УДК 378.016:004.056.5

Сергій Мельник

ГЕНЕЗА ОСНОВНИХ ПОНЯТЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КОНТЕКСТІ ПРОФЕСІЙНОЇ ПІДГОТОВКИ У ВИЩОМУ НАВЧАЛЬНОМУ ЗАКЛАДІ

Необхідність формування професійної компетентності майбутніх фахівців з інформаційної та кібернетичної безпеки актуалізується нагальною потребою реагування на сучасні виклики та загрози інформаційному суверенітету, захищеності інформаційних ресурсів України. Тому при визначенні компетентностей майбутніх фахівців особливої ваги набуває питання формування понятійно-категоріального апарату діяльності у цих сферах, починаючи з термінології у галузі інформаційної безпеки.

Системні питання інформаційної безпеки досліджувалися багатьма українськими вченими, такими як А. Баранов, Н. Волошина, Л. Євдоченко, Б. Кормич, В. Ліпкан, А. Марущак, А. Новицький, В. Панченко, В. Петрик, О. Солодка, А. Тихомиров, В. Фурашев, В. Хлевицький, Л. Щукін та ін. Однак попри високий рівень розробленості проблеми пропонується авторське бачення щодо визначення основних понять інформаційної безпеки та їх співвідношень.

На сьогоднішній день відомо багато різних підходів до визначення сутності базових понять у сфері інформаційної безпеки. Базове поняття «інформація» [1] обґрунтовується, насамперед, сферами й особливостями її застосування.

З урахуванням відомих підходів [6] під *інформаційними ресурсами* можна розуміти закріплену на носіях систематизовану інформацію з відповідним семантичним наповненням. Тобто інформаційними ресурсами можуть бути як документи, так і будь-які інші повідомлення на носіях інформації (далі під інформацією будемо розуміти саме інформаційні ресурси).

Даючи визначення поняття «інформаційний простір» [7], ми, перш за все, розуміємо середовище. Отже, за аналогією, науковці визначають інформаційний простір як інформаційні ресурси, що створюються, розповсюджуються, обробляються, зберігаються та використовуються в інформаційній інфраструктурі – організаційно-технічній системі, яка призначена для створення, розповсюдження, обробки, зберігання та використання інформаційних ресурсів відповідно.

Виходячи з класифікації носіїв інформації, об'єктами захисту є діловодство, автоматизовані системи, телекомунікаційні мережі, об'єкти інформаційної діяльності [8] та система управління персоналом (насамперед, система контролю благонадійності та лояльності персоналу). Поширений термін «інформаційно-технічні впливи» [3] є різновидом інформаційно-технологічних впливів.

На нашу думку, в контексті завдань із забезпечення інформаційної безпеки доцільно виокремити підхід, який охоплює життєвий цикл інформації. Крім того, доцільно звернути увагу на такі уточнення, як «повідомлення», «носій інформації», «інформаційні ресурси», а також поняття «інформаційний простір (або середовище)», «контент».

Мета статті полягає у науковому обґрунтуванні понятійно-категоріального апарату інформаційної безпеки в контексті формування професійної компетентності майбутніх фахівців у вищому навчальному закладі.

Завданням статті є дослідження ґенези основних понять інформаційної безпеки людини, суспільства і держави через визначення: об'єктів і суб'єктів захисту; загроз інформаційній безпеці; поняття інформаційної безпеки та забезпечення інформаційної безпеки