (наприклад, сайт мережі Інтернет), що забезпечує її загальнодоступність, а також пряму/опосередковану пропозицію ознайомлення/копіювання.

Література

1. Про судову практику в справах про злочини у сфері обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів: Постанова Пленуму Верховного суду України від 26 квітня 2002 р. № 4 – [Електронний ресурс]. – Режим доступу: http://www.zakon.rada.gov.ua

2. Кирбят'єв, Олег Олександрович. Кримінальна відповідальність за створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут [Текст] : автореф. дис. ... канд. юрид. наук : 12.00.08 / Кирбят'єв Олег Олександрович ; Класич. приват. ун-т. – Запоріжжя, 2015. – 20 с.

3. Тарабановська В. І. Основи методики розслідування злочинів, пов’язаних з незаконним тиражуванням та розповсюдженням аудіовідеопродукції : дис. канд. юр. наук : 12.00.09 / Тарабановська Валерія Ігорівна – Київ, 2012. – 232 с.

4. Ухвала Броварського міськрайонного суду Київської області від 07.08.2013р. (Справа № 361/6538/13-к Провадження № 1-кп/361/335/13) – [Електронний ресурс]. – Режим доступу: // http://reyestr.court.gov.ua/

УДК 32.019.51

Верголяс О. О.
Національна академія СБ України

ІНФОРМАЦІЙНА ЛОГІСТИКА ЯК ЕЛЕМЕНТ ПСИХОЛОГІЧНОЇ ХАРАКТЕРИСТИКИ ЦІЛЬОВОЇ АУДИТОРІЇ СПЕЦІАЛЬНОЇ ІНФОРМАЦІЙНОЇ ОПЕРАЦІЇ

Для досягнення максимальної ефективності спеціальної інформаційної операцій, окрім інших характеристик цільової аудиторії СІО, необхідно визначити інформаційну логістику (джерела отримання та поширення інформації) цільової аудиторії.

Спеціальні інформаційні операції – це сплановані дії, спрямовані на ворожу, дружню або нейтральну аудиторію шляхом впливу на її свідомість і поведінку за допомогою використання певним чином організованої інформації та інформаційних технологій для досягнення певної мети [1].

1. Джерела отримання інформації. Телебачення, радіо, газети, журнали, сайти, групи та сторінки у соціальних мережах. Важливо не тільки визначити пропорції співвідношення споживання інформації з тих чи інших джерел, але й визначити конкретний перелік найбільш популярних серед представників цільової аудиторії засобів масової інформації, лідерів суспільної думки, інтернет-сайтів, сторінок та груп у соціальних мережах. Окрім зазначеного варто детально проаналізувати не тільки наявність чи відсутність тих чи інших джерел в «інформаційному раціоні» споживача, але й дати характеристику джерелам, а саме тематиці джерел (політика, спорт, мода), ідеологічному забарвленню (ліберальні, нейтральні, центристські тощо), формату інформації (комікси, випуски новин на телебаченні чи радіо, записи у соціальних мережах лідерів суспільної думки тощо).

Визначивши перелік джерел отримання інформації цільовою аудиторією, організатори можуть виокримити вибір інформаційних ресурсів, лідерів суспільної думки, адміністраторів сайтів, сторінок та груп у соціальних мережах, які необхідно взяти під контроль чи (та) залучити до СІО. Відбір найбільш авторитетних та найбільш відвідуваних джерел інформації збільшить ефективність інформаційно-психологічного впливу через охоплення ширшої аудиторії та довіри до інформаційних матеріалів, що розроблені організаторами СІО.

Особливо важливо чітко визначити джерела отримання інформації цільовою аудиторією у випадку інформаційно-психологічної війни, коли представники цільової аудиторії усвідомлюють наявність інформаційного протиборства і уважно ставляться як до самої інформації так і до джерел отримання інформації а органи державної влади та спецслужби перешкоджають спробам отримати контроль чи (та) залучити до СІО лідерів суспільної думки, адміністраторів сайтів, сторінок та груп у соціальних мережах тощо. В такому випадку необхідно провести заходи або із залучення до проведення СІО наявних представників цільової аудиторії або проникнення власного агенту впливу під виглядом представника цільової аудиторії з метою їх використання і як джерела отримання інформації і як джерела поширення інформації в середині цільової аудиторії.

2. Джерела поширення інформації в середині цільової аудиторії. Означає визначення кола осіб, які є «генераторами», «передавачами» та безпосередньо «споживачами» інформації, а також основні майданчики, де циркулює інформація (сторінки та групи в соцмережах і на форумах, місця громадського харчування, паління, тощо).

Використовуючи зазначені місця можна поширювати інформацію фактично оминаючи лідерів і передавачів та додатково охопити нецільову аудиторію. Загалом, такі інформаційні майданчики як форуми, сторінки та групи у соцмережах важливі та цікаві для організаторів СІО тим, що за певних умов (жорсткість модерації ресурсу, критичність чи «болючість» теми для користувачів ресурсу та інше) на таких майданчиках доволі легко підтримувати на належному рівні циркуляцію та поширення інформаційних матеріалів, просто залишаючи коментарі у темі чи дописі для повторного привернення до матеріалу уваги.

Не зважаючи на те, що саме явище інтернет-форумів є відносно давнім, такі інформаційні майданчики, попри поширення та розвиток соцмереж, і досі користуються попитом серед користувачів мережі Інтернет. Відповідно, при аналізі інформаційної логістики цільової аудиторії на предмет джерел поширення інформації в середині цільової аудиторії необхідно приділити достатньо уваги і таким, на перший погляд застарілим, інформаційним майданчикам.

Джерела отримання та поширення інформації всередині цільової аудиторії можуть перетинатись між собою та дублювати один одного. Завдання організаторів на підготовчому етапі СІО полягає у визначенні таких джерел для оптимізації використання сил та ресурсів при здійсненні ІПВ на цільову аудиторію. Окрім цього, це дозволить автономізувати поширення інформації серед споживачів інформації, тим самим мінімізуючи як витрати сил та ресурсів, так і ризики викриття спроб ІПВ з боку суб'єкту СІО.

Література

1. Галамба М. Сутність, види та методи спеціальних інформаційних операцій [Електронний ресурс] / Микола Галамба // Юридичний журнал – Режим доступу до ресурсу: http://www.justinian.com.ua/magazine.php?id=79.

УДК 005.3

Головко О. М.
Науково-дослідний інститут інформатики і права
Національної академії правових наук України

ДЕСТРУКТИВНІ МЕДІАВПЛИВИ: ДО ПИТАННЯ КРИМІНАЛІЗАЦІЇ

Інформаційні потоки суттєво перевищили спроможність їх адекватного опрацювання, що приведе до масового переходу від аналітичного до феноменологічного сприйняття дійсності, суттєво посилюючи ймовірність ірраціональних реакцій, поширення панічних настроїв тощо [2, с. 41].

Впливовість віртуального простору лише набирає обертів, хоча й здається, що він заполонив більшу частину добового часу людини. У зв'язку з цим набули особливої актуальності питання тайм-менеджменту, інформаційної культури, здатності правильно споживати відомості, котрі ми отримаємо з інформаційного простору інколи навіть без суб'єктивної на те волі людини (радіо у транспорті, реклама по телебаченню, перенасичення надмірно емоційним новинним контентом). У такій ситуації левову частину інформаційного простору бере на себе медіапростір, який може виступати не тільки посередником, а й реальним гравцем суспільно-політичної обстановки.

В першу чергу, йдеться про зовнішнє деструктивне втручання та вплив на людську свідомість, а отже й на психіку. Зокрема, варто звернути увагу на взаємодію з представниками найбільш проблемних груп у суспільстві, а отже й найбільш уразливих до інформаційної деструкції, особливо маніпулятивного характеру. Зокрема, ідеться про представників національних меншин, деяких соціальних груп, населення окремих регіонів і територій [2, с. 93].

На прикладі зі східноукраїнськими регіонами завжди відомим фактом було те, як болісно місцеве населення сприймає мовне питання. Достатньо було лише іскри, щоб на цьому ґрунті спалахнуло ціле полум'я ненависті й ворожнечі. Завданням держави в цьому випадку мало бути: 1) недопущення радикальних висловів з цього приводу; 2) демонстрація толерантності та компромісу всіх сторін політичного процесу, а не тільки безапеляційно ворожих виступів радикальних рухів; 3) робота з населенням по упередженню тиску зовнішніх агентів на ці больові точки. Нажаль, у даному аспекті медіа виступили інструментом поглиблення «мови ворожнечі», вивільнення агресії та виправдання її «благими» мотивами.

Зауважимо, що у вищеописаній ситуації внутрішня загроза деструктивного медіавпливу чомусь досі залишається поза меншою політико-правовою увагою, аніж зовнішня. Однак, некомпетентність медіавиробника, недотримання журналістських стандартів, виправдання так званої «мови ворожнечі» національним інтересом також завдає колосальної шкоди психологічному стану людини, її адекватному світосприйняттю через призму численних висновків у ЗМІ, а не власного досвіду чи аналітичних вмінь.

Якщо нестійкі до медіавпливів верстви населення є тим сегментом аудиторії ЗМК, які потребують додаткового інформування про можливі інформаційно-психологічні небезпеки та загрози, то для суб'єкта впливу вони стають цільовою аудиторією, особливо це стосується осіб, котрі мають медіа аддикції, стали об'єктом інформаційної віктимізації. Окремого дослідження також потребують особи, котрі в результаті деструктивних впливів набули негативного роду девіацій.

Як засвідчили події 2014 р. в Україні, використання внутрішніх кризових ситуацій для інтенсифікації негативного інформаційного впливу становить серйозну проблему, що посилюється

неучастю вітчизняних ЗМІ у формуванні державницької громадської думки [2, с. 40]. Таким чином, у кризових ситуаціях уразливість та незахищеність психіки щодо отриманої інформації набуває загальнонаціонального, а в деяких випадках навіть світового масштабу. Власне в такому разі людина, як правило, починає споживати будь-які відомості дуже емоційно, вірячи в кардинально різкі сюжети розвитку подій. При цьому до медіаджерел особа звертається з більшою довірою, ніж у буденні дні, вважаючи їх ретранслятором реальності. Ось тут і ховається пастка для пасивного медіаспоживачів, якими досі залишається більшість населення нашої держави. Внаслідок цього пересічна людина, котра не має навіть базових навичок сприйняття повідомлень з медіапростору просто втрачає розуміння сприйнятих численних подій які в кожному ЗМІ подано по різному.

Так, з одного боку, це і є керівна ідея плюралізму думок та свободи слова, а з іншого – це автоматично може бути використано зловмисниками для введення людей в оману та формування громадської думки на підставі неповних, викривлених чи навіть маніпулятивних відомостей. Ключовим вирішенням такої колосальної проблеми вбачаємо опрацювання та реалізацію комплексу превентивних заходів, покладених на підвищення інформаційної культури населення, особливо в кризових та буферних регіонах.

Тому важко не погодитись з Савінової Н.А., яка зазначає, що говорячи про кримінально-правову норму і закон про кримінальну відповідальність загалом, ми спочатку визначаємо їх первинну охоронну функцію, і лише після цього – регулятивну і превентивну [1, с. 137]. У випадку з медіавпливами робота першочергово має бути спрямована на попередження даних проявів. Специфіка полягає у складності визначення суб’єктного складу та доведення вини, хоч медіавпливи й мають конкретну мету (економічну, політичну, ідеологічну тощо). Однак потерпання людини від цинічного та відкритого втручання у психічні процеси її свідомості не мають залишатися безкарними.

Підсумовуюче сказане, існує потреба у розробці конкретних практичних механізмів по збереженню цілісності та стійкості людської свідомості від інформаційно-психологічних, особливо медіа небезпек, загроз та впливів. Не останню роль у цьому має відігравати пропагування ідеї медіаграмотного населення, здат-

ного хоча б на побутовому рівні відрізняти дезінформацію, маніпуляції та інформаційні провокації. Що ж стосується небезпек та загроз вище даного рівня – держава має їх перехоплювати та попереджати на тій стадії, доки вони ще не завдали непоправної шкоди людині як представнику масового медіаспоживання, суспільству та національним соціально-політичним процесам. Механізмом реалізації цього є криміналізація конкретних випадків медіавпливу.

Література

1. Савінова Н.А. Кримінально-правова комунікація у дискурсі ефективності кримінально-правового регулювання / Н.А.Савінова // Право України. – 2015. – №9. – 136-141 с.

2. Системна криза в Україні: передумови, ризики, шляхи подолання : аналіт. доп. / Я. А. Жаліло, К. А. Кононенко, В. М. Яблонський [та ін.]; за заг. ред. Я.А. Жаліла. – К. : НІСД, 2014. – 132 с.

УДК 316.485.6:351.746.1(477)

Давиденко М. О.
Національна академія СБ України

ПОШИРЕННЯ РЕЛІГІЙНОГО ЕКСТРЕМІЗМУ В УМОВАХ РОСІЙСЬКОЇ ІНФОРМАЦІЙНОЇ АГРЕСІЇ: АСПЕКТИ ПРОТИДІЇ

На сучасному етапі внутрішня нестабільність в Україні може бути спричинена ускладненням та радикалізацією релігійного чинника, в тому числі і під впливом зовнішніх факторів, таких як інформаційна війна з боку суміжних держав, пряма підтримка антиукраїнських сил та рухів, що виступають під гаслами порушення існуючої територіальної цілісності України або завдання іншої шкоди її національним інтересам.

Так, протягом окупації Автономної Республіки Крим військами Російської Федерації (далі - РФ), розгортання і ескалації військового конфлікту на Сході України, активізації сепаратистських ідей в Придністров'ї та Закарпатті, одним із основних чинників почав виступати релігійний фактор.

Для досягнення своїх геополітичних інтересів Російська Федерація ще початку 2014 року розпочала реалізацію в Україні проекту *«Русская весна 2.0 – возрождение Новороссии»* (першою «Русской весной» в РФ вважається захоплення Криму). До зазначеного проекту, розробленого т.зв. «мозковими центрами» та за участі спецслужб РФ і ЗМІ, планувалось залучення російськомовних громадян південно-східних регіонів України, прихильників попередньої влади, віруючих «канонічної церкви» та членів навколоцерковних організацій.

Одним із інструментів проведення проекту «Русская весна» та впровадження доктрини «Русского мира» на тимчасово окупованих територіях стало поширенням інформації в низці друкованих ЗМІ, мережі Інтернет, на телебаченні, що популяризує діяльність Руської православної церкви (далі-РПЦ), закликів щодо підтримки незаконних збройних формувань «Руської православної армії», а в окремих випадках щодо доцільності перебування на теренах т.зв. «ДНР» та «ЛНР» священнослужителів, які начебто вороже налаштовані проти РПЦ, а саме УПЦ КП та УГКЦ. Саме цікаве, що інформаційна стратегія РФ налаштована на те, щоб виховати у населення відношення до священнослужителів, які підтримують РПЦ, сепаратистів та представників незаконних збройних формувань, як таких, що «захищають і визволяють» Україну.

Так, на початку окупації Криму Патріарх Московський Кирил офіційно заявив, що політична діяльність однієї з трьох найбільших в Україні Церков - Української Греко-Католицької Церкви проходить під «русофобськими гаслами» та в останні місяці кинула «глибоку тінь» на відносини між Російською православною церквою і Ватиканом [1].

А глави і представники традиційних релігійних громад Росії 3 квітня 2014 року спеціальній заяві «висловили глибоку заклопотаність у зв'язку з подіями, що відбуваються в Україні». Міжрелігійна рада Росії говорить про важливість збереження загального культурного, духовного простору і приписує Україні «утиски деяких релігійно-громадських діячів, загрози нормальному функціонуванню монастирів, храмів, мечетей і синагог» [2]. Водночас одним з лідерів ЛНР Стрілковим-Гіркіним була здійснена спроба створити т.зв. *«Православний центр ополчения»* у м. Луганськ.

Як показує практика,інформаційна пропаганда РФ діє досить ефективно, оскільки на Донбасі духовну підтримку озброєним повстанцям продовжують надавати окремі священики УПЦ. На Великдень біля будівлі управління СБУ в Луганській області, зайнятого озброєними проросійськими активістами, настоятель храму Святих Гурія, Самона і Авіва УПЦ протоєрей Павло Батарчуков очолив хресний хід. Під час хресного ходу отець Павло окропив святою водою повстанців та бійців «ДНР» на барикадах в ім'я «упокорення пристрастей і зміцнення духу в ім'я миру, побажавши їм стійкості і мужності» [3].

Крім того, архиєпископ Луганський і Альчевський УПЦ Митрофан (Юрчук) висловив погляд, що Київ повинен прислухатися до голосу людей Південно-Східного регіону і не має права ігнорувати результати референдуму про державну самостійність Луганської народної Республіки [4].

Як результат «визвольної політики» у Криму та на Сході України сепаратисти та священики Московського патріархату почали інвентаризовувати майно, що належить представникам Київського патріархату, УГКЦ, почалися збройні захоплення храмів разом із бійцями «ДНР» та «ЛНР», побиття та вбивства священників, вчинення антисемітських акцій та вчинення інших кримінально-протиправний діянь на ґрунті расової, релігійної нетерпимості.

Таким чином, основними методами використання релігійного фактора в Україні можемо визначити проведення акцій інформативного впливу та спеціальних інформативних операцій, в яких звертається увага щодо негативної діяльності церков на Україні, поширення чуток і пліток про расову, релігійну чи національну нетерпимість, здійснюється інформативна пропаганда стосовно «православного тероризму», «Руської православної армії» тощо.

З іншого боку, на нашу думку, російські інформаційні «мозкові центри» не володіють реальною інформацією про стан справ у релігійній сфері України, в багатьох випадках видають бажане за дійсне та і в цілому не відрізняються новизною чи креативністю. У механізмах протидії інформаційній експансії РФ основні складові (оперативні та адміністративні) звичайно ж за правоохоронними органами. Разом з тим, у розвінчанні нав’язуваних міфів РПЦ, нівелювання їх впливу на суспільну думку вагоме слово мають сказати і релігієзнавці. Лише спільними зусиллями

правоохоронців, науковців, представників ЗМІ та інститутів громадянського суспільства вдасться здійснити «щеплення суспільства» від привнесених ззовні хвороб – «сепаратизм і тероризм» та релігійний екстремізм.

Література

1. Патріарх Кирил назвав «русофобською» діяльність УГКЦ / [Електронний ресурс] // Режим доступу : http: http://risu.org.ua/ua/index/all_news/community/religion_and_policy/56588/

2. Загроза нормальному функціонуванню монастирів / [Електронний ресурс] // Режим доступу : http: http://risu.org.ua/ua/index/all_news/orthodox/moscow_patriarchy/55979/

3. У Луганську священики УПЦ (МП) і УПЦ КП знаходяться по різні сторони барикад / [Електронний ресурс] // Режим доступу http: http://risu.org.ua/ua/index/all_news/community/religion_and_policy/56182/

4. Архиєпископ УПЦ (МП) заявив, що Київ має визнати референдум у Луганську / [Електронний ресурс] / Режим доступу http: http://risu.org.ua/ua/index/all_news/state/national_religious_question/56480

УДК 331.108

Іванчук Т. С.
Львівський державний університет безпеки життєдіяльності
Кухарська Н. П.
кандидат фізико-математичних наук, доцент
Львівський державний університет безпеки життєдіяльності

АНАЛІЗ ЗАГРОЗ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА З БОКУ ЙОГО ПЕРСОНАЛУ

В сучасних умовах господарювання, коли ситуація в країні в цілому та в економіці зокрема характеризується значною нестабільністю, підприємства піддаються постійним впливам різноманітних загроз. За статистикою зовнішні і внутрішні загрози економічній безпеці підприємства співвідносяться як 20 до 80. Тобто 4/5 усіх проблем породжуються внутрішнім середовищем компанії.

Розглянемо внутрішні загрози підприємства, джерелом яких є персонал.

1. Розкрадання майна підприємства (корпоративне шахрайство). Може проявлятися в трьох варіантах: дрібні разові розкра-

дання; постійні розкрадання у невеликих та середніх розмірах, які розглядаються крадієм як своєрідна «надбавка до зарплати»; розкрадання в особливо великих розмірах – організація «бізнесу в бізнесі».

2. Використання ресурсів підприємства (матеріальних, фінансових, технічних, транспортних та ін.) в особистих цілях. Найчастіше це явище має місце на підприємствах, де погано налагоджений контроль з боку керівників лінійних підрозділів за використанням їхніми підлеглими робочого часу.

3. Умисне псування і нищення майна підприємства (диверсія). Як показали дослідження CERT (Computer Emergency Response Team) серед корпоративних диверсантів є велика частка фахівців, які тим чи іншим чином пов'язані з інформаційними технологіями (IT). На технічно підкованих диверсантів припадає 87 % інцидентів, а саме: до 38 % таких інцидентів причетні системні адміністратори, до 21 % – програмісти, до 14 % – інженери і ще до 14 % – фахівці з IT. Аналітики також підрахували, що у 31 % випадку про плани та (або) діяльність диверсанта знали інші (колеги – у 64 % випадків, друзі – у 21 %, члени сім'ї – у 14 %). У 14 % диверсантів були спільники [1].

4. Отримання заробітної плати за невиконану роботу (саботаж). У класичному визначенні саботаж – це свідоме невиконання або недбале виконання своїх обов'язків, прихована протидія здійсненню чого-небудь.

За цілями саботажу інциденти можуть бути класифіковані таким чином:

Зниження репутації організації, наприклад, шляхом компрометації якості послуг, що надаються організацією, або інші способи нанесення збитків відносинам організації з клієнтами з метою заволодіння клієнтською базою організації.

Саботаж діяльності контрагентів організації.

Зрив, перешкоджання, маніпулювання і піддавання іншим впливам управління, ведення, результату деякої бізнес-діяльності, допоміжної діяльності або окремого проекту організації. Наприклад, для отримання конкурентами організації чи іншими суб'єктами ринкових відносин певних переваг, зловмисником створюються умови, що перешкоджають забезпеченню організацією її законних прав.

Саботаж здійснюваних підприємством заходів безпеки і створення вразливостей з метою зниження захищеності інформаційних активів організації перед зовнішніми і внутрішніми загрозами.

Приховування доказів, створення хибних версій та інших перешкод для розслідування протиправної діяльності на підприємстві.

Маніпулювання ринками цінних паперів шляхом створення "негативу" через розповсюдження інформації про надзвичайні події в організації.

Помста організації або окремим її працівникам.

Екстремістські, терористичні, політичні та інші схожі їм цілі.

За відомостями аналітиків, 92 % випадкам саботажу передує неприємний інцидент на роботі або ціла серія таких інцидентів. Так, 47 % випадків пов'язані із звільненням з роботи, 20 % спровоковані суперечкою з нинішніми або колишніми колегами, причиною 13 % випадків саботажу є пониження в посаді або переведення на іншу роботу [1].

5. Шантаж компетентністю ("я – незамінний працівник"). Суть цього явища полягає у вимозі працівником деяких пільг і преференцій за його реальні або надумані унікальні виробничі знання та вміння.

6. Шантаж повноваженнями (концентрація в одних руках повноважень за кількома посадами) призводить до створення сприятливих умов для крадіжок. Особливо це небезпечно, коли компетенції однієї людини в рамках одного бізнес-процесу акумулюють в собі компетенції кількох посадових осіб.

7. Торгівля секретами (продаж "на сторону" комерційних секретів підприємства). Для попередження цього явища на підприємстві слід запровадити режим комерційної таємниці. Без встановлення такого режиму будь-які розписки, зобов'язання та додатки до трудової угоди з працівником стосовно збереження в секреті комерційної інформації підприємства будуть безпідставними.

8. Порушення дисципліни. Загальний стан дисципліни є показником готовності і можливостей колективу вирішувати виробничі завдання. Високий рівень дисципліни досягається шляхом дотримання розумного співвідношення між заходами заохочення та покарання, заснованому на понятті "справедливість".

9. Створення в колективі нестерпного морально-психологічного клімату (“мобінг”). Буває, що у колективі виникає ситуація, коли “виживають” неугодного. Причин тому може бути багато і, як правило, цим питанням займається служба управління персоналом, HR-менеджери та інші профільні фахівці. З точки зору безпеки, це явище має бути своєчасно виявлене та викоренене, так як працівник, що піддається “виживанню” з боку колег, стає потенційним “диверсантом”, “саботажником” і “продавцем секретів”.

10. Схильність працівників до різних адитивних залежностей. Адитивна поведінка характеризується прагненням відійти від реальності за допомогою зміни свого психічного стану. Виокремлюють хімічні та нехімічні форми адикцій. До нехімічних відносять: азартні ігри (гемблінг), сексуальну адикцію, любовну адикцію, адикцію відносин, трудову адикцію, адикцію до витрати грошей, ургентні адикції, Інтернет та комп'ютерну адикцію. Проміжне місце між хімічними та нехімічними адикціями займає адикція від їжі (булімія, анорексія). При цій формі адикції безпосередньо задіяні біохімічні механізми. До хімічних форм залежності відносять алкогольну залежність і наркотичну. Є очевидним, що працівники схильні до будь-якого виду залежності – “слабка ланка” підприємства. Боротися з залежностями – не є завданням системи безпеки. Залежності необхідно виявляти і враховувати в повсякденній роботі. Якщо ж залежність співробітника завдає шкоди підприємству, то вихід тільки один – звільнення.

Вищеперелічені загрози, джерелом яких є персонал, здатні порушити стійкість, розвиток і навіть привести до зупинки діяльності організації. У зв’язку з цим, основним завданням діяльності служби управління персоналом має бути забезпечення своєчасності виявлення, аналізу, запобігання і прогнозування потенційних загроз економічній безпеці організації з боку її працівників.

Література:

1. Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors [Electronic resource]. – Access mode : https://resources.sei.cmu.edu/asset_files/SpecialReport/2005_003_001_51946.pdf

УДК 327.5/327.8

Ізмалков О. М
Національний гірничий університет

ВИКОРИСТАННЯ РОСІЙСЬКОЮ ФЕДЕРАЦІЄЮ РЕФЛЕКСИВНОГО УПРАВЛІННЯ ЯК СКЛАДОВОЇ ГІБРИДНОЇ ВІЙНИ

Гібридна війна - це війна з використанням регулярної та нерегулярної армії, а також збройних формувань з боку країни-агресора. Держава яка розпочинає гібридну війну використовує професійних командирів, та терористичні організації. Основна відмінність гібридної війни від звичайної в тому, що виконавець робить можливим проведення війни замість держави. Гібридна війна є стратегією, яка використовується для просування своїх політичних цілей на полі бою із застосуванням військової сили.

Визначено три умови, завдяки яким може бути використана гібридна війна Російської Федерації (РФ) проти України:

РФ має своїх прихильників на території України;

РФ має вплив на українські ЗМІ;

3) Держава проти якої ведеться гібридна війна не має здорового громадянського суспільства. [1 с 23]

РФ використовує передові форми гібридної війни в Україні, що в значній мірі спирається на елементи інформаційної війни, в РФ називають це «рефлексивне управління». «Рефлексивне управління» спонукає противника обирати дії найбільш вигідні для своїх цілей.

Основні функції «рефлексивного управління»:

1) негативний вплив політичних партій на ситуацію в країні;

2) значна кількість населення з антиукраїнськими настроями;

3) знищення індустріальної інфраструктури на окупованій території.

Рефлексивне управління і інформаційна війна РФ в цілому, не є результатом теоретичних інновацій, а є планом дестабілізації ситуації в Україні.

Ключовими елементами рефлексивних методів управління РФ в Україні є:

1) заперечення фактів операцій, спрямованих проти України, для приховування присутності регулярних збройних сил РФ;

2) приховування мети і завдань РФ в конфлікті на сході України;

3) збереження правдоподібним законність дій РФ проти України.

Рефлексивне управління включає чотири різних періоди:

1) дослідження;

2) практична орієнтація;

3) психолого-педагогічний;

4) соціально-психологічний [2 с 244].

Ця теорія використовується в інформаційній війні РФ проти України та має розглядатись як загроза заподіяння неприйнятних рівнів пошкоджень проти держави або групи держав, шляхом атак на інформаційні ресурси.

Один з найефективніших способів впливу на інформаційні ресурси тієї чи іншої держави полягає в використанні рефлексивних заходів контролю та управління. Ця мета найкраще досягається шляхом дезінформації, призначеної для впливу на інформаційний ресурс. Інформаційний ресурс визначається як:

інформація і передавачі інформації, метод або технологія отримання, передачі, збору, зберігання і використання цієї інформації;

2) інфраструктура, в тому числі інформаційні центри, засоби для автоматизації інформаційних процесів;

3) програмування та математичні засоби для управління інформацією;

4) адміністративні та організаційні органи, які керують інформаційними процесами, наукові співробітники, персонал, який обслуговує засоби інформатизації.

На стратегічному рівні, уряд РФ заперечує причетність своїх збройних сил до ситуації на сході України. Результатом рефлексивного управління є наявність в Україні нестабільної ситуації вираженої в поганому орієнтуванні українського населення в достовірності викладеної для них інформації.

Рефлексивне управління має дві значні переваги для РФ:

не знаючи справжніх цілей РФ, противник ставиться в положення, в якому він повинен вгадати їх;

2) зберігаючи ініціативу, поки противник орієнтується в даній ситуації.

РФ, визнаючи недоліки противника, використовує гібридну війну як важливу складову для підтримання інформаційної війни проти України. Гібридна стратегія буде завжди створювати значні проблеми для світового співтовариства, саме через використання рефлексивного управління. [2 с 248]

У якості головних засобів протидії цим недолікам пропонується:

1) проведення результативної стабілізаційної політики;

2) евакуація мирного населення з району збройного протистояння. Підвищення відповідальності високопосадовців за невиконання своєї роботи.

3) Підготовка проекту з відновлення постраждалих територій на сході України.

РФ використовує техніку рефлексивного управління для переконання США та їхніх європейських союзників залишатися пасивними в українському питанні. Мета РФ зірвати і дестабілізувати ситуацію в Україні за допомогою військових і невійськових засобів. Щоб запобігти цьому світове співтовариство повинно стати готовим до використання рефлексивних методів управління і знайти способи боротьби з ними, для здобуття успіхів в протидії гібридної війни.

Література

1. Peter Apps, “Russia raises military clout with reforms after Georgian war,” Reuters, February 27, 2014: 22-25 с.

2. Timothy L. Thomas, “Russia’s Reflexive Control Theory And The Military,” Journal Of Slavic Military Studies 2014, 17: 237–256 с.

УДК 342.6

Калашнікова Т. А.
Національна академія СБ України
Семчишина С. В.
Національна академія СБ України

СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ ДЕРЖАВНОЇ ПОЛІТИКИ В СФЕРІ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

Головною метою державної інформаційної політики стосовно національних інформаційних ресурсів, є створення необхідних економічних і соціокультурних умов та правових і організаційних механізмів формування, розвитку і забезпечення ефективного використання національних інформаційних ресурсів в усіх сферах життя і діяльності громадянина, суспільства й держави.

Тому функції державного управління інформаційними ресурсами можна сформулювати, як:

- розробка й прийняття політичних рішень, законодавчих і нормативно-правових актів щодо забезпечення системи управління національними інформаційними ресурсами та удосконалення механізмів реалізації правових норм чинного законодавства;
- розробка і реалізація організаційних заходів і нормативно-методичного забезпечення відомчих і регіональних структур та недержавного сектора в сфері формування та використання інформаційних ресурсів за умови координації діяльності згаданих структур;
- оптимізація державної політики інформатизації щодо забезпечення науково-технічних, виробничо-технологічних і організаційно-економічних умов створення та застосування інформаційних технологій, інших елементів інформаційної інфраструктури для формування, розвитку і ефективного використання інформаційних ресурсів та сприяння доступу громадян до світових інформаційних ресурсів, глобальних інформаційних систем;
- забезпечення функціонування ефективно діючої комплексної системи захисту інформаційних ресурсів;
- забезпечення захисту громадян, суспільства і держави від хибної, спотвореної та недостовірної інформації;

- контроль за встановленим порядком і правилами формування, розвитку і використання інформаційних ресурсів;

- нагляд за додержанням законодавства в сфері формування, розвитку, використання інформаційних ресурсів та здійснення правосуддя у сфері суспільних інформаційних відносин [2,с.48].

Для досягнення вказаної цілі в процесі подальшої розбудови корінного української державності на перший план в інформаційній сфері постають такі завдання:

зміцнення єдності інформаційного простору та усунення інформаційних погроз цілісності держави;

створення інформаційних умов для інтенсивного формування громадянського суспільства;

забезпечення інформаційного середовища для постійної відкритої взаємодії між державною владою і громадянським суспільством, що формується;

створення правових, економічних і організаційних умов для об'єднання державних й недержавних інформаційних ресурсів, інформаційно-комунікаційних мереж і систем у єдину загальнодержавну інформаційно-комунікаційну інфраструктуру та систему національних інформаційних ресурсів.

Тому варто зазначити, що під час розробки концепції державної інформаційної політики України треба виходити з необхідності прийняття таких базових принципів:

відкритості інформаційної політики;

рівності інтересів всіх учасників інформаційних відносин;

системності;

пріоритетності вітчизняного виробника;

несуперечності – головні заходи повинні бути спрямовані на забезпечення державних інтересів України, але не суперечити соціальним інтересам громадян країни;

соціальної орієнтації – фінансування державою тільки того, що спрямовано на інформаційний розвиток соціальної сфери.

Державна інформаційна політика це політика, яка засобами державної влади створює та забезпечує функціонування правової системи регулювання інформаційних відносин, захищає права людини, забезпечує збалансування інтересів людини, суспільства та держави у всіх сферах інформаційної діяльності.

Література

1. Закон України “Про державну таємницю” від 21.01.1994 // Відомості Верховної Ради України, 1994, № 16. – Ст. 93.

2. Информационное право: основы практической информатики. Учебное пособие / И. Л. Бачило. - М.: 2003. - С. 48.

3. Закон України “Про інформацію” // Відомості Верховної Ради, 1992, № 48. – Ст. 650-651.32

4. Закон України “Про захист інформації в інформаційно- телекомунікаційних системах” від 05.07.1994 // Відомості Верховної Ради України, 1994, № 31. – Ст. 286, із змінами 2005 р.

УДК 341.1/8

Князєв С. О

кандидат юридичних наук, старший науковий співробітник

Національна академія СБ України

Адрага І. І.

Національна академія СБ України

МОЖЛИВОСТІ ВИКОРИСТАННЯ ДОСВІДУ КРАЇН СХІДНОЇ ЄВРОПИ У ВІТЧИЗНЯНІЙ СИСТЕМІ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ

Надійна охорона державної таємниці безперечно має важливе значення, оскільки дана категорія інформації з обмеженим доступом є найбільш уразливою для життєво важливих інтересів будь-якої держави.

Відповідно до статті 1 Закону України «Про державну таємницю» охорона державної таємниці визначається як комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів, спрямованих на запобігання розголошенню секретної інформації та втратам її матеріальних носіїв [1.ст.1].

Реалізацію даного комплексу заходів забезпечують відповідні, законодавчо визначені, суб`єкти, серед яких важливе місце займає СБ України. Стаття 5 Закону України «Про державну таємницю» визначила СБ України спеціально уповноваженим державним органом у сфері забезпечення охорони державної таємниці.

Разом з тим, новітні реалії, в тому числі, в інформаційній сфері, пов`язані з російською загрозою, іншими докорінними змінами у зовнішньому та внутрішньому безпековому середовищі України обумовлюють необхідність створення нової системи забезпечення національної безпеки України.

У цьому контексті, зважаючи на нову Стратегію національної безпеки України, яка була затверджена Указом Президента України від 26 травня 2015 року № 287/2015, до актуальних загроз національній безпеці України віднесені загрози кібербезпеці і безпеці інформаційних ресурсів, що, у свою чергу, включає:

уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак;

фізична і моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом [4].

Порівняльне законодавство пострадянських країн, які раніше входили до складу СРСР, дозволяє дійсно говорити про спільну спадщину щодо вирішення питань пов’язаних з охороною державної таємниці.

Звідти, актуальним питанням стає врахування досвіду охорони секретної інформації, як у провідних країнах світу, так і пострадянських, але які вже певний час були зорієнтовані на Євроінтеграцію. Зокрема, дослідження досвіду Латвійської та Естонської Республік.

Так, у Латвійській Республіці суб'єктами охорони державної таємниці визначені державні органи, посадові особи і співробітники таких органів, а також інші особи, які у зв'язку з виконанням ними своїх посадових (службових) або трудових обов'язків створюють, отримують, зберігають або використовують матеріальні носії державної таємниці.

Організація охорони державної таємниці покладається на Кабінет Міністрів. Відповідно до законодавства Латвійської Республіки, головними координаторами та контролюючими органами щодо застосування заходів охорони державної таємниці виступають Бюро із захисту Конституції, Служба військової контрозвідки і Служба безпеки [2.ст.7].

Виходячи з цього ми бачимо, що у Латвійській Республіці відсутній єдиний орган державної влади, який би займався охо-

роною державної таємниці, натомість це питаня перебуває в компетенції кількох спеціальних органів.

В Естонському Законі «Про державну таємницю» окремо визначаються особи які, наділені правом віднесення інформації до державної таємниці, а саме: Президента Республіки, Члени уряду Республіки, командувач збройними силами, керівники виконавчих органів державної влади, канцлери міністерств, посадові особи не нижче рівня старшого чиновника. За результатами вивчення законодавства цієї країни, ми також не побачили єдиного органу, який би займався охороною державної таємниці [3.ст.8].

Ще одним важливим аспектом щодо охорони державної таємниці є визначення ступенів секретності та термінів на які інформація може бути обмежена у доступі.

В Естонській Республіці визначені наступні ступені секретності: «Цілком таємно», «Таємно», «Конфіденційно», проте, на відміну від України, в Естонії кожен ступінь секретності не має окремого терміну обмеження. Загальний термін засекречування інформації не перевищує 50 років, а щодо конфіденційних джерел, розвідки і контррозвідки – не більше 75 років. Раз на рік здійснюється перегляд секретних відомостей щодо перевірки відповідності їх ступенів секретності та термінів обмеження [3.ст.7].

У законі Латвійської Республіки визначено такі ступені секретності: «Особливої важливості», «Цілком таємно», «Таємно». Відомості зі ступенем «Таємно» обмежуються на 5 років, зі ступенем «Цілком таємно» - 10 років, зі ступенем «Особливої важливості» - 20 років. Дані про осіб, що займаються оперативно-розшуковою діяльністю, обмежуються на 75 років [2.ст.8].

Крім того, порівнюючи існуючі в Латвійській Республіці та Естонській Республіці ступені секретності доцільно акцентувати увагу й на їх відмінностях. Отже, В Естонському законодавстві використовується таке поняття, як «Конфіденційно», що можливо трактувати, як інформацію з обмеженим доступом, яка є власністю держави, але не становить державної таємниці. Фактично, аналог вітчизняної службової інформації.

По-друге, це терміни віднесення до секретної інформації. На прикладі Естонії ми бачимо, що визначений загальний термін засекречування, але специфіка полягає в тому, що раз на рік здійс-

нюється перегляд інформації щодо перевірки відповідності наявного ступеня секретності та можливої зміни терміну обмеження.

Таким чином, навіть адоптація у вітчизняному законодавстві процедури щорічного перегляду ступенів секретності, на наше переконання, дозволить більш ефективно використовувати бюджетні кошти на охорону матеріальних носіїв, які дійсно містять секретну інформацію уразливу для національної безпеки.

Отже, підсумовуючи вище сказане, можна дійти висновку, що кожна держава з метою охорони інформації, що містить державну таємницю формує спеціальну систему її захисту, залежно від наявних загроз, правової системи та інших чинників. Навіть невеличке порівняння окремих правових норм Латвійської Республіки та Естонської Республіки дозволяє говорити про можливості вдосконалення вітчизняного законодавства у сфері охорони державної таємниці.

Звідти, подальші змістовні порівняльно-правові дослідження, безперечно потрібні для приведення існуючої загальнодержавної системи охорони державної таємниці до потреб сьогодення, можливості ефективного протистояння сучасним загрозам.

Література

1. Закон України «Про державну таємницю» від 21.01.1994 [Електронний ресурс]. – Режим доступу: http://www.zakon.rada.gov.ua

2. Закон Латвійської Республіки «Про державну таємницю» від 29.10.1996 [Електронний ресурс]. – Режим доступу: http://lib.rada.gov.ua

3. Закон Естонської Республіки «Про державну таємницю» від 11.11.1997 [Електронний ресурс]. – Режим доступу: http://estonia.news-city.info

4. Указ Президента "Про Стратегію національної безпеки України" від 26.05.2015 №287/2015 [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua

УДК 355.482 : 005.3 : 94 (477)

Лісов О. С.
Національна академія СБ України

ДЕЯКІ АСПЕКТИ ЗАСТОСУВАННЯ ІСТОРИЧНИХ ЗНАНЬ В ІНФОРМАЦІЙНІЙ СФЕРІ В УМОВАХ ПРОВЕДЕННЯ АНТИТЕРОРИСТИЧНОЇ ОПЕРАЦІЇ

Відповідно до статті 7 Закону України «Про основи національної безпеки України» однією із реальних загроз національній безпеці України в інформаційній сфері є намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

Одним із заходів запобігання вказаній загрозі є здійснення постійного моніторингу інформаційного простору в Україні, зокрема офіційних сайтів органів державної влади та місцевого самоврядування з метою відповідності розміщеної на них інформації вимогам чинного законодавства України.

В районі проведення антитерористичної операції, на території Донецької та Луганської областей, яка підконтрольна органам влади України такі сайти відіграють на сьогодні важливу роль у формуванні регіонального інформаційного простору.

Більшість вказаних інформаційних ресурсів мають рубрики «історія міста», «історія району», ознайомлення з якими сприяє кращому розумінню впливу історичного чинника на розвиток суспільно-політичної обстановки в регіоні. Проведений аналіз статей з історії міст та районів підконтрольних територій Донецької та Луганської областей дає змогу визначити наступні тенденції:

- матеріали статей переважно складаються із тверджень, ідеологічних установок та концепцій, усталених за радянських часів;
- територія регіону часто ототожнюється з Півднем Росії, Донбасом і дуже рідко з Україною, що сприяє укоріненню пропагандистської риторики Російської Федерації з приводу т.зв. «ЛНР, ДНР, Новоросії» (наприклад «народ Донбасу» замість «народ України» тощо);
- позитивна роль у розвитку міст, районів та регіону загалом пов’язується з Російською імперією та СРСР;
- період Української Революції 1917-1921 рр. описується як «громадянська війна», що призвела до негативних економічних наслідків;

- період Української Держави (Гетьманату П. Скоропадського) висвітлюється як австро-німецька окупація;

- становлення комуністичного тоталітарного режиму 1917-1991 рр. в Україні зображується як виключно позитивний етап розвитку регіону;

- майже не висвітлюються події Голодомору 1932-1933 рр. в Україні, що є порушенням вимог статі 3 Закону України «Про Голодомор 1932-1933 років в Україні» з боку деяких органів місцевого самоврядування Донецької та Луганської областей;

- замовчуються репресії комуністичного тоталітарного режиму 1917-1991 рр. в Україні, що не відповідає змісту Закону України «Про реабілітацію жертв політичних репресій на Україні»;

- у зазначених матеріалах не враховано вимоги законів України «Про засудження комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів в Україні та заборону пропаганди їхньої символіки», «Про правовий статус та вшанування пам'яті борців за незалежність України у XX столітті»;

- замовчується здобуття Україною незалежності як фундаментальне досягнення нашого народу;

- новітній період суверенної України в історії міст часто зображується лише у негативному світлі здебільшого крізь призму низки економічних криз та занепаду важкої промисловості.

Такі матеріали не відповідають національно-державницькому розумінню історії України та негативно впливають на загальне інформаційне поле в районі проведення антитерористичної операції.

З метою недопущення розміщення на офіційних сайтах органів державної влади та місцевого самоврядування матеріалів з історії міст та районів, що мають тенденційний та антиукраїнський характер, необхідно створити механізм їх рецензування у провідних наукових установах країни, зокрема в Інституті історії України Національної академії наук України, Українському інституті національної пам'яті, а також залучати до цієї роботи громадські організації, наприклад Національну спілку краєзнавців України.

УДК 378.2

Лукіянюк Я. В.
Львівський державний університет безпеки життєдіяльності
Мандрона М. М.
кандидат технічних наук
Львівський державний університет безпеки життєдіяльності

ПРОБЛЕМНІ ПИТАННЯ ПІДГОТОВКИ ФАХІВЦІВ У ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Швидкий розвиток ІТ-технологій та удосконалення телекомунікаційних систем потребує удосконалення сучасних систем захисту інформації, які б забезпечували зберігання, обробку та безпечне передавання конфіденційної інформації комунікаційними мережами. Захист інформації тривалий час був секретною галуззю знань у СРСР [1]. Наприклад, викладати криптографію мав право тільки інститут криптографії, зв'язку та інформатики (ІКЗІ). Проблемна ситуація вирішилась у 1990-х роках, коли стало неможливо ігнорувати інтенсивний розвиток сучасних ІТ-технологій [2].

Національна безпека держави – це захищеність важливих для життя інтересів людини і громадянина, суспільства та держави.

Важливою складовою національної безпеки держави є інформаційна безпека, головним фактором якої є "фактор людини". Людина є основним носієм і користувачем інформації, вона ж є основним суб'єктом і об'єктом інформаційної боротьби.

До середини 90-тих років підготовка фахівців з питань технічного захисту інформації у ВНЗ України не проводилась. Початком підготовки фахівців у сфері інформаційної безпеки вважають з моменту підписання наказу Державної служби України з питань технічного захисту інформації та Міністерства освіти України від 28 грудня 1995 р. № 66/358 "Про співробітництво між Міністерством освіти України і Державною службою України з питань технічного захисту інформації".

Нами проаналізовано фактори [1-4], від яких залежить захищеність інформаційного простору:

- рівень обізнаності населення про проблеми інформаційної безпеки;
- рівень підготовки силових міністерств та відомств, їхніх керівників та особового складу;

- рівень підготовки кваліфікованих фахівців у сфері інформаційної безпеки, які б могли перевіряти інформаційне середовище та проводити відповідні дії щодо забезпечення захисту.

Отже, із перелічених факторів можна зробити висновок щодо актуальності проблеми підготовки фахівців у галузі інформаційної безпеки.

Особливості сфери інформаційної безпеки наведено у рис. 1 та рис. 2 зображено структуру системи такої підготовки [3].

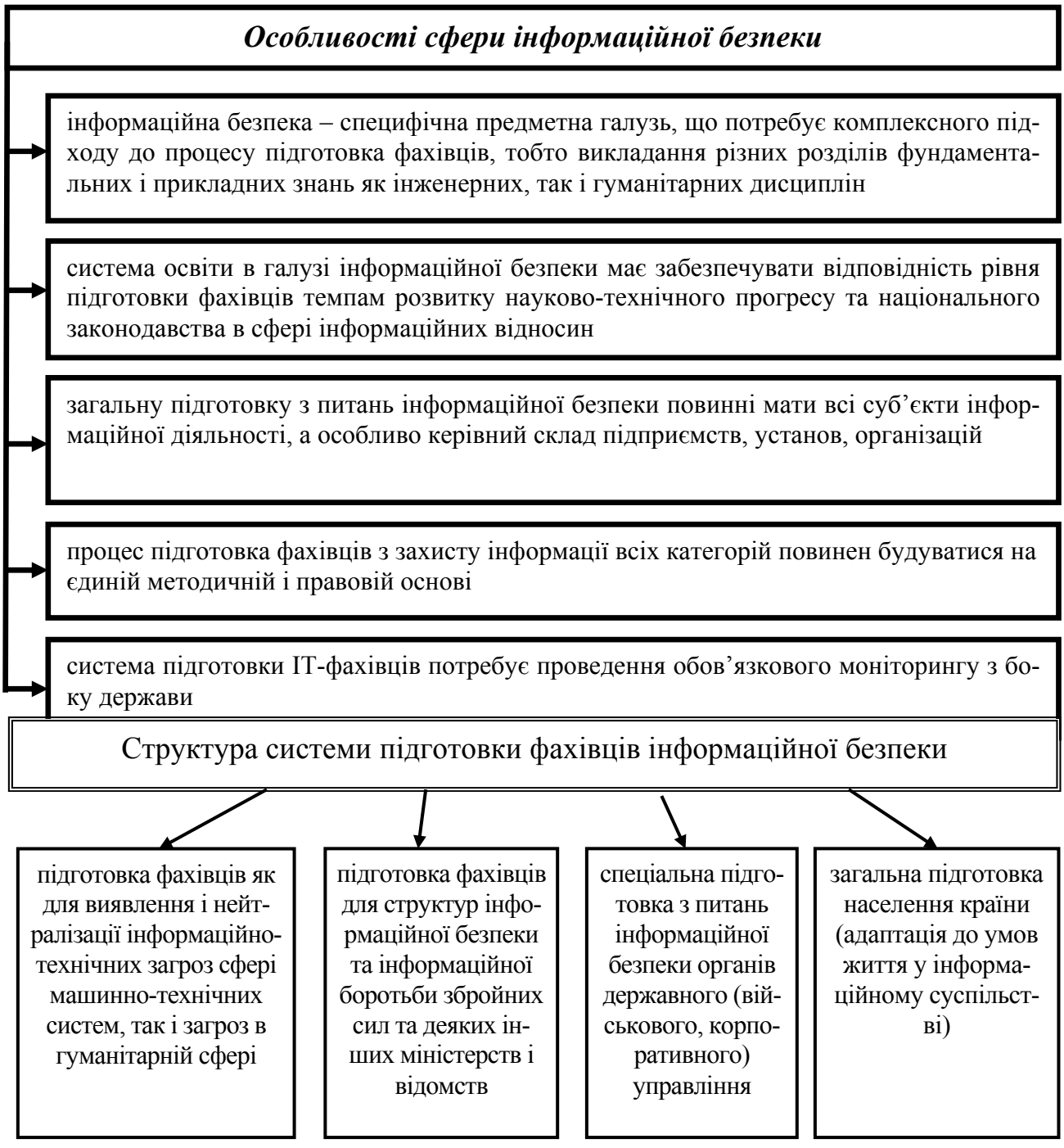

Рис. 2. Структура системи підготовки фахівців інформаційної безпеки

До позитивних моментів у підготовці фахівців з інформаційної безпеки в Україні належить:

- наявність в Україні спеціалізованих вищих навчальних закладів з високим рівнем підготовки фахівців, які визнані не тільки в Україні, а й за кордоном;

- використання у навчальному процесі провідної кредитно-модульної системи організації навчання;

- розширення міжнародних зв'язків із закордонними центрами та їхніми технологіями підготовки фахівців.

Однак існує багато недоліків, а саме:

- недостатнє адаптування організації навчального процесу до сучасних проблем у сфері інформаційної безпеки, оскільки у наш час інформаційні та комп'ютерні технології стрімко розвиваються, а стандарти викладання не встигають своєчасно оновлювати;

- поєднання у підготовці фахівців визначеного напряму додатково елементів інших напрямів, внаслідок чого не вистачає часу на достатню підготовку з профільних дисциплін та невідповідність кваліфікаційним вимогам;

- необхідність організації підготовки, враховуючи більш конкретні об'єкти діяльності випускників, окремо фахівців гуманітарного і технічного профілю, а також цивільних та військових фахівців;

- недостатня увага до підвищення кваліфікаційного рівня фахівців за місцем праці, враховуючи специфіку роботи.

Для вирішення зазначених проблем необхідно розвивати певні складові державної системи підготовки кваліфікованих фахівців з інформаційної безпеки в Україні, а саме:

- створення науково-методичні комісії за відповідними галузями знань;

- розвиток профільних науково-дослідних установ;

- створення необхідного рівня підсистеми перепідготовки та підвищення кваліфікаційного рівня фахівців;

- розвиток підсистеми спеціальної підготовки з питань інформаційної безпеки особового складу;

- створення більш сприятливих умов для адаптації визначених верств населення до інформаційного суспільства.

Таким чином, система підготовки кадрів для роботи у сфері інформаційної безпеки проводиться безсистемно і не відповідає

вимогам сучасності, та ще є далекою від досконалості. Удосконалення процесу навчання передбачає корегування існуючих навчальних програм та планів, розроблення та введення нових навчальних дисциплін.

Література

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

2. Грайворонський М.В. Безпека інформаційно-комунікаційних систем / Грайворонський М.В., Новіков О.М. – К. : Вид. група BHV, 2009. – 608 с.

3. Підготовка фахівців із захисту інформації в Україні [Бабак В.П., Козловський В.В., Хорошко В.О., Чирков Д.В.] // Захист інформації. – 2001. – № 4. – С. 57-69.

4. Маклаков Г. Научно-методологические аспекты подготовки специалистов в области информационной безопасности. [Електронний ресурс]. – Доступно з: http://www.crime-research.ru/articles/ Maklakov0105/10.

УДК 323:351/343:341

УДК 32.019.5 (477)

Озерний І. М.
Національна академія СБ України

СИСТЕМА СТРАТЕГІЧНИХ КОМУНІКАЦІЙ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ: ПЕРСПЕКТИВИ РОЗВИТКУ

Актуальність теми дослідження полягає у тому, що на сьогодні наша країна знаходиться у стані неоголошеної війни або гібридної, як її називають. Противник використовує всі можливі способи її ведення, в тому числі інформацію як один із інструментів впливу на суспільство та формування громадської думки. За допомогою ЗМІ та інтернет-ресурсів він намагається вплинути та донести до громадськості нелегітимну, недостовірну інформацію, деморалізувати збройні сили України.

Донедавна органи державної влади, зокрема органи безпеки та оборони України не використовували стратегічні комунікації у системі зв'язків з громадськістю. На даний час потреба в цьому

стає все більш актуальною, оскільки стратегічні комунікації визначають прийняття рішення в різних умовах життєдіяльності суспільства і забезпечують вирішення завдань у межах стратегії розвитку держави. За допомогою стратегічних комунікацій відбувається спланований обмін інформацією, налагодження необхідних державі зв'язків із суспільством. Тому перед сектором безпеки та оборони України постало завдання шляхом взаємодії зі ЗМІ та громадськістю доносити точну, правдиву, повну інформацію до населення, діаспори, закордонних партнерів. Водночас, пріоритетне завдання сьогодні – дати ефективну і змістовну відповідь передусім на військову, а також інформаційну агресію проти нашої держави.

З огляду на те, що наукові дослідження у даній сфері на сьогодні лише починають запроваджуватись, метою даного дослідження є аналіз перспектив розвитку системи стратегічних комунікацій сектору безпеки і оборони України.

Відповідно до Дорожньої карти Партнерства у сфері стратегічних комунікацій між Радою національної безпеки і оборони України та Міжнародним секретаріатом НАТО система стратегічних комунікацій сектору безпеки і оборони України передбачає роботу на таких рівнях [1]:

Стратегічний рівень

Рівень 1: Створення самодостатньої внутрівідомчої і урядової/міжвідомчої системи стратегічних комунікацій:

- Збір інформації про наявні комунікаційні структури в усіх установах та її аналіз;
- Розбудова комплексної внутрівідомчої і урядової/міжвідомчої системи стратегічних комунікацій;
- Розробка оперативної нормативної документації та ключових критеріїв ефективності відповідного персоналу;
- Надання консультативної допомоги при оцінюванні та сертифікації відповідного персоналу;
- Забезпечення підготовки та інструктажу на початковому етапі.

Рівень 2: Розробка і реалізація національної стратегії України у галузі стратегічних комунікацій:

- Огляд можливих існуючих варіантів національної стратегії, так званого національного наративу;
- Надання допомоги у розробці національного наративу України;

- Дорадча допомога у застосуванні каналів комунікації з метою просування українського національного наративу на національному і міжнародному рівнях.

Рівень 3: Створення системи підготовки у галузі стратегічних комунікацій (підготовка інструкторів):

- Аналіз наявного потенціалу/досвіду на всіх напрямах стратегічних комунікацій у міністерствах та установах;
- Створення он-лайн електронної бази даних навчальних матеріалів з відкритим доступом і проведення курсів у галузі стратегічних комунікацій для урядових комунікаторів;
- Розробка стандартів аналізу і оцінки професійної підготовки, нормативної документації та процедур;
- Впровадження навчальних програм/курсів із стратегічних комунікацій до навчального плану відповідних освітніх закладів.

Операційний рівень

Рівень 1: Вдосконалення нормативних документів, що регламентують процес комунікації у структурах безпеки і оборони:

- Аналіз/огляд чинних нормативних актів (політики/нормативної документації/ посадових інструкцій/ законів), що регламентують процес комунікації у структурах безпеки і оборони;
- Розробка нових стандартів та нормативних документів, у разі необхідності;
- Підготовка персоналу щодо застосування нових стандартів і правил;
- Запровадження нових стандартів і правил.

Рівень 2: Підвищення ефективності державних ЗМІ

- Сприяння включенню різних державних ЗМІ до ширшої структури урядової комунікації і допомога у підвищенні їх потенціалу;
- Забезпечення необхідної підготовки наявного персоналу.

Тактичний рівень

Рівень 1. Невідкладні заходи

Підготовка наявного персоналу у галузі зв’язків з громадськістю/громадської дипломатії в оборонних і безпекових структурах з таких питань:

- Основи зв’язків з громадськістю/ громадської дипломатії:
- Відносини зі ЗМІ (організація прес-турів, залучення ЗМІ, створення медіа-продукту);
- Написання повідомлень у сфері зв’язків з громадськістю;

- Написання промов і публічні виступи;
- Використання соціальних мереж і цифрових ЗМІ;
- Комунікація в умовах кризової ситуації.
- Підготовка інструкторів у структурах безпеки і оборони.
- Курси англійської мови для речників/комунікаторів.
- Розробка політики та нормативної документації із стратегічних комунікацій/ зв'язків з громадськістю/громадської дипломатії.

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

Аналіз перспектив розвитку системи стратегічних комунікацій сектору безпеки і оборони України свідчить, що заходи Партнерства у сфері стратегічних комунікацій сприятимуть розвитку здатності України здійснювати ефективні комунікації, забезпеченню системної взаємодії між усіма зацікавленими суб'єктами урядового та неурядового сектору, та стануть ефективним механізмом протидії інформаційній агресії РФ проти України.

Література

1. Дорожня карта Партнерства у сфері стратегічних комунікацій між Радою національної безпеки і оборони України та Міжнародним секретаріатом НАТО [Електронний ресурс] // Офіційний сайт РНБО України. – Режим доступу: http://www.rnbo.gov.ua/news/2283.html.

Покровська А. В.
Національний інститут стратегічних досліджень при Президентові України

ЄВРОПЕЙСЬКИЙ ДОСВІД ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ ПРОТИДІЇ ТЕРОРИСТИЧНІЙ АКТИВНОСТІ В ІНТЕРНЕТІ

Сучасний стан розвитку суспільства та резонансні події останніх десятиліть демонструють, що асиметричні методи дося-

гнення цілей, до яких належить тероризм, є одними з найбільших загроз національній безпеці держави. Тероризм нині є феноменом позатериторіальним та вимагає оперативного реагування на національному, регіональному та глобальному рівнях. Оскільки сучасний тероризм проявляється не лише у фізичній формі безпосередніх терактів, а й в інформаційній та медійній сферах, проблема впровадження відповідних механізмів протидії тероризму у цих сферах постає ключовою у розумінні пов'язаних з ним загроз. Терористичні та екстремістські угруповання є дедалі активнішими в комунікаційних мережах, отримуючи фактично необмежені можливості для пропаганди, спілкування, фінансування, пошуку прихильників, тренування та координації дій, підбурювання до терористичних актів та реалізації кібер-атак, особливо з врахуванням можливостей соціальних медіа (мереж).

Серед провідних держав Європи, Великобританія, Франція та Німеччина впродовж останніх десятиліть отримали чималий досвід масштабних терактів та крайніх проявів екстремізму. Поряд з ефективними «жорсткими» механізмами боротьби з тероризмом, ці держави одними з перших у світі почали законодавчо та інституційно впроваджувати заходи боротьби з тероризмом в Інтернеті та пресі, намагаючись при цьому не порушувати баланс між забезпеченням національної безпеки та свободою слова.

Система антитерористичної діяльності Великобританії, зокрема в інформаційному просторі, забезпечується потужною законодавчою та прогресивною стратегічною базою. Головними органами антитерористичної діяльності виступають розвідувальні служби та поліцейські об'єднання, а також Королівська прокурорська служба, які тісно взаємодіють між собою та з урядом. Особливу роль у боротьбі з ескалацією тероризму у віртуальному середовищі відіграє Підрозділ боротьби з тероризмом в Інтернеті, унікальна структура, створення якої за останні 5 років дозволила зробити процес виявлення злочинних дій терористів та їх прихильників значно ефективнішим [1]. Разом із впровадженням законів, держава активно взаємодіє з ІКТ провайдерами через неурядові організації та об'єднання, вагома роль серед яких належить Internet Watch Foundation; між цією організацією та поліцією підписана угода про співробітництво з метою сприяння обміну інформацією та пришвидшення процедур виявлення та видалення контенту [2].

У Франції система антитерористичної боротьби відрізняється тим, що у країні немає єдиного уповноваженого у даній сфері органу. На боротьбу з тероризмом скеровуються максимум зусиль служб, що мають до цього відношення. Такими є Директорат національної поліції, Антитерористичний підрозділ Генерального директорату судової поліції, Антитерористичний координаційний центр, жандармерія та розвідка [3]. Після трагічних подій 7 січня та 13 листопада 2015 року, інформаційно-комунікаційні засоби протидії терористичній загрозі у Франції стали значно жорсткішими. Так, після теракту у редакції Charlie Hebdo був розроблений та у подальшому прийнятий у травні закон, що значно розширює повноваження правоохоронних органів при зборі інформації про підозрюваних у тероризмі; закон дозволяє державі моніторити телефонні дзвінки та електронну пошту підозрюваних без дозволу суду, збирати метадані користувачів у Інтернет-провайдерів [4]. Попри те, що терористична загроза у Франції залишається значною та режим надзвичайного стану продовжується, державі слід не забувати про узгодження дій, що можуть обмежити свободи громадян, з громадянським суспільством.

Система боротьби з тероризмом у Німеччині, зважаючи на федеральну форму устрою, є розгалуженою, – до неї входять понад 40 безпекових структур, які координує Об'єднаний антитерористичний центр [5]. Ефективним виявленням терористичної загрози в Інтернеті займатиметься, зокрема, сформований у грудні минулого року антитерористичний підрозділ поліції [6]. Питання обмеження свободи слова поки що не стоїть гостро в Німеччині, однак у зв'язку з міграційною кризою державі доведеться встановлювати більший контроль над інформаційним простором для недопущення радикалізації та надання можливим ісламістам "кисню публічності".

Якщо говорити про Україну у даному контексті, то слід зазначити, що наша держава зіштовхнулася нині з масштабною проблемою ескалації підтримуваних Росією терористичних сепаратистських рухів на Сході, хоча, на жаль, не визначилась з самого початку з форматом боротьби та не надала достатньої уваги інформаційно-комунікаційному та медійному фронту цієї боротьби. Так, згідно з дослідженням Інституту економіки та миру «The Global Terrorism Index 2015», Україна знаходиться на 12 місці із 162 за рівнем терористичних інцидентів, маючи оцінку 7.2

із 10 [7]. Суміжне дослідження цього аналітичного центру «Global Peace Index 2015» помістило Україну на 150 місце з оцінкою 2.845, наша держава знаходиться між Лівією та Нігерією [8].

Разом з тим, Україною зробила певні позитивні кроки у напрямі реформування системи антитерористичної боротьби. Створюються, зокрема, оперативні антитерористичні підрозділи в рамках Національної поліції України. Однак, все ще вимагає вирішення проблема продуманого законодавчого регулювання системи здійснення антитерористичних операцій. У цьому контексті набуває особливого значення чітке визначення рамок антитерористичної діяльності, зокрема, в інформаційній сфері. У даному напрямі для України представляє інтерес адаптація з врахуванням національної специфіки досвіду антитерористичної законотворчої та, за можливості, інституційної діяльності трьох зазначених провідних європейських країн, а також діяльності їхніх безпекових структур боротьби з тероризмом, їх взаємодії з громадянським суспільством.

Література

1. The Counter-Terrorism Internet Referral Unit [Електронний ресурс] – Режим доступу: http://www.npcc.police.uk/ NPCCBusinessAreas/ PREVENT/TheCounterTerrorismInternetReferralUnit.aspx.

2. Service Level Agreement between the Association of Chief Police Officers (ACPO) and the Internet Watch Foundation (IWF) [Електронний ресурс] – Режим доступу: https://www.iwf.org.uk/assets/media/ hotline/SLA%20ACPO%20IWF%20FINAL%20OCT%202010.pdf.

3. Committee of Experts on Terrorism. Profiles on counter-terrorist capacity, France [Електронний ресурс] – Режим доступу: https://www.coe.int/t/dlapil/codexter/Country%20Profiles/Profiles%202013%20France_EN.pdf.

4. Surveillance law prompts unease in France [Електронний ресурс] – Режим доступу: http://www.bbc.com/news/world-europe-32497034.

5. Germany fights terror with red tape [Електронний ресурс] – Режим доступу: http://www.politico.eu/article/one-threat-40-agencies-germanys-terror-response-europol-weapons/.

6. Germany introduces new counter-terrorism police unit [Електронний ресурс] – Режим доступу: http://www.washingtontimes.com/ news/2015/dec/16/germany-introducing-new-counter-terrorism-police-u/.

7. The Global Terrorism Index 2015 [Електронний ресурс] // The Institute for Economics and Peace (IEP). – 2015. – Режим доступу: http://economicsandpeace.org/wp-content/uploads/2015/11/Global-Terrorism-Index-2015.pdf.

8. Global Peace Index 2015 [Електронний ресурс] // The Institute for Economics and Peace (IEP). – 2015. – Режим доступу: http://economicsandpeace.org/wp-content/uploads/2015/06/Global-Peace-Index-Report-2015_0.pdf.

УДК 005.3

Савченко А. С.
Національна академія СБ України

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ

Стрімке розгортання державотворчих процесів в Україні, соціально-економічні реформи, розвиток науково-технологічної сфери викликають різке зростання вимог до рівня інформатизації суспільства та інформаційно-аналітичного забезпечення органів державної влади.

На сучасному етапі переходу від індустріального до інформаційного суспільства у всіх провідних країнах світу розвиток інформаційного простору та інформаційних технологій стає безпосереднім джерелом економічного зростання, забезпечення обороноздатності країни, соціально-політичної стабільності та розвитку демократичних засад в управлінні державою. Головний зовнішній прояв інформаційного суспільства – це інтенсивне насичення всіх сфер його життєдіяльності інформаційними продуктами та інформаційно-телекомунікаційними технологіями. Отже, цим тенденціям повинні слідувати усі ієрархічні рівні управління державою.

Для України, в якій на тлі економічних реформ розгортається адміністративна реформа, питання формування інформаційно-аналітичної бази, для прийняття управлінських рішень на державному рівні, є особливо актуальним. Ефективна та якісна система інформаційного забезпечення органів державної влади є невід'ємною складовою професійного функціонування системи державного управління. Впровадження та всебічне використання сучасних інформаційних технологій в управлінській діяльності забезпечує інформаційно-аналітичну підтримку прийняття управлінських рішень на всіх рівнях, а також супроводжує інформа-

ційну підтримку соціально-економічного розвитку держави і її окремих регіонів, забезпечує інформаційні потреби державних службовців та інших категорій громадян, створює умови для об'єктивного формування громадської думки щодо діяльності органів влади, а також послуг, які вони надають[3].

Усе це свідчить про актуальність завдань наукової статті, та підтверджує необхідність розробки методичних та практичних рекомендацій, щодо вдосконалення системи державного управління на основі сучасного інформаційно-аналітичного забезпечення всіх ланок державної влади.

Інформаційне забезпечення є важливою функціє у державно-управлінської діяльності. За відсутності необхідної інформації складно приймати об’єктивні та своєчасні державні управлінські рішення. У зв'язку з цим, робота державних органів має забезпечуватися своєчасною інформаційною підтримкою.

Термін "інформаційно-аналітичне забезпечення" становлять два взаємопов’язані елементи, а саме:

- інформаційний – відносно самостійної діяльності спеціально підготовлених фахівців, зайнятих пошуком, відбором, обробкою, накопиченням, узагальненням і збереженням інформаційних одиниць (перший етап процесу інформаційно-аналітичного забезпечення у системі управління будь-якого механізму);

- аналітичний – як похідний другий етап процесу інформаційно-аналітичного забезпечення у системі управління будь-якого механізму: виробництво спеціально підготовленими фахівцями на підставі наявних інформаційних одиниць і складних розумових процесів нового знання щодо явища або події, що вивчається [2].

Отже, інформаційно-аналітичне забезпечення – це процес створення оптимальних умов задля задоволення інформаційних потреб та реалізації посадових обов'язків органів державної влади на основі формування та використання інформаційних ресурсів. Метою інформаційно-аналітичного забезпечення державних органів виконавчої влади є створення умов для прийняття ефективних державних управлінських рішень [2].

Система інформаційно-аналітичного забезпечення управління визначається як взаємозалежна та сформована сукупність організаційних, правових, інформаційних, програмно-технологічних компонентів, що забезпечують необхідну якість

прийнятих управлінських рішень за рахунок доцільного використання інформаційного ресурсу.

Сьогодні стан управління в органах державної влади та місцевого самоврядування України характеризується збільшенням обсягу робіт, які вимагають використання сучасних комп'ютерних засобів, інформатизації різноманітних складових їх діяльності, впровадження нових інформаційних технологій. У цих умовах завданням процесу інформатизації діяльності органів державної влади є задоволення інформаційних потреб центральних органів, органів регіональної влади і місцевого самоврядування на основі єдиного інформаційного простору, автоматизації повного комплексу управлінських та ділових процесів, застосування сучасних засобів автоматизованого управління, соціально-економічного моніторингу, електронного документообігу, аналітичної обробки даних та підтримки прийняття рішень, а також формування і використання інформаційних ресурсів і сучасних технологій; створення і впровадження інформаційно-аналітичних систем забезпечення діяльності органів державної влади.

Отже, вважаю за доцільне звернути увагу на те, що в сучасних умовах державотворення в Україні відсутня єдина Концепція формування інформаційно-аналітичного забезпечення системи органів державної влади, а також потрібне нагальне вдосконалення законодавчого забезпечення розвитку інформаційно-аналітичної діяльності у сфері державного управління.

Література

1. Дєгтяр А. О. Аналітично-організаційне забезпечення прийняття та реалізації державно-управлінських рішень: дис... д-ра наук з держ. управління: 25.00.02 / Донецький держ. ун-т управління. – Донецьк, 2005.

2. Коваль Р.А. Інформаційно-аналітичне забезпечення діяльності органів державної влади /Р.А. Коваль //Теорія та практика державного управління : зб. наук. праць. – Х. : Вид-во ХарРІ НАДУ «Магістр», 2006. – № 1 (113).

3. Лавріненко В. Інформаційно-аналітичне забезпечення діяльності органів державної влади //Вісник Національної академії державного управління при Президентові України. - 2003. - № 3.

4. http://www.kmu.gov.ua/ Проект Концепції формування та функціонування інформаційно-аналітичної системи органів державної влади та органів місцевого самоврядування.

5. Присяжна Л. Функціональний аналіз моделей комунікації для інформаційного забезпечення органів державної влади //Наукові праці Національної бібліотеки України імені В.І.Вернадського. - 2008. - Вип. 21.

УДК 004.912

Савченко Д. С.
Національна академія СБ України

ОЦІНКА СХОЖОСТІ ПОСЛІДОВНОСТЕЙ СИМВОЛІВ В ЗАВДАННЯХ З АВТОМАТИЗОВАНОЇ ОБРОБКИ НЕСТРУКТУРОВАНИХ ТЕКСТІВ

В умовах швидкого зростання неструктурованої текстової інформації в сучасних комп'ютерних мережах і обмеженими людськими ресурсами для її опрацювання в контексті вирішення завдань із забезпечення кібернетичної безпеки особливої актуальності набуває проблема інтелектуалізації методів автоматизованої обробки неструктурованих текстів.

Особливістю автоматизованої обробки неструктурованих текстів – тобто текстів, викладених природною мовою людини, є необхідність врахування випадкових помилок у них, і, як наслідок, – необхідність використання методів нечіткого зрівняння знайдених у текстах слів із записами у словниках, тобто здійснення пошуку на підставі схожості із ключовою послідовністю.

Завдання пошуку на підставі схожості з ключовою послідовністю (Approximate Search) розв'язуються в рамках теорії інформаційного пошуку як складової теорії інформації. Теоретичні засади інформаційного пошуку були закладені, починаючи з середини минулого століття, багатьма науковцями, такими як Блейхут Р. (Blahut R.) [1], Гасфілд Д. (Gusfield D.), Селтон Г. (Salton G.), Укконен Е. (Ukkonen E.) [5] та іншими. Питання метрики текстів і дистанції між текстами вивчали Левенштейн В. І. [2], Дамерау Ф. (Damerau F.) [3], Хемінг (Hamming), Вагнер Р. (Wagner R. A.), Фішер М. (Fischer M. J.) [6] та інші.

Під метрикою текстів при цьому мається на увазі функція відстані між двома словами в певному просторі, яка дозволяє оцінити ступінь їх схожості. Строге математичне визначення ме-

трики включає в себе необхідність відповідати умові нерівності трикутнику. Між тим, у більшості випадків під метрикою розуміють більш загальне поняття, що не вимагає виконання такої умови, і це поняття має назву дистанції.

Обчислення схожості строк (або послідовностей символів) є частковим випадком визначення схожості об'єктів, а відтак – частиною задачі пошуку нечітких дублікатів. Як правило, оцінка схожості оперує чисельними показниками в діапазоні від 0 до 1, де 0 означає абсолютну несхожість, а 1 – повне співпадіння дублікатів. При цьому, на практиці використовується низка коефіцієнтів схожості: Серенсена (Sörensen) [4], Жаккара (Jaccard), Кульчинського (Kulczinsky), Отіаі (Ochiai), Шимкевича-Симпсона (Szymkiewicz, Simpson), Браун-Бланке (Braun-Blanquet) тощо.

Одним із наукових завдань автоматизованої обробки неструктурованих текстів є обґрунтування такого методу визначення схожості між послідовностями символів, який залежав би від схожості цих послідовностей з точки зору сприйняття їх людиною.

Інтуїтивно зрозуміло, що людина співвідносить окрему (відірвану від контексту) послідовність символів з одним із відомих слів, комбінацією слів або частиною більшого слова на підставі аналізу співпадіння їх символьно-позиційних характеристик: тобто, чим більше однакових символів знаходяться в однакових відносних позиціях (відносно інших символів у послідовності), тим більше схожі послідовності між собою з точки зору сприйняття їх людиною.

Для врахування символьно-позиційних характеристик при оцінці схожості послідовностей символів можна використовувати метод аналізу N-грам, з яких вони складаються. Сутність такого методу полягає у наступному.

Розглянемо послідовність символів $\overline{S}_1$ у вигляді $\overline{S}_1 = x_1 x_2 \ldots x_n$, що складається із n символів x_i у позиціях $i = 1, 2, \ldots, n$, а також послідовність символів $\overline{S}_2$ у вигляді $\overline{S}_2 = y_1 y_2 \ldots y_m$, що складається із m символів y_j у позиціях $j = 1, 2, \ldots, m$. Кожний символ x_i послідовності $\overline{S}_1$ і кожний символ y_j послідовності $\overline{S}_2$ належить до множини A певного алфавіту символів $A = \{a_1, a_2, \ldots, a_k\}$, $x_i \in A$, $y_j \in A$.

Кожну із заданих послідовностей $\overline{S}_1$, $\overline{S}_2$ можна уявити як сукупність окремих символів, а також як сукупність груп сусідніх символів (N-грам): по два символи (біграм), по три символи (три-

грам), і т.д. аж включно до N символів (N-грам), де $N = n$ для $\overline{S}_1$, $N = m$ для $\overline{S}_2$.

Так, перша послідовність $\overline{S}_1$ становить собою сукупність n символів $x_1, x_2, \ldots, x_n$, сукупність $n-1$ біграм $x_1x_2, x_2x_3, \ldots, x_{n-1}x_n$, сукупність $n-2$ триграм $x_1x_2x_3, x_2x_3x_4, \ldots, x_{n-2}x_{n-1}x_n$, і т.д. включно до 1 n-грами $x_1x_2\ldots x_n$, яка і є власне послідовністю $\overline{S}_1$. Друга послідовність $\overline{S}_2$ становить собою сукупність m символів $y_1, y_2, \ldots, y_m$, сукупність $m-1$ біграм $y_1y_2, y_2y_3, \ldots, y_{m-1}y_m$, сукупність $m-2$ триграм $y_1y_2y_3, y_2y_3y_4, \ldots, y_{m-2}y_{m-1}y_m$, і т.д. аж до 1 m-грами $y_1y_2\ldots y_m$, яка і є власне послідовністю $\overline{S}_2$.

Якщо вважати окремі символи послідовності також одним із варіантів N-грами (а саме – монограмою), то загальну кількість усіх можливих варіантів N-грам для послідовності символів довжиною n можна визначити як $(n^2+n)/2$, оскільки кількості різних варіантів N-грам для цієї послідовності утворюють числовий ряд $n, n-1, n-2, \ldots, 3, 2, 1$. Відтак, послідовність $\overline{S}_1$ має $(n^2+n)/2$ варіантів N-грам, а послідовність $\overline{S}_2$ має відповідно $(m^2+m)/2$ варіантів N-грам.

Наприклад, оберемо для оцінки схожості двох послідовностей символів коефіцієнт схожості Серенсена, який визначається як:

$$K = \frac{2c}{a+b},$$

де: a – кількість елементів в першому наборі, b – кількість елементів в другому наборі, c – кількість спільних елементів для першого и другого набору, K – коефіцієнт схожості Серенсена.

Тоді схожість σ послідовностей $\overline{S}_1$ і $\overline{S}_2$ на підставі коефіцієнту схожості Серенсена можна охарактеризувати як відношення кількості їх N-грам, що співпадають між собою, до загальної кількості N-грам в обох послідовностях:

$$\sigma_{S_1S_2} = 2q : \frac{n^2+n+m^2+m}{2} = \frac{4q}{n^2+n+m^2+m},$$

де q – кількість спільних пар N-грам для обох послідовностей.

Наприклад, розглянемо схожість послідовностей символів “ТЕКСТ” і “ТЕСТ”. Перша послідовність утворює сукупність з 15 N-грам: “Т”, “Е”, “К”, “С”, “Т”, “ТЕ”, “ЕК”, “КС”, “СТ”, “ТЕК”, “ЕКС”, “КСТ”, “ТЕКС”, “ЕКСТ” і “ТЕКСТ”. Друга послідовність утворює сукупність з 10 N-грам: “Т”, “Е”, “С”, “Т”, “ТЕ”, “ЕС”,

“СТ”, “ТЕС”, “ЕСТ” і “ТЕСТ”. Як видно, 6 пар N-грам в обох послідовностях спільні: “Т”, “Е”, “С”, “Т”, “ТЕ”, “СТ”. Тоді схожість зазначених послідовностей дорівнює:

$$\sigma(TEKCT, TECT) = \frac{4 \times 6}{5^2 + 5 + 4^2 + 4} = 0{,}48$$

Вочевидь, що у випадку, коли обидві послідовності повністю співпадають, їх схожість σ завжди дорівнює 1. Коли в обох послідовностях немає навіть жодного спільного символу, їх схожість завжди дорівнює 0.

Частковими випадками оцінки схожості послідовностей символів методом аналізу N-грам є оцінка з обмеженням максимальної довжини N-грами: біграмний метод (враховує лише збіг окремих символів і біграм), триграмний метод (враховує збіг окремих символів, біграм і триграм) тощо. При цьому, монограмний метод (який враховує лише збіг окремих символів) не розглядається, оскільки він нечутливий до порядку слідування символів у послідовності.

Отже, запропонована інтерпретація схожості послідовностей символів враховує не тільки кількісне співпадіння символів, з яких складаються послідовності, але й також співпадіння порядку слідування цих символів, при цьому враховуються не абсолютні, а саме відносні позиції символів. Наприклад, в послідовностях “ТЕКСТ” і “ПІДТЕКСТ” жоден із символів не співпадає за своєю абсолютною позицією у послідовностях, в той час як схожість послідовностей, оцінена за методом аналізу N-грам, сягає значення 0,588, головним чином із-за наявності спільного фрагменту.

Важливим недоліком для практичного використання зазначеної міри схожості послідовностей символів в контексті вирішення завдань з автоматизованої обробки неструктурованих текстів є неможливість уникнути повного перебору словника і подальшого сортування результатів для встановлення кожного разу найбільш імовірних еквівалентів словникових статей для заданого текстового фрагменту.

Література

1. Блейхут Р. Теория и практика кодов, контролирующих ошибки: Пер. с англ. — М.: Мир, 1986. — 576 с.

2. Левенштейн В. И. Двоичные коды с исправлением выпадений, вставок и замещений символов / Докл. Академий Наук СССР, 1965. С. 845-848. [т.163.4]

3. Damerau F. A. Technique for Computer Detection and Correction of Spelling Errors // Communications of the ACM. 1964. Vol. 7. No. 3. P. 171-176

4. Sörensen T. A method of establishing groups of equal amplitude in plant sociology based on similarity of species content // Kongelige Danske Videnskabernes Selskab. Biol. krifter. Bd V. № 4. 1948. P. 1-34.

5. Ukkonen E. Algorithms for Approximate String Matching // Information and Control. 1985. No. 64. P. 100 - 118.

6. Wagner R. A., Fischer M. J. The String-to-string Correction Problem // Journal of ACM. 1974. Vol. 21. No. 1. P. 168 - 173

УДК 005.3

Селіна М. Б.
Національна академія СБ України

ЩОДО ЗАРОДЖЕННЯ ТА РОЗВИТКУ ФОРМ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ ЯК ЕЛЕМЕНТІВ СПЕЦІАЛЬНОЇ ІНФОРМАЦІЙНОЇ ОПЕРАЦІЇ

На сучасному етапі розвитку суспільства з‘явилися нові форми протистояння та протиборства між країнами. Найбільш новітньою формою конфронтації стали т.зв. гібридні війни, у яких ключова роль віддається інформаційній складовій. На користь цього свідчить досвід останніх конфліктів, значна кількість яких перейшла з суто збройного протиборства в інформаційний простір, що став новим «полем» протистояння. Це пов’язано з тим, що роль інформаційних технологій та засобів масової інформації значно збільшилася і вони стали ключовим засобом досягнення військово-політичних цілей різних держав, а інформація – зброєю, яка не наносить фізичної шкоди, проте може стати «детонатором» для початку значних деструктивних процесів у суспільстві, у тому числі відправною точкою початку збройного протистояння. Розуміючи це, керівництво більшості розвинених країн світу використовують спеціальні органи, сили та засоби для проведення спеціальних інформаційних операцій (далі – СІО), головною метою яких є здійснення морально-психологічного впливу на населення, у т.ч. збройні сили противника, а також на вище керівництво держав. Незважаючи на те, що поняття «спеціальні інформаційні операції» вперше з‘явилося у 90-х роках минулого

сторіччя [1], а в Україні стало поширеним лише останнім часом і, для переважної більшості пересічних громадян України, пов‘язано з агресією Російської Федерації проти нашої країни, воно не є винаходом сьогодення. Зокрема, такі форми інформаційно-психологічного впливу (ІПВ) як дезінформація, пропаганда, залякування, які є елементами СІО, мають дуже давню історію. Їх зародження почалось у глибокий давнині одночасно з виникненням збройного протистояння, як складова частина збройної боротьби у вигляді психологічного засобу ослаблення бойового духу супротивника та підняття бойового духу власних сил. З розвитком та удосконаленням інформаційних технологій розвивались та удосконалювалися і форми ІПВ. Так, відповідно до виду носіїв інформації та способу її розповсюдження можна виділити чотири етапи розвитку цих форм: вербальний, паперовий, технічний та телекомунікаційний.

На першому етапі у якості основного носія та розповсюджувача інформації виступала людина. Способи розповсюдження інформації обмежувалися вербальними технологіями, а саме виступами ораторів, релігійних діячів, розповсюдженням чуток, а також використанням наочних засобів залякування.

На цьому етапі почалося залякування противника власною бойовою міццю (іноді уявною), застосування дезінформації, використання пропагандистських написів на камінних, деревах та будівлях. Відомості про перші спроби здійснення інформаційних операцій, а саме використання форм ІПВ містяться у стародавніх літописах, релігійній, філософській літературі та ін. Зокрема, про залякування згадується у Біблії, де розповідається історія Гедеона, який так залякав супротивника, що той розгубився і вдарив по своїх військах [2 – с.238].

У Стародавньому Китаї пропаганда, залякування та дезінформація застосовувалися в політиці та військовій діяльності. Зокрема, у «Трактаті про військове мистецтво» китайського полководця Сунь-цзи, який можна назвати однією з перших робіт з проведення інформаційних операцій [3 - с. 8-10], наголошується на необхідності психологічної обробки власних населення і війська з метою досягнення єдності в суспільстві, здійснення інформаційних диверсій для розладнання військових союзів ворожої держави з іншими державами [4- с.8-9], дезінформації противника тощо.

Дезінформація та пропаганда широко застосовувалися в Стародавній Греції та Римі. Класичним прикладом дезінформації є «троянський кінь», який зіграв вирішаючу роль у троянській війні, а вираз «троянський кінь» наразі у колі професійних розвідників використовується для позначення операцій по дезінформації противника з подальшою його поразкою.

Значний внесок у розвиток інформаційних операцій зробили араби часів Халіфату і татаро-монголи. Зокрема, Чингізхан та Батий широко застосовували дезінформацію противника та негативну пропаганду.

Із збільшенням грамотності населення почався «паперовий» етап, який характеризувався розповсюдженням листування, початком друкування книг, газет та ін. У цей же період з'явився ефективний засіб для розповсюдження пропагандистських матеріалів чи дезінформації - листівка.

Значних результатів щодо вдосконалення засобів впливу на ворога досягли в Ордені єзуїтів у першій половині XVI ст., де вперше започаткували використання листівок, лозунгів та організували фахову підготовку членів ордену, яким доручалася справа дискредитації противника у воєнні та мирні часи.

Форми ІПВ продовжують широко використовуватися і у війнах Середньовіччя, для чого почали застосовуватися друковані ілюстровані «інформаційні» листівки. У цей же період Н.Макіавелі у творі «Государь» значну увагу приділяє проблемам інформаційного впливу на підданих та противників, ретельно розглядає питання доцільності акцій залякування та демонстрації правителем різних чеснот як необхідної сторони політичної діяльності [5].

Поворотним моментом у історії інформаційних операцій став винахід друкарського станку та удосконалення видавничої справи. Книгодрукування і поява публічного друкованого інформаційного видання – газети, створили необмежені можливості для використання форм ІПВ не лише у військовій сфері, а й майже в усіх сферах суспільного життя. На даному етапі одна з ключових ролей у розвитку інформаційних операцій у військових умовах належить Наполеону Бонапарту, бойовим операціям якого передувало розповсюдження чуток про значну чисельну перевагу його військ, після чого розповсюджувалися памфлети та листівки. Для цього в армії Наполеона використовувалася походна типо-

графія з комплектом іноземних шрифтів. Наполеон вважав, що чотири газети в змозі завдати більше шкоди, ніж стотисячна армія та часто використовував газети з метою дезінформації [6, с.118-122].

Пропаганду та дезінформацію противника успішно використовували багато монархів та полководців того часу. Про використання інформації для досягнення поставленої мети під час війни свідчать твори та діяльність Клаузевіца, Жофа, Суворова, Кутузова, Мілютіна, Міхневича та інших [7, с.64].

З середини XIX ст. винахід нових носіїв інформації – фотографії та наступне відкриття електрики і нових засобів розповсюдження інформації – телеграфу, телефону, радіо, кіно, а пізніше телебачення дав поштовх початку третього «технічного» етапу розвитку та удосконаленню форм ІПВ. На цьому етапі значно посилилася наочність та образність засобів інформаційного впливу, збільшились можливості накопичення та зберігання інформації будь-якого об'єму. Стало можливим здійснення масового інформаційного впливу на населення різних країн світу. Можна стверджувати, що саме цей етап став переламним у розвитку та удосконаленні форм ІПВ. На цьому етапі відбувся перехід із суто військового використання форм ІВП у політичну площину. Поворотним пунктом у розвитку інформаційних операцій стала Перша світова війна, під час якої сторони намагалися вплинути на перебіг конфлікту за допомогою інформації та медіа. При штабах армій створювалися відповідні відділи й підрозділи, які організовували «війну слів» — агітацію супротивника. Пропаганда серед війська і населення противника з випадкової зброї перетворилася на один з провідних військових інструментів.

Розвиток науки та техніки у XX ст. дозволив значно удосконалити технологічну основу для проведення інформаційних операцій, що зробило їх одним з найефективніших засобів досягнення зовнішньо та внутрішньополітичних цілей. Вже у 20-х рр. США вели радіопередачі на регіони своїх «традиційних інтересів» країни Латинської Америки. Великобританія — на свої колонії. Німеччина, яка домагалася перегляду умов Версальського миру — на німців Померанії і Верхньої Сілезії у Польщі, Судетів у Чехії. Тоді ж, у 30-х рр., інформаційні операції перестають бути додатком до збройних конфліктів і перетворюються у самостійне

явище — як от: німецько-австрійська радіовійна 1933-34 рр. з приводу приєднання Австрії до рейху [8].

Під час Другої світової війни ворогуючи сторони активно застосовували такі самі методи інформаційних операцій, що і під час Першої світової війни. З кінця 40-х до середини 80-х р.р. у світі відбулося чимало військових конфліктів – в Кореї, В‘єтнамі, Афганістані, військові операції проти Іраку тощо, в яких також активно застосовувалися форми ІВП.

Проте події в Перській затоці в січні 1991 р., Югославії у 1999 р., перша і друга "чеченські кампанії" в Росії, і звісно «гібридна війна» на території нашої країни внесли нові риси в уявлення про засоби та методи війни у сучасному інформаційному суспільстві. Так, з розвитком сучасних телекомунікаційних технологій, які розпочались з появою персональних комп‘ютерів та відкритих телекомунікаційних мереж, стартував четвертий «телекомунікаційний» етап, який вивів форми ІПВ на новий рівень. На сучасному етапі в якості основного носія інформації стали виступати комп’ютерні носії, а головним засобом доведення інформації до суб‘єкта – телекомунікаційні мережі. Стало можливим здійснення прихованого інформаційного впливу як на конкретного користувача комп‘ютерної мережі, так і на широку аудиторію глобальних відкритих телекомунікаційних комп‘ютерних мереж. Як наслідок значно розширено можливості здійснення СІО, які дійсно стали потужною зброєю сучасності та дають змогу суб‘єктам їх проведення підготувати грунт для забезпечення власних військово-політичних та інших інтересів як на території чужих держав, так і своїх. У цьому контексті, вивчення та дослідження історичного досвіду використання форм ІВП у конфліктах дає можливості виявити основні закономірності інформаційної складової збройної боротьби, які притаманні і сучасним локальним конфліктам, дозволяє зрозуміти логіку становлення форм інформаційно-психологічних впливів як самостійного засобу досягнення військово-політичних задач. Що у свою чергу дає можливості не лише організувати заходи з протидії антиукраїнським СІО, а дозволяє здійснити ефективне проведення СІО в інтересах України.

Література

1. Гриняев С. Взгляды военных экспертов США на ведение информационного противоборства [Електронний ресурс] / С. Гриняев // Зарубежное военное обозрение. – 2001. – Режим доступу до ресурсу: http://psyfactor.org/infowar1.htm.
2. Библия – Москва, 2002. – 1376 с..
3. Информационно-психологическая безопасность в епоху глобализации: Учебное пособие / [В. М. Петрик, В. В. Остроухов, А. А. Штоквиш та ін.]. – Киев, 2008. – 543 с.
4. Сучасні технології та засоби маніпулювання свідомістю, ведення інформаційних війн і спеціальних інформаційних операцій: Навчальний посібник / [В. М. Петрик, В. В. Остроухов, О. А. Штоквиш та ін.]. – Київ, 2006. – (Росава).
5. Макиавели Н. Государь / Николло Макиавели. – Москва: Планета, 1990. – 79 с.
6. Інформаційна безпека держави: Підручник / [В. М. Петрик, М. М. Присжнюк, Д. С. Мельник та ін.]. – Київ: ДНУ "Книжкова палата України", 2016. – 264 с.
7. Історія інформаційно-психологічного протиборства: Підручник / [Є. Д. Скулиш, Я. М. Жарков, Л. Ф. Компанцева та ін.]. – Київ: Науково-видавничий відділ Національної академії СБ України, 2012. – 209 с.
8. Манойло А. В. ГОСУДАРСТВЕННАЯ ИНФОРМАЦИОННАЯ ПОЛИТИКА В ОСОБЫХ УСЛОВИЯХ: Монография [Електронний ресурс] / А. В. Манойло // МИФИ,. – 2003. – Режим доступу до ресурсу: http://www.evartist.narod.ru/text24/0022.htm.

УДК 005.3

Сластіна О. В.
Національна академія СБ України

СУЧАСНІ ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ УКРАЇНИ З БОКУ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ

В сучасних умовах важливого значення набувають проблеми інформаційно-психологічної безпеки особистості і суспільства, адже інформаційна безпека України протягом останніх років знаходиться під впливом Російської Федерації, яка здійснює проти України інформаційну війну. Ця війна розпочалася не як супровід анексії АР Крим та не як протидія Майдану, вона відбувається упродовж усіх років незалежності України. РФ

здійснює цілеспрямований негативний інформаційно-психологічний вплив на Україну з огляду на власні короткострокові чи стратегічні інтереси. Основним же пріоритетом для російського керівництва є перерозподіл та посилення свого політичного й економічного впливу у світі, насамперед у спосіб забезпечення відновлення домінуючих позицій на пострадянському просторі із залученням України до сфери свого геополітичного впливу.

Аналіз негативних інформаційно-психологічних впливів, які здійснює РФ у межах довготривалої інформаційної кампанії проти України впродовж останніх років, дає змогу виокремити такі їх основні напрями, що зачіпають основні сфери національної безпеки України та становлять загрозу національним інтересам:

• у зовнішньополітичній сфері – перешкоджання євроінтеграції України у спосіб формування упередженого ставлення світової спільноти до української влади, поширення недостовірної, неповної та викривленої інформації про Україну;

• у внутрішньополітичній сфері – формування образу ворога – українця серед російськомовних громадян України та росіян, а також спроби формування упередженого ставлення світової спільноти до патріотичних рухів в Україні у спосіб поширення викривленої, недостовірної та упередженої інформації щодо становища в Україні росіян та інших етнічних груп, статусу російської мови;

• у сфері державної безпеки – посягання на державний суверенітет і територіальну цілісність України у спосіб порушення питань про приналежність АР Крим, та формування «Новороссии» на Сході України;

• в економічній сфері – витіснення України зі світового та російського ринків у спосіб розповсюдження недостовірної інформації про якість окремих груп товарів чи низький рівень наукових розробок у певних галузях;

• у соціальній та гуманітарній сферах – протидія переосмисленню власної історичної спадщини, нівелювання українських культурних цінностей і формування проросійських настроїв у суспільстві у спосіб насаджування міфу про спільний «русский мир», заперечення існування окремої від росіян української нації з власною мовою, культурою та історією тощо.

Для досягнення своєї мети в інформаційній війні проти нашої держави РФ використовує весь наявний арсенал традиційних і сучасних методів впливу, до яких варто віднести використання пропаганди, агітації, тенденційної інформації, напівправди та відвертої неправди («фейку») [2, с. 23].

- пропаганда (скерована на всі верстви населення, прикладом слугує анімаційний фільм створений нібито дітьми, що втекли з Донбасу в РФ. Основним гаслом фільму є «Рятуйте людей Донбасу».);
- напівправда (інформаційні повідомлення під час анексії Криму, коли російські ЗМІ заявляли про масовий перехід українських силовиків на бік Росії або про добровільну здачу військових частин, складів, зброї, інших військових об'єктів російським військовим. Хоча таких випадків було значно менше);
- «фейк» (розтиражована російськими ЗМІ інформація про дитину, яку начебто розіп'яли українські військові на Донбасі; інформація подана через російські новини про створення Чорного моря украми вручну, відриванням; інформація, про канібалізм у Домі профспілок; інформація про вчителів Запорізької школи, що забороняють дітей годувати снігурів, що символізують РФ; інформація про українських військових, що вбивають мирне населення та ґвалтують жінок на блокпостах тощо);
- преса (а саме газети, українські версії російських видань, які поширювали матеріали, що пропагували російську доктрину, спрямовану на розвал України, такі як «Известия», «Коммерсантъ» тощо);
- радіомовлення (прикладом є радіостанція «Голос Росії», відома своєю антиукраїнською позицією, здійснювала своє мовлення на хвилях «Радіо Ера»);
- Інтернет (прикладом є соціальні мережі, де зяляється багато негативних коментарів про Україну. Зараз Інтернет є одним із найпотужніших засобів масової інформації, бо може замінти і телебачення, і радіо, і книжкову продукцію тощо);
- книжкова продукція (наприклад, твір М. Калашнікова «Независимая Украина. Крах проэкта» 2009 року, Г. Савіцького «Украина в крови. Бандеровский геноцид» 2014 тощо);
- кінопродукція (хороша постановка "Тараса Бульби", правда у ньому справжньої історії дуже мало, більшість перекручування фактів, провокування ідей "русского мира",

козаки вірні слуги московського царя (коли відбуваються події фільму поняття " Російська Імперія " не існувало в природі; серіал «Всі чоловіки – сво», фільм «Брат – 2»).

Через систему засобів інформації, кіно, радіо, телебачення, пресу, наочні засоби простежується використання опосередкованого навіювання, що здійснюється поза особистих контактів. У цьому випадку ефект навіювання залежить від авторитетності джерела і життєвої значущості інформації, які можуть викликати довіру і знизити опір впливу, який внушають. Навіювання цього виду досить ефективно використовується в практиці. На відміну від прямого, при непрямому навіюванні завжди вдаються до допомоги додаткового подразника. Словесної формули може не бути зовсім [2, с. 256].

Щодо найсвіжіших подій початку 2016 року, то він відзначився значним збільшенням активності Росії в інформаційній війні проти України, за рівнем абсурдності – безпрецедентним навіть за мірками Кремля.

Так, спочатку головний російський «інформаційний боєць» – телеканал Life news повідомив, що ФСБ РФ отримала інформацію про підготовку терористичних нападів з боку ІДІЛ в місцях масового скупчення людей в Києві. Більше того ФСБ встановило десять осіб потенційних терористів, дані про яких буцімто були передані до СБУ. Реакція СБУ була короткою і виваженою – суха констатація того, що не існує жодних контактів с ФСБ, а даний посил – чергова підробка. «Сенсація» навіть залишилася майже поза увагою українських ЗМІ…

Далі, буквально за декілька днів британське видання The Independent опублікувало матеріал, в якому лейтмотивом стало планування Україною відправки військ в Сирію. При цьому наводиться «анонімне джерело з Міністерства оборони України». За даними газети, Київ готується відправити військовий контингент до Сирії для підтримки Заходу в боротьбі з ІДІЛ. Плюс один із мотивів є можливість зіткнутися з російськими військами, тому що українці зараз найкращі у світі «у знанні тактики і мови росіян» , – вище за The Independent. На відміну від попередньої новини, дана «сенсація» мала певний резонанс в Україні. МО України, звичайно, заперечило наведені «одкровення». Також було привернуто увагу, що The Independent належить російському олігархові Олександру Лєбєдєву, що має

вагомі частки в таких гігантах російського бізнесу як РАО ЄЕС «Россия» і «Аэрофлот» [3].

Таким чином, аналізуючи наявні загрози, нині назріла нагальна потреба в переосмисленні на державному рівні проблеми забезпечення інформаційно-психологічної безпеки та налагодження дієвого внутрішньодержавного та зовнішнього інформування. Також вбачається за доцільне:

• на концептуальному рівні – розробити й затвердити відповідні керівні документи державної політики: Стратегію інформаційно-психологічної безпеки;

• на інституційному рівні – утворити Координаційний центр з питань інформаційно-психологічної безпеки;

• на законодавчому рівні – внести зміни до чинного законодавства для захисту українського інформаційного простру від розповсюдження кіно-, аудіо-, книжкової та іншої інформаційної продукції антиукраїнського змісту у спосіб визначення загальних критеріїв віднесення таких творів до заборонених для розповсюдження в нашій державі.

Література

1. Конах В. К. Негативні інформаційно-психологічні впливи Російської Федерації проти України та можливі засоби протидії / Вікторія Костянтинівна Конах. // Стратегічні пріоритети. – 2014. – №3. – С. 23.

2. Потеряхіна А. Л. Психологія управління / А. Л. Потеряхіна. – Київ: Астропринт, 1999. – 432 с.

3. Кост П. «Російській «відчай». Чим викликана остання агонія кремля в інформаційній війні» [Електронний ресурс] / Павло Кост. – 2016. – Режим доступу до ресурсу: http://defence-ua.com/.

УДК 342.9

Старенький М. І.
Львівський державний університет безпеки життєдіяльності
Полотай О. І.
кандидат технічних наук
Львівський державний університет безпеки життєдіяльності

ДО ПРОБЛЕМИ ПІДГОТОВКИ ФАХІВЦІВ ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

В наш час швидкими темпами почали розвиватись комп'ютерні технології та інформаційний простір. Мережа Інтернет в наш час є доступною для будь-якого користувача, практично кожен має інформацію яка зберігається на віддалених серверах, здійснює електронні платежі, це все стало невід'ємною частиною нашого сьогодення. Зважаючи на розвиток та важливість документів, котрі зберігаються в глобальній мережі, збільшилось число спроб несанкціонованого заволодіння конфіденційною інформацією. Унаслідок цього процесу, все більш гостро постає питання захисту інформації, відбір та підготовку фахівців в галузі «інформаційна безпека».

В Україні є документи, котрі регламентують питання інформаційної безпеки: Концепція Національної безпеки України та Концепція технічного захисту інформації в Україні. Дані документи стали підставою для визначення основних принципів та напрямків державної політики у сфері інформаційної безпеки. Дані документи містять головні проблеми, котрі постали, та можливі шляхи та засоби їх вирішення. Все це потребує професійних кадрів, що у свою чергу передбачає відповідну систему підготовки фахівців у даній галузі.

Через відсутність в державі чіткої стратегії, підготовка кадрів для галузі інформаційної безпеки практично не має попиту. В даній ситуації має місце лише створення окремих елементів, котрі не завжди є правильними. Враховуючи базу різноманітних технічних вищих навчальних закладів (ВНЗ), навчання спрямоване на технічні й технологічні аспекти захисту інформації. Якщо ж брати до уваги юридичні ВНЗ, там навчання проходить лише з

посиленим вивченням організаційно-правових аспектів інформаційної безпеки.

Всі ці проблеми можна вирішити, адже в наш час є значна кількість вузів, що надають «подвійну» освіту. Кожен з випускників має базовий рівень знань в тій чи іншій сфері, володіє іноземною мовою та його подальше життя неможливе без використання комп'ютера. Якщо ж говорити про інформаційну сферу, то прикладом може стати факультет управління та інформатики Національного університету внутрішніх справ України, де по закінченню навчання студентам видаються два дипломи державного зразка – юриста-правознавця та фахівця в галузі інформаційних технологій.

Кожному відомо, що головною проблемою навчального процесу є правильне та ефективне проведення занять з метою підвищення їх ефективності. Важливу роль в цьому відіграє мотивація слухачів [2]. Згідно з опитуваннями, котрі були проведені у різноманітних вузах за напрямом підготовки фахівців з інформаційної безпеки було виявлено, що значна більшість студентів, котрі знаходяться на навчанні виявили бажання вступити на дану спеціальність з метою вивчення тонкощів злому різноманітних мереж. Відповідно значно менша частина, прагне навчитись захищати мережу від всіх потенційних загроз.

Опираючись на результати опитування, можна з впевненістю сказати, що більшість майбутніх фахівців схильні до прихованої злочинності в галузі інформаційних технологій. Виникає наступне питання: Кого власне готують більшість ВНЗ – фахівців із захисту інформації чи навпаки, комп'ютерних злочинців?

Таким чином, підготовка фахівців в нашій державі є ще далекою від ідеалу та потребує значної кількості корегувань та доповнень. Найбільш вагоме значення в процесі навчання та підготовки фахівців має виховання високих моральних цінностей. Як правило, найбільшою загрозою не зважаючи на використання новітніх технологій в наш час залишається людський фактор [1].

Авторами даних соціологічних опитувань були винесені наступні висновки: проблема людського фактору слід вирішувати у двох напрямках: більше уваги приділяти конкурсному відбору при наборі фахівців та оптимізація виховної роботи в процесі навчання [3].

Також окрім головної проблеми існує ряд другорядних, а саме: низький рівень професійної підготовки керівників та спів-

робітників. Одним з шляхів подолання даної проблеми є проведення переатестації всього складу, котрий має безпосереднє відношення до навчання майбутніх фахівців.

Отже, на даному етапі розвитку комп'ютерних технологій в Україні є значний ряд проблем, проте, не враховуючи всі неблагополучні аспекти розвитку фахівців інформаційної безпеки, слід зазначити, що також є і позитивні моменти: наявність досить потужних центрів та вищих навчальних закладів, котрі здійснюють спеціалізовану підготовку фахівців, тісна взаємодія з іншими країнами, використання їх досвіду та наявність програм, в основі яких є обмін студентами. Саме ці аспекти та вирішення проблем описаних вище можуть допомогти нашій державі вийти на вищий рівень захисту інформації та підготовки висококваліфікованих фахівців у даній сфері діяльності.

Література

1. Юдин О.К. Концепция подготовки специалистов в области информационной безопасности (часть 1). [Електронний ресурс]. – Режим доступу з http://itiss.info/publishing/experts-articles/48-yudin/ 127-koncepciya-podgotovki-specialistov-v-oblastiinformacionnoi-bezopasnosti-chast-1

2. Закон України "Про Концепцію Національної програми інформатизації". [Електронний ресурс]. – Режим доступу з http://zakon2.rada.gov.ua/laws/show/75/98-вр

3. Постанова Кабінету міністрів України № 787 від 27.08.2010 р. "Про затвердження переліку спеціальностей, за якими здійснюється підготовка фахівців у вищих навчальних закладах за освітньо-кваліфікаційними рівнями спеціаліста і магістра".

УДК 342.72/.73

Тугарова О. К.
кандидат юридичних наук
Національна академія СБ України
Курінська Я. В.
Національна академія СБ України

ПОНЯТТЯ ПРОФЕСІЙНОЇ ТАЄМНИЦІ В ЗАКОНОДАВСТВІ УКРАЇНИ

Закон України «Про доступ до публічної інформації» закріплює вичерпний перелік інформації з обмеженим доступом: кон-

фіденційна інформація, службова інформація і таємна інформація. Особливе місце серед існуючих видів посідає професійна таємниця, яка відповідно до ч.1 ст.6 Закону є видом таємної інформації [1].

У вітчизняному законодавстві чітко не визначено поняття «професійної таємниці», не врегульовані її ознаки та види. Проте, визначення змісту поняття «професійна таємниця», окреслення її суттєвих ознак є необхідною передумовою формування механізму охорони інформації та захисту легітимних інтересів особи у цивілізованому суспільстві.

Дослідженням питання професійної таємниці у різні часи займалися Б.А. Кормич, П.В. Макалінський, В.Н. Лопатін, М.А. Федотов, О.Д. Святоцький, М.М. Михеєнко та інші. Вони сформулювали низку важливих положень, які продуктивно використовувалися в науці протягом тривалого часу. Але, проблема визначення характерних ознак професійної таємниці, з'ясування її співвідношення з іншими видами інформації з обмеженим доступом й досі залишилися не до кінця вирішеними у сучасному законодавстві, що ускладнює реалізацію відповідних нормативних положень на практиці.

Аналіз законодавчих положень вітчизняного законодавства засвідчив, що розкриття терміну «професійна таємниця» раніше містилося у двох нормативно-правових актах. Закон України «Про фінансові послуги та державне регулювання ринків фінансових послуг» визначив професійну таємницю як матеріали, документи, інші відомості, якими користуються в процесі та у зв'язку з виконанням своїх посадових обов'язків посадові особи державних органів, що здійснюють регулювання ринків фінансових послуг, та особи, які залучаються до здійснення цих функцій, і яким забороняється розголошувати у будь-якій формі до моменту прийняття рішення відповідним уповноваженим державним органом (п.11 ст.1 Закону). Подібне визначення містилося в Законі України «Про Рахункову палату», який ототожнював професійну таємницю із станом збереження матеріалів, документів, інших відомостей, якими користуються посадові особи Рахункової палати та особи, які залучаються до здійснення функцій Рахункової палати під час проведення перевірок, ревізій, обслідувань, і про які забороняється розголошувати у будь-якій формі до моменту прийняття рішення Рахункової палати (ст.20 Закону).

Аналіз нормативних приписів зазначених вище джерел засвідчив, що зміст поняття “професійна таємниця” раніше охоплював інформацію, яка стає відомою органам регулювання ринків фінансових послуг та Рахунковій палаті у ході здійснення їхніх службових або посадових обов’язків. Проте, така інформація є службовою, оскільки стосується реалізації напряму роботи цих органів і втрачає свій статус з моменту прийняття рішення з відповідного питання. Захист такої інформації повинен здійснюватися відповідно до положень про службову інформацію, як різновиду інформації з обмеженим доступом (на сьогодні вище зазначені норми не є чинними; Закон України «Про внесення змін до деяких законодавчих актів України у зв’язку з прийняттям Закону України», «Про інформацію» та Закону України «Про доступ до публічної інформації» виключив зазначені норми з вітчизняного законодавства [2]).

Вивчення положень Закону України «Про доступ до публічної інформації», Закону України «Про інформацію» та інших наукових джерел дає можливість визначити ознаки професійної таємниці як окремого виду інформації з обмеженим доступом.

До таких ознак належать наступні:

1) інформація, що становить зміст професійної таємниці, є інформацією з обмеженим доступом, і довірена або стала відомою особі виключно через виконання нею своїх професійних обов’язків;

2) особа, якій довірено інформацію, не перебуває на державній службі, у протилежному випадку – таку інформацію слід вважати службовою таємницею;

3) поширення інформації може зашкодити правам або легітимним інтересам конкретної особи, визначеної законом.

У сучасній науці традиційно до видів професійних таємниць відносять адвокатську, лікарську, нотаріальну, аудиторську таємниці, таємницю сповіді та таємницю журналістських джерел. Спільним для них є вимога не розголошувати довірену інформацію особою, яка належить до певної професії.

Крім того, чинним законодавством, встановлюється додаткові гарантії захисту від стороннього доступу до такої інформації, несанкціонованого (дозволеного) її власником. Це, наприклад, нормативні заборони щодо неможливості допиту в якості свідків адвокатів, нотаріусів, лікарів, психологів, священнослу-

жителів, якщо вони не звільнені від обов'язку зберігати професійну таємницю власником інформації (ст.65 КПК України) [3].

З урахуванням зазначених ознак, поняття «професійна таємниця» можна сформулювати наступним чином. Професійна таємниця – це інформація обмеженого доступу, що стала відомою або була довірена представнику певної професії через виконання ним своїх професійних обов'язків, неправомірне розголошення чи використання якої може спричинити настання негативних наслідків як для власника такої інформації, так і для її володільця, якому вона була довірена згідно закону.

Важливим для забезпечення інтересів фізичних та юридичних осіб у сучасному законодавстві є визначення правового механізму охорони інформації, що стає відомою особам внаслідок здійснення певної професійної діяльності на рівні спеціалізованого законодавства в сфері інформації з обмеженим доступом. Розробка та прийняття спеціального закону дозволить більш чітко врегулювати відносини між суб'єктами, що здійснюють певну професійну діяльність (володільці інформації), та їх клієнтами (власники інформації), які довіряють важливі для них відомості.

На сьогодні, нажаль, переважна кількість науковців схильна до простого перерахування різновидів професійних таємниць, ніж до пошуку підстав для розробки їх класифікації. Тому критичне осмислення проблеми класифікації професійних таємниць потребує діалектичного підходу до розуміння сукупності суспільних відносин, що виникають з приводу збереження певної інформації, яка стає предметом професійної таємниці.

Література

1. Закон України «Про доступ до публічної інформації» від 13.01.2011 [Електронний ресурс]. Режим доступу: http://zakon3.rada.gov.ua

2. Закон України «Про внесення змін до деяких законодавчих актів України у зв'язку з прийняттям Закону України», «Про інформацію» та Закону України «Про доступ до публічної інформації» від 27.03.2014 [Електронний ресурс]. Режим доступу: http://zakon3.rada.gov.ua

3. Кримінальний процесуальний кодекс України від 13.04.2012 [Електронний ресурс]. Режим доступу: http://zakon0.rada.gov.ua

УДК 342.727

Тугарова О. К.
кандидат юридичних наук
Національна академія СБ України
Шайкова М. А.
Національна академія СБ України

ПРОБЛЕМНІ ПИТАННЯ ЗАПРОВАДЖЕННЯ ІНСТИТУТУ ВИКРИВАЧІВ ІНФОРМАЦІЇ В УКРАЇНІ

Прийнятий у 2011 році Закон України «Про доступ до публічної інформації» запровадив важливий принцип свободи інформації - захист особи, яка розкриває відомості, що становлять суспільний інтерес. Такі особи в міжнародному праві отримали назву «викривачів («whistleblowing») інформації».

У сучасному розумінні інформаторство (whistleblowing) — це доброчесне та правдиве повідомлення особи (інформатора) про будь-які зловживання або порушення, які можуть нанести шкоду правам і свободам громадян, інтересам держави чи суспільства в цілому [1].

Стаття 11 Закону України «Про доступ до публічної інформації» закріплює особливі гарантії захисту викривачів інформації , а саме: « посадові та службові особи не підлягають юридичній відповідальності, незважаючи на порушення своїх обов'язків, за розголошення інформації про правопорушення або відомостей, що стосуються серйозної загрози здоров'ю чи безпеці громадян, довкіллю, якщо особа при цьому керувалася добрими намірами та мала обґрунтоване переконання, що інформація є достовірною, а також містить докази правопорушення або стосується істотної загрози здоров'ю чи безпеці громадян, довкіллю» [2]. Отже, держава на рівні законодавства гарантує особливий захист особи, яка в супереч своїм обов’язкам оприлюднює достовірну інформацію, що становить суспільній інтерес.

На сьогодні, значних успіхів у розвитку інституту інформаторства здобули такі країни як США, Південна Корея та Румунія. США відзначилася такими здобутками як: найкращий механізм, який гарантує захист викривачів інформації; наявність спеціалізованого закону «Про наклеп», який дозволяє громадянам подавати позов від імені керівництва про повернення коштів, викрадених через договірне шахрайство тощо.

Південна Корея надала широке поняття «інформатор»; розробила дієвий механізм конфіденційності викривачів інформації; запровадила матеріальну винагороду інформаторам, а також систему санкцій для тих, хто завдає негативні дії у відношенні до викривачів інформації; створила незалежний орган, що приймає заяви або повідомлення від викривачів інформації (у тому числі про репресії).

Румунія, у свою чергу, прийняла Закон «Про захист інформаторів»; створила механізм відмови держслужбовця або працівника виконувати розпорядження керівника, яке він вважає незаконним; зобов'язала державні органи розробити внутрішню політику про інформаторів; створила механізм захисту анонімності повідомлення.

Незважаючи на існуючий позитивний досвід зарубіжних країн, запровадження інституту викривачів інформації в Україні пов'язано із існуванням певних проблем. Одна з них проявляється у ставленні суспільства до викривачів інформації, оскільки на рівні масової свідомості цей інститут сприймається в основному негативно. Причиною цього стали соціальні стереотипи, які виникли в результаті історичного розвитку суспільства в умовах тоталітарного режиму правління, під час якого від дій інформаторів постраждала велика кількість людей. І на сьогодні ці спогади залишились у кожній сім'ї, тому інформаторство сприймається як ганебна дія, «стукацтво». Про це, зокрема, свідчать наступні дослідження проведені міжнародною організацією «Transparency International» [3].

Ще однією проблемою є те, що на сьогодні в Україні відсутній законодавчий акт, який би з повнотою визначив поняття «викривач інформації», закріпив дієвий механізм захисту таких осіб, починаючи з моменту повідомлення про факт скоєння правопорушення, визначив підстави звільнення особи від юридичної відповідальності тощо» [4].

Відповідно до Закону України «Про доступ до публічної інформації», підставами, що дозволяють звільнити особу від відповідальності є: обґрунтовані переконання та добрі наміри особи, достовірність інформації яку вона надає, докази правопорушення. В свою чергу зазначений перелік підстав не розкрито у законі, через що кожен може їх розглядати оціночно, з долею суб'єктивізму, що являється не допустимо в юриспруденції. Також в Законі відсутня вказівка щодо спеціального уповноваженого органу державної влади, до компетенції якого б відносилося прийняття повідомлень про факт скоєного правопорушення.

Необхідно зауважити і на тому, що в останні роки рівень довіри громадян до державних установ значно знизився. Підтвердженням цього слугують дані отримані під час проведення дослідження, яке організували Фонд «Демократичні ініціативи» ім. Ілька Кучеріва та соціологічна служба Центру Разумкова з 22-27 липня 2015 року. У ході опитування 2011 громадян з усіх регіонів країни (окрім Криму та районів Донбасу) були отримані наступні результати [4]:

Якою мірою Ви довіряєте наступним інституціям? (липень-2015)

	Зовсім не довіряю	Переважно не довіряю	Переважно довіряю	Цілком довіряю	Важко сказати	Баланс довіри-недовіри
Президентові України	33,3	29,2	25,8	3,7	8,0	-33,0
Верховній Раді України	44,4	34,0	13,6	1,9	6,2	-62,9
Уряду України	45,1	29,5	16,0	2,3	7,1	-56,3
Збройним Силам України	19,1	17,6	41,3	13,4	8,6	18,0
Службі безпеки України	32,7	28,7	23,7	3,6	11,3	-34,1
Місцевій владі	25,9	30,7	29,5	5,0	8,9	-22,1
Судам	51,4	28,8	10,4	2,4	7,0	-67,4
Прокуратурі	51,4	28,2	9,9	2,8	7,7	-66,9
Національній поліції	40,3	34,7	16,1	2,1	6,8	-56,8

Враховуючи отримані дані, можна констатувати, що у потенційного інформатора відсутнє бажання звертатися до відповідних органів з повідомленням, оскільки довіра до них є вкрай низькою.

Вбачається, що для забезпечення рівного та гарантованого захисту викривачам інформації в Україні, доцільно було б:

по-перше, прийняти спеціальний законодавчий акт, який би врегульовував всі актуальні питання, пов'язані з діяльністю інформаторів в Україні;

по-друге, запровадити обов'язковий курс лекцій з однакової тематики у державних установах, різної форми власності підприємствах, організаціях, ВНЗ, з метою зміни негативного ставлення до викривачів інформації.

Література

1. Ставлення до доброчесних інформаторів [Електронний ресурс] : www.iahr.com.ua/files/works_docs/120.pdf

2. Про доступ до публічної інформації: Закон України // Відомості Верховної Ради України (ВВР), 2011, № 32, ст. 314

3. Transparency International – це міжнародна недержавна організація по боротьбі з корупцією, яка має близько 100 національних осередків та відома своїми антикорупційними дослідженнями, зокрема Індексом сприйняття корупції [Електроний ресурс]. – Режим доступу : http://www.transparency.org/.

4. Ініціатива 11 [Електронний ресурс] : https://initziativa11.org/who-is-initiative-11/?lang=uk

УДК 343.131

Тугарова О. К.
кандидат юридичних наук, доцент
Національна академія СБ України
Набока А. Г.
Національна академія СБ України

ЗАБЕЗПЕЧЕННЯ ОХОРОНИ КОМЕРЦІЙНОЇ ТАЄМНИЦІ У ВІТЧИЗНЯНОМУ ЗАКОНОДАВСТВІ

Забезпечення інформаційної безпеки є однією з основних функцій цивілізованої, розвинутої і сильної держави. Необхід-

ність забезпечення інформаційної безпеки зумовлюється не лише потребою захищеності національної безпеки України в цілому, а й врахуванням того, що потенційні і реальні загрози в інформаційній сфері можуть впливати на зміну свідомості і поведінку людей та завдавати значну шкоду їх легітимним правам і інтересам.

Закон України «Про основи національної безпеки» серед загроз в інформаційній сфері виділяє розголошення інформації, яка становить державну таємницю, або іншої інформації з обмеженим доступом, спрямованої на задоволення потреб і забезпечення захисту національних інтересів суспільства і держави (ст.7 Закону) [1].

В системі інформації з обмеженим доступом особливе місце посідає інформація, що становить комерційну таємницю. Через високу прибутковість комерційна таємниця нерідко стає бажаним об’єктом протиправних дій і привертає до себе підвищену увагу злочинного світу. Саме тому охорона та захист інформації, що становить зміст комерційної таємниці, є пріоритетним напрямом вітчизняного кримінального судочинства.

Захист суспільних відносин у сфері обігу комерційної таємниці забезпечується, насамперед, нормами чинного кримінального законодавства. Кримінальний кодекс України (надалі – КК України) визнає злочинними, по-перше: умисні дії, спрямовані на отримання відомостей, що становлять комерційну або банківську таємницю, з метою розголошення чи іншого використання цих відомостей, а також незаконне використання таких відомостей (ст. 231 КК України); по-друге: умисне розголошення комерційної або банківської таємниці без згоди її власника особою, якій ця таємниця відома у зв'язку з професійною або службовою діяльністю, якщо воно вчинене з корисливих чи інших особистих мотивів (ст. 232 КК України) [2]. Аналогічні приписи містяться в Законі України «Про захист від недобросовісної конкуренції», нормами якого передбачена адміністративна відповідальність за неправомірне збирання комерційної таємниці, розголошення комерційної таємниці, схилення до розголошення комерційної таємниці, неправомірне використання комерційної таємниці (ст.ст. 16-19 Закону) [3]. Крім того, відповідальність за вчинення дій, що виражаються в отриманні, використанні, розголошенні комерційної таємниці, а також іншої конфіденційної інформації з метою

заподіяння шкоди діловій репутації або майну іншого підприємця передбачені ч.3 ст.164^3 Кодексу України про адміністративні правопорушення [4].

Проведений порівняльний аналіз норм чинного законодавства засвідчив, що основна відмінність кримінально-правового й адміністративно-правового захисту комерційної таємниці полягає у наслідках протиправних дій. Кримінальна відповідальність наступає виключно за умови заподіяння істотної шкоди суб'єкту господарської діяльності. Проте, на сьогоднішній день чинне законодавство не містить чіткого визначення розміру істотної шкоди суб'єкта господарювання, через що така важлива кваліфікуюча ознака стає оціночною категорією, не позбавленою елементів суб'єктивізму. Вбачається, що такою шкодою слід вважати:

- банкрутство підприємства;
- втрату прибутку у розмірі річного прибутку;
- ліквідацію або реорганізацію підприємства внаслідок протиправних дій конкурентної розвідки;
- втрату інтелектуального і кадрового потенціалу підприємства.

Можливо, що запропонований перелік не є повним, через що означена проблема може стати предметом подальших наукових дискусій і творчих пошуків сучасної вітчизняної науки.

Література

1. Про основи національної безпеки: Закон України від 19.06.2003 № 964-IV [Електронний ресурс]. – Режим доступу: htth://zakon.rada.gov.ua

2. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III [Електронний ресурс]. – Режим доступу: htth://zakon.rada.gov.ua

3. Про захист від недобросовісної конкуренції: Закон України від 07.06.1996 № 236/96-ВР [Електронний ресурс]. – Режим доступу: htth://zakon.rada.gov.ua

4. Кодекс України про адміністративні правопорушення: Закон України від 07.12.1984 № 8073-X [Електронний ресурс]. – Режим доступу: htth://zakon.rada.gov.ua

УДК 342.727: 341.645.5

Тугарова О. К.
кандидат юридичних наук, доцент
Національна академія СБ України
Овсянніков А. С.
Національна академія СБ України

ЗАБЕЗПЕЧЕННЯ ПРАВА НА ДОСТУП ДО ІНФОРМАЦІЇ В РІШЕННЯХ ЄВРОПЕЙСЬКОГО СУДУ З ПРАВ ЛЮДИНИ

Право на доступ до інформації є фундаментальним правом кожної людини, яке дістало визнання в багатьох нормативно-правових документах міжнародного і національного законодавства передових країн світу. В Україні право на доступ до інформації закріплено на рівні Основного Закону держави – Конституції України [1]. Стаття 34 Конституції гарантує право кожної особи на свободу думки і слова, на вільне вираження своїх поглядів і переконань, а також право на вільне збирання, зберігання, використання і поширення інформації усно, письмово або в інший спосіб – на свій вибір. Реалізація зазначеного права стає можливою за умови належного функціонування механізмів його захисту.

В системі захисту права на доступ до інформації важливу роль відіграють органи судової влади як національного, так і міжнародного рівня. Особливе місце в системі таких органів займає Європейський суд з прав людини (надалі - ЄСПЛ), який розглядає позови громадян різних країн щодо порушення прав і свобод, визначених у Конвенції про захист прав людини і основоположних свобод (надалі - Конвенція) [2].

Стаття 10 Конвенції гарантує право кожного на свободу ви вираження поглядів. Це право включає свободу дотримуватися своїх поглядів, одержувати і передавати інформацію та ідеї без втручання органів державної влади. Здійснення цих свобод, оскільки воно пов’язане з обов’язками і відповідальністю, може підлягати таким формальностям, умовам, обмеженням або санкціям, що встановлені законом і є необхідними в демократичному суспільстві в інтересах національної безпеки, територіальної цілісності або громадської безпеки, для запобігання заворушенням чи злочинам, для охорони здоров’я чи моралі, для захисту репутації чи прав інших осіб, для запобігання розголошенню

конфіденційної інформації або для підтримання авторитету і безсторонності суду.

Проведений аналіз практики ЄСПЛ засвідчив, що кількість позовів від українських громадян до зазначеної інституції Ради Європи зростає у кожного року. Адже в Україні майже не залишилося прав людини, які б не порушувалися. У європейських країнах також існують різноманітні порушення прав людини, але їхня кількість є дуже незначною порівняно з Україною. Згідно з даними, які подані на сайті ЄСПЛ, на стадії розгляду перебуває 16 тисяч 150 скарг від українських позивачів, що становить 19 % від кількості справ з усіх 47 країн. У цій статистиці Україна лідирує [3]. При цьому найбільша кількість порушень, встановлених рішенням ЄСПЛ проти України, становлять:

- право на свободу та особисту недоторканність (ст. 6 Конвенції);
- заборона катування (ст. 3 Конвенції);
- право на ефективний засіб правового захисту (ст. 13 Конвенції);
- захист власності (ст. 1 Першого протоколу до Конвенції) [4].

Разом з тим слід зазначити, що відсоток справ, пов'язаних з порушенням права на доступ до інформації є чи не найнижчим в Європі. Станом на 2015 рік в ЄСПЛ лише дев'ять справ стосувалися порушення зазначеного права. При цьому, незважаючи на існуючи прецеденти, судові справи здебільш стосувалися порушення права на таємницю листування, телефонних розмов телеграфної та іншої кореспонденції осіб, які перебували в місцях позбавлення волі (справи «Алієв проти України», «Данкевич проти України», «Кузнєцов проти України», «Полторацький проти України», «Хохлич проти України» тощо). Про що це свідчить? Недовіра населення міжнародним судовим інстанціям? Необізнаність населення щодо своїх прав? Недосконалість вітчизняного законодавства з приводу захисту права на доступ до інформації?

Вбачається, що відповідь на дані питання є очевидною. Утвердження верховенства права, останні позитивні зміни в українському суспільстві, активна діяльність вітчизняних і зарубіжних інституцій у дослідженні зазначеної проблематики постійно зменшують потребу в констатації ЄСПЛ фактів порушень права на доступ до інформації в Україні. Проте, вітчизняне законодавство, яке до речі, визнано одним з найкращих в Європі і посідає 9-те місце серед 89 країн світу, потребує постійного вдоскона-

лення. На наш погляд, гармонізації законодавства у сфері обігу інформації сприятимуть наукові розробки щодо визначення поняття суспільно-необхідної інформації, більш чіткого правового врегулювання алгоритму віднесення відомостей до категорії службової інформації, законодавчого врегулювання механізму захисту викривачів інформації.

Література

1. Конституція України: Закон України від 28.06.1996 № 254 к/96-ВР [Електронний ресурс]. – Режим доступу: htth://zakon.rada.gov.ua

2. Конвенція про захист прав людини і основоположних свобод: Міжнародний документ від 04.11.1950 [Електронний ресурс]. – Режим доступу: htth://zakon.rada.gov.ua

3. І.Беззуб. Національна стратегія у сфері прав людини в Україні: оцінки експертів/ Беззуб І.: Центр дослідження соціальних комунікацій [Електронний ресурс]. – Режим доступу: htth://nbuviap.gov.ua

4. Статистика щодо України. Уповноважений ВР України з прав людини1950 [Електронний ресурс]. – Режим доступу: htth://zaxid.net

УДК 340.5

Фтоян А. М.
Національна академія СБ України

ЩОДО УДОСКОНАЛЕННЯ СИСТЕМИ ЗАХИСТУ КОМЕРЦІЙНОЇ ТАЄМНИЦІ

На сьогодні небагато торговельних підприємств піклується про зберігання у таємниці інформації, що за статусом може бути віднесена до конфіденційної. Така постанова проблеми не випадкова. Це пояснюється тим, що незначна кількість торговельних підприємств розуміє важливість і необхідність організації системи захисту комерційної таємниці. В таких умовах особливо важливим стає розробка ефективної системи захисту комерційної таємниці з боку самого підприємства.

Досвід розвинутих країн світу свідчить про те, що можна загубити до 30% і більше виручки або стати банкрутом, коли не турбуватися про захист власної комерційної таємниці [4].

Проводячи дослідження законодавства і літературних джерел, присвячених проблемам захисту комерційної таємниці, визначено, що:

по-перше, законодавство не робить розмежування з комерційної таємниці між різними галузями економіки;

по-друге, у своїх наукових роботах провідні економісти і науковці увагу приділяють сааме комерційній таємниці виробничого підприємства [2].

Щоб розробити дійову систему захисту комерційної таємниці, необхідно вивчити всі можливі шляхи незаконного оволодіння нею.

Існують такі протиправні дії, що дозволяють оволодіти конфіденційною інформацією підприємства:

- повідомлення, надання та пересилка відомостей, що становлять комерційну таємницю,
- підкуп співробітників підприємства, що володіють або мають доступ до конфіденційної інформації,
- підслуховування та підглядування (спостереження),
- підключення до технічнихзасобів,
- крадіжка,
- копіювання та фотографування,
- перехоплювання,
- знищення.

Також оволодінню комерційною таємницею сприяють:

- низький рівень контролю за достиганням заходів безпеки,
- незадовільні умови праці,
- неефективна система заохочування працівників,
- економія на більш досконалих технічних засобах захисту,
- текучість кадрів,
- недосконала система оплати праці,
- аварійний стан основних фондів,
- невідповідність співробітника займаємій посаді [1].

Керівництво разом з службою безпеки розробляють стратегію і тактику зберігання комерційної таємниці.

На підприємстві повинні бути створений жорстокий режим доступу до інформації конфіденційного характеру. Це передбачає:

1) пропускний режим до приміщень, де зберігаються відомості, що становлять комерційну таємницю. Надана перепустка

не має бути передана іншій особі, використана для задоволення особистих потреб та ін. Тому для інформації різного типу конфіденційності потрібні неоднакові перепустки(за кольором або за позначками, або за способом фіксування та ін.). Крім того, можливо через певні інтервали часу змінювати форму та зміст перепустки;

2) ретельний підбір кадрів, що працюють з конфіденційною інформацією. Відомо, що чим менше людей мають доступ до таких відомостей, тим більше ймовірність зберегти їх в таємниці. Отже, необхідне обмежене коло осіб, що можуть мати доступ до тієї чи іншої секретної інформації. Доступ повинні маги тільки ті особи, яким відомості потрібні для виконання функцій згідно з Посадовою інструкцією. У справі співробітника повинні бути також відзив керівника структурного підрозділу з візами керівників відділу кадрів, служби безпеки та керівника підприємства; угоду про нерозголошення комерційної таємниці. Зразок Угоди про нерозголошення відомостей, що ставлять комерційну додається;

3) встановлення відповідальності за розголошення комерційної таємниці торговельного підприємства. Відповідальність у випадку незаконних дій, що ведуть до заволодіння комерційною таємницею, фіксується у Посадових інструкціях, Положенні про комерційну таємницю, Положенні служби безпеки підприємства. Законодавчо закріплена дисциплінарна, адміністративна та кримінальна відповідальність за порушення. У відповідності до цього на підприємстві можуть бути розроблені власні способи притягнення до відповідальності, що не суперечать законодавству України [3].

Основними недоліками нормативно-правової бази у сфері забезпечення безпеки розвитку суб’єктів підприємницької діяльності є: відсутність законів прямої дії про безпеку підприємства, надання охоронних послуг, детективну діяльність, захист комерційної таємниці та конфіденційної інформації; невідповідність нормативно-правової бази реаліям сьогоднішнього дня та декларативність існуючих документів; відсутність чіткого інституційного механізму моніторингу, наукової експертизи правового забезпечення безпеки функціонування суб’єктів господарювання.

Література

1. Новікова О.Ф., Покотиленко Р.В. Економічнабезпека: стан, проблеми, шляхи вирішення. // ВісникДонДУЕТ. Економічні науки. — 2004. — №7. — С. 24-31

2. Скібіцький О. В. Організація бізнесу. Менеджмент підприємницької діяльності: [навч. посібник для студ. вищ. навч. закл.] / О. В Скібіцький, В. В. Матвеєв, Л. І. Скібіцька. – К. : Кондор, 2011. – 912 с.

3. Ткачук Т. Методиконкурентноїрозвідки// Бизнес и безопасность. - №5. - 2006. - с. 21-26

4. Про внесення змін до Закону України «Про інформацію»: Закон України // Голос України. – 2011. – 9 лютого. – № 24

УДК 342.6

Царик А. О.
Національна академія СБ України
Ничитайло І. М.
кандидат юридичних наук, доцент
Національна академія СБ України

ПЕРСПЕКТИВА РОЗВИТКУ ТА ШЛЯХИ ВДОСКОНАЛЕННЯ СИСТЕМИ СУБ'ЄКТІВ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В УКРАЇНІ

Сьогодні українське суспільство перебуває в процесі стрімкого розвитку, який характеризується здійсненням комплексу реформ, насамперед конституційної та адміністративної, посиленням процесів демократизації суспільства та формуванням громадянського суспільства, дерегуляцією ринку, децентралізацією та деконцентрацією влади, набуттям Україною статусу асоційованого члена ЄС, а також веденням проти України інформаційної війни, здійсненням спеціальних інформаційних операцій Росією. Саме тому країні необхідний чіткий механізм здійснення управління в усіх сферах життєдіяльності, якісні зміни в системах, структурах, їх правовому статусі а також вдосконалення методів функціонування органів державної влади [1].

У зв'язку з цим перед наукою управління постає низка актуальних завдань, щодо дослідження та узагальнення понять і закономірностей з метою вдосконалення та приведення у відповідність сучасним потребам системи взаємодії та координації дер-

жавних органів України, а також ліквідації процесів, що не відповідають умовам та вимогам сучасного розвитку державності.

У світлі сучасних подій все більшої актуальності набуває питання оптимізації системи суб'єктів захисту інформації як складової інформаційної безпеки, оскільки системі суб'єктів захисту інформації в Україні притаманні такі проблеми, як низька координованість їх діяльності, перетинання повноважень, і як наслідок відсутність системності у взаємовідносинах між елементами даної системи.

Дослідження організаційно-правових питань вдосконалення взаємовідносин органів державної влади в сфері захисту інформації слід почати з визначення системи органів (суб'єктів) з підтримки інформаційної безпеки.

Загальну систему суб'єктів забезпечення захисту інформації в Україні становлять:

1) органи законодавчої влади і державного управління загальної компетенції – Верховна Рада України, Кабінет Міністрів України;

2) Конституційний суд, суди загальної юрисдикції;

3) органи виконавчої влади:

а) правоохоронні органи – Прокуратура України, Міністерство оборони України, Міністерство внутрішніх справ України, Служба безпеки України;

б) галузеві органи державного управління, що регулюють інформаційні відносини в певних галузях – Комітет з питань інформатизації та зв'язку, Державний комітет телебачення і радіомовлення України, Державна служба інтелектуальної власності, Державна служба спеціального зв'язку та захисту інформації;

4) громадські структури – підприємства, установи, організації різних форм власності, діяльність яких пов'язана з наданням послуг зв'язку, із захистом інформації, інформаційні агентства, суб'єкти видавничої справи.

Зазначена система завдяки взаємодії всіх гілок влади і громадських структур формально гарантує підтримку інформаційної безпеки в державі [2]. Але на практиці ми дуже часто зустрічаємося з відсутністю чіткої координації зусиль в сфері забезпечення інформаційної безпеки. Спостерігається так званий ефект «лебідь, рак і щука», коли кожен елемент зазначеної системи намагається отримати перевагу перед іншими, або дублює дії іншої.

На жаль, досі в Україні відсутні загальнонаціональні міжвідомчі координаційні структури, що могли б узгоджувати та координувати діяльність різних відомств щодо забезпечення захисту інформації. Такі координуючі функції могла б узяти на себе або Рада національної безпеки і оборони України (через свої структури), або спеціально створений державний орган (до чого схиляється все більше експертів) [3].

В нашій державі вже існує низка профільних підрозділів, у структурі декількох відомств, які ефективно забезпечують захист інформації: у структурі Служби безпеки України – Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки, у структурі Міністерства оборони України – Головне управління зв'язку та інформаційних систем та Головне управління розвідки, Управління боротьби з кіберзлочинністю у складі Міністерства внутрішні справ України, тощо. Проте зважаючи на сучасний стан проблем в країні та застосування проти нашої держави інформаційної зброї, як на інформаційно-психологічному рівні так і в кіберпросторі, доцільним було б створення спеціально уповноваженого органу державної влади з питань забезпечення інформаційної безпеки, який міг би об'єднати всі функції вищеперелічених підрозділів, доопрацювати їх та стати дієвим механізмом захисту інформаційної безпеки в державі. Це могло б суттєво змінити проблему дублювання повноважень, а також допомогти ефективно та швидко вирішувати ключові проблеми інформаційної безпеки на загальнодержавному рівні.

Щодо взаємовідносин між елементами системи суб'єктів забезпечення захисту інформації в Україні можна виділити такий основний недолік, як низька взаємодія органів державної влади та приватного сектору. Саме це питання стає ключовим, зважаючи на те, що значна кількість інформаційної інфраструктури перебуває у приватній власності. Змінити ситуацію могло б підвищення взаємної довіри між бізнесом і державними інституціями, що в свою чергу спонукало б повідомляти урядові структури про порушення задля вчасної їх нейтралізації.

Таким чином, для України залишається актуальною низка проблемних питань, вирішення яких потребуватиме певних зусиль як з боку держави. Від ефективності їх вирішення залежатиме те, якою мірою Українська держава зможе ефективно

відповісти на сучасні виклики, зокрема в сфері захисту інформації. Більшою мірою ці проблеми потребують вирішення або в інституційній, або нормативно-правовій площині, однак суттєва їх частина безпосередньо пов'язана із проблемою вироблення взаємної довіри у взаємовідносинах трикутника «держава – бізнес – суспільство».

Література

1. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : закон України від 9.01.2007 р. № 537-V [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/537–16

2. Бурило Ю.П. Організаційно-правові питання державного управління в інформаційній сфері .: Дис. канд. наук: 12.00.07 - 2008. [Електронний ресурс]. – Режим доступу : http://adminpravo.com.ua/index.php/2010-04-13-14-05-13/145-2010-09-28-13-27- 30/1942-22-.html

3. Дубов Д. В. Стратегічні аспекти кібербезпеки України / Д. В. Дубов // Стратегічні пріоритети. - 2013. - № 4. - С. 119-127. - Режим доступу: http://nbuv.gov.ua/UJRN/spa_2013_4_18.

УДК 005.3

Цифра Є. І.
Національна академія СБ України

СИСТЕМИ ЕЛЕКТРОННОГО УРЯДУВАННЯ В КОНЦЕПЦІЇ G2G: НОРМАТИВНО-ПРАВОВИЙ АСПЕКТ

Електронне урядування (е-урядування) є одним із сучасних інструментів розвитку інформаційного суспільства, впровадження якого сприяє створенню умов для ефективного і прозорого державного управління, покращення процедур надання адміністративних послуг фізичним та юридичним особам (громадянам та бізнесу), зменшенню передумов для скоєння корупційних діянь тощо [2].

Тому метою впровадження технологій е-урядування є ефективне використання можливостей сучасних інформаційно-комунікаційних технологій у відносинах «держава-бізнес-громадянин» для:

- забезпечення відкритості інформації про діяльність органів державної влади та органів місцевого самоврядування, створення можливостей безпосередньої участі громадян та інститутів громадянського суспільства у процесах підготовки та проведення експертизи проектів рішень, які приймаються на всіх рівнях державного управління;

- підвищення якості та доступності державних адміністративних послуг, спрощення процедур та скорочення адміністративних витрат;

- підвищення якості адміністративних та управлінських процесів, забезпечення дієвого контролю за результатами діяльності органів державної влади та місцевого самоврядування.

Загалом, говорячи про впровадження технологій G2G, доцільно виділити наступні основні завдання:

- інформатизацію в органах державної влади та місцевого самоврядування на всіх рівнях;

- електронні міжвідомчі та міжнародні взаємовідносини;

- впровадження комп'ютерних систем, здатних підтримувати всі необхідні функції взаємодії цих органів із населенням і бізнесовими структурами.

Тобто технології електронного урядування в концепції G2G є, насамперед, технологіями електронного документообігу.

Впровадження систем електронного документообігу в органах державної влади та місцевого самоврядування дозволяє підвищити ефективність функціонування усіх складових системи державного управління, а саме:

- прискорити рух документів, забезпечити своєчасність їх розгляду;

- скоротити терміни підготовки та прийняття управлінських рішень шляхом автоматизації процесів колективного створення та використання документів;

- підвищити якість рішень за рахунок надання виконавцю максимально повної бази документів (інформації);

- значно знизити витрати на розмноження, передачу і збереження копій паперових документів, а отже й підвищити ефективність роботи, як окремих державних службовців, так і конкретного органу державної влади та місцевого самоврядування.

На сьогоднішній день спостерігається значне відставання нашої держави від країн Європейського Союзу щодо стану впровадження сучасних інформаційних технологій у сфері державно-

го управління, хоча за останні декілька років Україна помітно прогресувала у цьому напрямку.

Не враховуючи фінансову сторону зазначеної проблеми вважається, що для переходу органів державної влади України на електронний документообіг необхідно забезпечити, в першу чергу, технологічне об'єднання систем електронного документообігу всіх органів державної влади шляхом забезпечення:

- сумісності систем електронного цифрового підпису, що використовуються в системах електронного діловодства України (з урахуванням потреб міжнародного співробітництва);
- сумісності систем електронного діловодства різних виробників як з точки зору форматів представлення даних, так і регламенту використання.

Загалом, нормативно-правове регулювання у сфері електронного документообігу спрямовано на реалізацію єдиної державної політики, що забезпечує юридичну силу електронних документів на державному рівні.

Таким чином, при впровадженні систем електронного урядування в Україні є можливість врахування досвіду інших країн, що пройшли цей шлях (особливо прибалтійських країн, Польщі, Чехії та інших). При цьому для концепції G2G основну увагу треба зосередити не лише на питаннях національної інфраструктури відкритих ключів та електронного діловодства, а також і питаннях забезпечення кібербезпеки, що стосуються удосконалення вітчизняної нормативно-правової бази технічного і криптографічного захисту інформації, розвитку в Україні індустрії комп'ютерної і мережевої безпеки, створення національної системи кібербезпеки тощо.

Література

1. Закон України від 22.05.2003 № 851-IV "Про електронні документи та електронний документообіг".

2. Закон України від 22.05.2003 № 852-IV "Про електронний цифровий підпис".

3. Постанова Кабінету Міністрів України від 28.10.2004 № 1452 "Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності".

4. Джига Т. Вітчизняний та зарубіжний досвід запровадження органах державної влади систем електронного документообігу: проблеми, переваги, рекомендації / Т Джига// [Електронний ресурс] // Режим доступу: http://old.niss.gov.ua/monitor/Juli2009/13.htm.

УДК 340.5

Шевчук Ю. В.
Національна академія СБ Україна
Шепета О. В.
кандидат юридичний наук
Національна академія СБ Україна

АНАЛІЗ МІЖНАРОДНИХ УГОД УКРАЇНИ ПРО ВЗАЄМНУ ОХОРОНУ СЕКРЕТНОЇ ІНФОРМАЦІЇ

Основу сучасних міжнародних відносин у світі складають міжнародні договори. Для кожної держави, зокрема для України, питання договірного оформлення відносин із зовнішнім світом посідає одне з найголовніших місць. Так, одним з перших питань, що виникли після проголошення незалежності України, яка стала повноправним суб'єктом міжнародного права, були угоди про встановлення дипломатичних відносин з іншими країнами зарубіжжя.

Україна як незалежна європейська держава стала повноправним суб'єктом міжнародного спілкування, заявила власну позицію і в міжнародних організаціях, в тому числі шляхом вступу у договірні відносини. Сфера її зовнішньополітичної діяльності стає все більш широкою, наповнюється новим змістом.

Зусилля керівництва держави спрямовані на захист національних інтересів України, політичної незалежності нашої держави, її територіальної цілісності, економічних інтересів, пов'язаних з інтеграцією економіки України у світове господарство.

Розвиваючи принципові положення, визначені в Декларації про державний суверенітет, які закріплені в Конституції, Україна у своїй зовнішній політиці спирається на фундаментальні загальнолюдські цінності, виступає за захист прав та інтересів громадян України, її юридичних осіб, створює умови для підтримання контактів з українцями за кордоном - вихідцями з України, дбає про задоволення національно - культурних і мовних потреб українців, які проживають за межами держави, надає їм допомогу згідно з міжнародним правом.

Найбільша кількість угод укладена з державами, які були визначені в якості стратегічних партнерів України, а також з прикордонними державами. Значна кількість угод була укладена з

колишніми республіками СРСР, країнами Східної Європи, розвиненими країнами Західної і Північної Європи, при цьому відчувається певний дисбаланс щодо укладення угод з країнами Африки, Латинської Америки і Азіатсько - тихоокеанського регіону.

На сьогодні Україна уклала міжурядові угоди про взаємну охорону секретної інформації з наступними державами: Вірменія, Грузія, Індія, КНР, Латвія, Молдова, Польща , Словакія, Туркменістан, ФРН, Хорватія , Казахстан та інші [1-12].

Такі договори як правило складаються з наступних структурних елементів:

- преамбула, в якій визначаються сторони і загальні цілі угоди ;
- погодження термінів і визначень, що використовується в угоді;
- таблиці узгодження грифів обмеження доступу, що використовуються у матеріальних носіях інформації, яка вступає в транскордонний обіг;
- обов'язки сторін щодо взаємного захисту інформації;
- процедури передачі інформації між сторонами і зазначенням державних органів кожної із сторін, які за це відповідають;
- процедури забезпечення захисту переданої інформації в ході її обігу;
- процедура організації взаємного контролю за режимом охорони переданої інформації стороною одержувачем;
- порядок дії сторін на випадок порушення умов договору [1-12].

Проаналізувавши угоди, можна стверджувати, кожна сторона має певний перелік обов'язків щодо захисту інформації, а саме: захист секретної інформації, переданої або створеної в процесі співробітництва Сторін; не змінювати гриф секретності, наданий організацією держави Сторони, що здійснила передачу, без письмової її згоди; упроваджені з отриманою секретною інформацією вживати такі ж заходи захисту , що використовується по відношенню до власної секретної інформації , ступені секретності якої порівнянні відповідно до таблиці узгодження грифів; користуватися секретною інформацією, отриманою від організації держави іншої Сторони , винятково в передбачених при її передачі цілях; не надавати третій стороні доступ до секретної інформації без попередньої письмової згоди Сторони , що її передала; надавати доступ до секретної інформації тільки особам, яким ознайомлення з даною інформацією необхідне для виконання

службових обов'язків з метою , передбаченою при її передачі або її спільному створенні;надавати доступ до секретної інформації лише тим особам, які мають відповідний допуск до секретної інформації і пройшли перевірку для оформлення допуску , що відповідає тій , яка необхідна для одержання допуску до прирівнюваної таємної інформації власної держави; забезпечувати на території власної держави проведення необхідних інспекційних перевірок та дотримання норм захисту таємної інформації [1-12].

Забезпечення інтересів держав на захист їх інформації досягається шляхом взяття державами на себе та виконання ними міжнародних зобов'язань, які стосуються взаємного визнання статусу інформації з обмеженим доступом, наданим у ході співробітництва іноземною стороною матеріалам.

Забезпечення належного режиму охорони цієї інформації за час перебування у розпорядженні іноземної сторони, інформування про факти розголошення наданої іноземною стороною інформації та забезпечення належного розслідування цих фактів та покарання винних у цьому осіб.

Проаналізувавши дані угоди можна дійти висновку, що при співробітництві з іноземними державами та ЄС , Україна доклала великих зусиль щодо захисту національної безпеки і державних інтересів у сфері захисту інформації з обмеженим доступом.

Література

1. Угода між Кабінетом Міністрів України та Урядом Грузії про взаємну охорону секретної інформації(Угоду ратифіковано Законом N 625-IV (625-15) від 06.03.2003). Режим доступу : http://zakon2.rada.gov.ua/show/268_001

2. Угода між Кабінетом Міністрів України та Урядом Республіки Вірменія про взаємну охорону секретної інформації (Угоду ратифіковано від 19.06.2003).Режимдоступу:http://search.ligazakon.ua/l_doc2.nsf/link1/MU02135.html

3. Угода між Кабінетом Міністрів України та Урядом Республіки Казахстан про взаємний захист секретної інформації(Угоду ратифіковано Законом N635-VI (635-17) від30.10.2008). Режим доступу: http://zakon4.rada.gov.ua/laws/show/398_053

4.Угода між Кабінетом Міністрів України та Урядом Республіки Молдова про взаємний захист секретної інформації (Угоду ратифіковано 07.09.2005). Режим доступу:http://search.ligazakon.ua/l_doc2.nsf/link1/MU04153.html

5. Угода між Кабінетом Міністрів України та Урядом Республіки Польща про взаємну охорону секретної інформації (Угоду ратифіковано Законом N 173-IV(173-15)від 26.09.2002) .
Режим доступу: http://zakon4.rada.gov.ua/laws/show/616_028

6. Угода між Кабінетом Міністрів України та Урядом Туркменістану про взаємну охорону секретної інформації (Угоду ратифіковано від 10.01.2002). Режим доступу: http://search.ligazakon.ua/ l_doc2.nsf/link1/MU01060.html

7. Угода між Урядом України та Урядом Китайської Народної Республіки про взаємну охорону секретної інформації (Угоду ратифіковано 20.11.2000). Режим доступу: http://zakon.nau.ua/doc/?code=156_038

8. Угода між Кабінетом Міністрів України та Урядом Республіки Хорватія про взаємну охорону секретної інформації (Угоду ратифіковано 26.07.2006) . Режим доступу: http://zakon.nau.ua/doc/?code=191_016

9. Угода між Кабінетом Міністрів України та Урядом Федеративної Республіки Німеччина про взаємний захист таємної інформації (Угоду ратифікованоЗаконом N 2937-III (2937-14) від 10.01.2002, ВВР, 2002, N 23, ст.157).Режим доступу: http://zakon4.rada.gov.ua/laws/show/276_008

10.Угода між Кабінетом Міністрів України та Урядом Латвійської Республіки про взаємну охорону секретної інформації (Угоду ратифіковано Законом N 2126-IV (2126-15) від 22.10.2004). Режим доступу: http://zakon4.rada.gov.ua/ laws/show/428_025

11. Угода між Україною та Республікою Індія про взаємну охорону секретної інформації (Угоду ратифіковано 07.04.2004) Режим доступу: http://www.yur-info.org.ua/doc/1743835/Ugoda-mizh-Ukrainoiu-ta-Respublikoiu-Indiia-pro-vzaiemnu-okhoronu-sekretnoi-informatsii

12. Угода між Урядом України та Урядом Словацької Республіки про взаємний захист таємної інформації та матеріалів (Угоду затверджено Постановою КМ N 1434(1434-98-п) від 14.09.98). Режим доступу: http://www.yur-info.org.ua/doc/1630730/Ugoda-mizh-Uriadom-Ukraini-ta-Uriadom-Slovatskoi-Respubliki-pro-vzaiemnii-zakhist-taiemnoi-informatsii-ta-materialiv

УДК 005.3

Шепета О. В.
кандидат юридичних наук
Національна академія СБ України
Когут В. В.
Національна академія СБ України

ЩОДО ВИЗНАЧЕННЯ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ УКРАЇНИ

Рівень сучасних викликів і загроз в інформаційній сфері підтверджує значущість положень статті 17 Конституції України про те, що захист державного суверенітету і забезпечення інформаційної безпеки є справою всього Українського народу [1].

Досліджуючи відносини в сфері забезпечення інформаційної безпеки науковці акцентують свою увагу на поняття „загрози інформаційній безпеці". Науковий аналіз згаданого питання дав змогу виявити відсутність єдності у поглядах, що стосуються класифікації зазначених загроз як на законодавчому, так і на науковому рівнях.

Цілком влучною є позиція О.Бодрука, що на практиці аналіз загроз – це завжди суб'єктивний процес сприйняття певною особою чи соціальною групою тих чи інших факторів через призму власних інтересів і фахового рівня. Водночас, об'єктивне визначення загроз передбачає чітке усвідомлення параметрів, за межами яких певне явище втрачає можливості саморегуляції та потребує зовнішнього втручання для збереження стабільності соціальної системи, а також певних умов, що перетворюють ті ж самі фактори або на реальну або на потенційну загрозу [2].

Відповідно до Закону України „Про основи національної безпеки України" до загроз національним інтересам і національній безпеці в інформаційній сфері відносять наступні:

1. Прояви обмеження свободи слова та доступу громадян до інформації;

2. Поширення засобами масової інформації культу насильства, жорстокості, порнографії;

3. Комп'ютерна злочинність та комп'ютерний тероризм;

4. Розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що е власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;

5. Намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації [3].

Вважаємо, що такий перелік є вкрай обмеженим в сучасних умовах прискорених процесів високого інформаційного насичення, розвитку інформаційних технологій та їх протиправного використання та застарілий.

Розширений перелік відомостей, що становлять потенційні та реальні загрози інформаційній безпеці України був у Доктрині інформаційної безпеки України, яку скасовано Указом Президента України 06.06.2014 року, натомість нового документу не ухвалено.

Враховуючи те, що інформаційна безпека є невід'ємною складовою національної безпеки, її регулювання потребує дієвих

механізмів у формі політичних рішень або прийнятих нормативно-правових актів. Функціонування відповідного механізму, на нашу думку, можливе лише за умови глибокого наукового осмислення теоретичних положень щодо інформаційної безпеки взагалі, та сутності загроз зокрема.

Чинники, що зумовлюють ескалацію загроз інформаційній безпеці, мають комплексний характер – вони охоплюють усі сфери життєдіяльності людини, суспільства і держави, а відповідно мають міжвідомчий характер.

Інформаційна безпека як складова національної безпеки відповідно до сучасного розвитку її теорії в узагальненому вигляді, ґрунтується на таких базових елементах: національні інтереси – загроза – захист. Саме загрози стану захищеності суспільних відносин є важливим елементом процесу забезпечення інформаційної безпеки.

Загрози інформаційній безпеці людини

Інтереси особистості, які необхідно охороняти в інформаційному суспільстві, полягають насамперед у реальному забезпеченні конституційних прав і свобод людини і громадянина на доступ до інформації, на використання інформації в інтересах здійснення не забороненої законом діяльності, а також у захисті інформації, що забезпечує особисту безпеку, духовний та інтелектуальний розвиток.

Загрози інформаційній безпеці суспільства

Інтереси суспільства полягають у захисті життєво важливих інтересів в інформаційній сфері, забезпечення реалізації конституційних прав і свобод людини і громадянина в інтересах зміцнення демократії, досягнення і підтримування суспільної злагоди.

Загрози інформаційній безпеці держави

Інтереси держави в інформаційній сфері полягають у створенні умов для гармонійного розвитку інформаційної інфраструктури держави, реалізації конституційних прав і свобод людини і громадянина в інтересах зміцнення конституційного ладу, суверенітету і територіальної цілісності країни.

Отже, проведений аналіз свідчить про те, що визначення загроз інформаційній безпеці України повинно базуватись на визначенні національних інтересів нашої держави, враховувати сучасні світові тенденції розвитку інформаційних технологій, а також політичну та геополітичну ситуацію.

Література

1. Конституція України // Сайт Верховної Ради України. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/559/2011.
2. Бодрук О. Структури воєнної безпеки: національний та міжнародний аспекти: монографія / О. Бодрук. – К.:НІПМБ, 2001. – 300 с.
3. Закон України "Про основи національної безпеки України", прийнятий 19 червня 2003 р. // Відомості Верховної Ради України. – 2003. – № 39. – Ст. 351.

УДК 65.012.8

Шиптицька І. І.
Львівський державний університет безпеки життєдіяльності
Кухарська Н. П.
кандидат фізико-математичних наук, доцент
Львівський державний університет безпеки життєдіяльності

ОБҐРУНТУВАННЯ НЕОБХІДНОСТІ РОЗРОБЛЕННЯ ОРГАНІЗАЦІЯМИ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

В умовах, коли нематеріальні активи підприємств, які існують зазвичай у вигляді інформації, мають дедалі більший вплив на розвиток бізнесу, його конкурентоздатність, управління інформаційною безпекою (ІБ) стає невід'ємною складовою загальної системи управління організацією. Значущість систематичної цілеспрямованої діяльності щодо забезпечення інформаційної безпеки залежить від ступеня автоматизації бізнес-процесів організації і є тим вищою, чим більша частка "інтелектуальної складової" в її кінцевому продукті, чим більша залежність діяльності підприємства від забезпечення конфіденційності певної інформації (технологій, ноу-хау, комерційних баз даних, маркетингової інформації, результатів наукових досліджень тощо).

Управління інформаційною безпекою на кожному конкретному підприємстві повинно здійснюватися в контексті його загальної господарської діяльності з урахуванням характеру функціонування компанії (технологій виробництва, специфіки ринків збуту, тощо), ситуації, що фактично склалася в ринковій конкурентній боротьбі, в державній політиці, а також з врахуванням розвитку правової і правоохоронної системи, рівня розвитку використовува-

них інформаційних і телекомунікаційних технологій та інших чинників, що мають вплив на поточну діяльність організації.

Для нейтралізації існуючих загроз і забезпечення ІБ на підприємствах слід створити систему менеджменту інформаційної безпеки, яка включає:

- формування та практичну реалізацію комплексної багаторівневої політики інформаційної безпеки підприємства та системи внутрішніх вимог, норм і правил;
- організацію департаменту (служби, відділу) інформаційної безпеки;
- розроблення системи заходів і дій на випадок виникнення непередбачуваних ситуацій (“управління інцидентами”);
- проведення аудитів (комплексних перевірок) стану інформаційної безпеки на підприємстві.

Кожен з цих напрямків організаційної роботи має свої особливості і повинен реалізовуватися з використанням специфічних методів менеджменту та відповідно до встановлених міжнародними стандартами правил.

Розглянемо більш детально політику інформаційної безпеки.

Згідно визначення, поданому у стандарті “Помаранчева книга” (Trusted Compute System Evaluation Criteria), політика інформаційної безпеки (ПолІБ) – це набір норм, правил і практичних прийомів, котрі регулюють управління, захист і розподіл цінної інформації [1].

Можна навести декілька вагомих аргументів на користь необхідності розробки політики інформаційної безпеки для організації будь-якого масштабу і виду діяльності. По-перше, ПолІБ є основою для захисту всіх активів організації, що мають вплив на забезпечення ІБ, в її рамках визначаються правила розмежування доступу до цих активів. Вона визначає, яка поведінка по відношенню до активів є дозволеною, тобто санкціонованою, а яка є забороненою, несанкціонованою і свідчить про незаконне їх використання. По-друге, політика інформаційної безпеки формує “правила гри” для всіх працівників організації та третіх осіб, що дає змогу досягнути згоди стосовно питань забезпечення ІБ як всередині самої організації (включаючи її керівництво), так і зовні. По-третє, ПолІБ допомагає зробити правильний вибір платформи для роботи з активами із врахуванням інструментальних засобів і процедур, що будуть використовуватися.

Серед інших причин, що спонукують організацію розробляти політику інформаційної безпеки, виокремимо такі:

Вимоги керівництва підприємства. Декілька серйозних інцидентів, що призвели до зупинки або сповільнення роботи компанії у результаті різних локальних і віддалених атак, розголошення конфіденційної інформації чи крадіжки комп'ютерів з цінною інформацією суттєво стимулюють появу такої ініціативи з боку керівництва.

Вимоги законодавства та стандартів у сфері інформаційної безпеки. Політика інформаційної безпеки дає змогу визначити правила, у відповідності до яких частина інформації підприємства може буде віднесена, наприклад, до категорії комерційної таємниці, а це дасть можливість захистити її юридично.

Вимоги клієнтів і партнерів щодо юридичного підтвердження в контрактах та договорах необхідного рівня забезпечення ІБ, як гарантію того, що їх конфіденційна інформація також буде захищена належним чином. Саме наявність ПолІБ є переконливим доказом намірів організації відносно забезпечення інформаційної безпеки.

Підвищення інвестиційної привабливості організації. Наявність ПолІБ позиціонує організацію як таку, що є "відкрита" для інвестицій.

Необхідність сертифікації за стандартами (наприклад, ISO/IEC 9001, 27002, 15408 і т.п.), що свідчитиме про необхідний рівень забезпечення ІБ в організації.

Усунення зауважень аудиторів і виконання їх рекомендацій. Будь-яка зовнішня аудиторська перевірка, у першу чергу, звертає увагу на необхідність формалізації всіх бізнес-процесів, в тому числі особливу увагу приділяє наявності в організації ПолІБ, на відповідність якій може проводитися аудит.

Забезпечення конкурентоздатності за рахунок оптимізації бізнес-процесів і підвищення результативності. Правильно розроблена і реалізована ПолІБ дає змогу зменшити час недоступності сервісів, викликаних інцидентами ІБ, таким чином поліпшити показники живучості організації.

Демонстрація зацікавленості керівництва в забезпеченні інформаційної безпеки значно підвищить пріоритет безпеки в очах працівників організації.

Створення корпоративної культури ІБ і широке залучення працівників в процес забезпечення інформаційної безпеки. Необхідно переконати працівників в тому, що забезпечення ІБ – їх прямий обов'язок. Це досягається шляхом введення процедури обов'язкового знайомства з вимогами ПолІБ і підписанням відповідного документа про те, що працівник з ними ознайомлений, вони йому зрозумілі і він зобов'язується їх виконувати. Політика інформаційної безпеки дає підстави ввести вимоги щодо підтримання необхідного рівня ІБ в перелік обов'язків кожного працівника. Також ПолІБ допомагає створити в організації атмосферу, сприятливу для пропаганди і підтримки високого пріоритету ІБ.

Зменшення вартості страхування. Наявність ПолІБ є необхідною і обов'язковою умовою укладання договорів страхування. Зауважимо, результати аудиту ІБ, проведеного незалежною організацією, впливають на вартість страхування.

Економічна доцільність. ПолІБ є дешевим і водночас доволі ефективним засобом забезпечення ІБ. Її послідовне втілення і чітке дотримання декларованих нею вимог у щоденному житті організації дозволяє знизити витратну частину бюджету, яка скеровується на забезпечення ІБ.

Успішна бізнес-практика. Наявність ПолІБ сприймається у бізнес-колах як вияв дотримання організацією правил хорошого тону.

Таким чином, політика інформаційної безпеки є вкрай необхідною для успішної організації режиму ІБ будь-якої вітчизняної організації. ПолІБ мінімізує вплив "людського фактора" і недоліки існуючих технологій захисту інформації. Крім того вона дисциплінує працівників організації і сприяє створенню корпоративної культури безпеки.

Література

1. Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STD, 1985 [Electronic resource]. – Access mode : http://csrc.nist.gov/publications/history/dod85.pdf.

ЗМІСТ

АКТУАЛЬНІ ПИТАННЯ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ В КОНТЕКСТІ ЗАПРОВАДЖЕННЯ В УКРАЇНІ СИСТЕМ ЕЛЕКТРОННОГО УРЯДУВАННЯ

ПРОБЛЕМНІ ПИТАННЯ ПІДГОТОВКИ ФАХІВЦІВ У ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

ІНФОРМАЦІЙНА БЕЗПЕКА ОЧИМА МОЛОДИХ ВЧЕНИХ

Електронна версія наукого видання на CD-ROM

АКТУАЛЬНІ ПРОБЛЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ

VII науково-практична конференція

Збірник матеріалів
(Київ, 18 березня 2016 року)

У двох частинах

Частина 2

Авторська редакція

Технічне редагування, макетування: *Вишневська О.С.*

Один електронний оптичний диск (CD-ROM)
Об’єм даних 1,2 Мб. Тираж 150 прим.

Видавець і виготовлювач
Національна академія Служби безпеки України,
вул. Трутенка,22, Київ, 03022
факс: (044) 257-30-35
E-mail: academy@ssu.gov.ua
Свідоцтво суб’єкта видавничої справи ДК № 99 від 23.06.2000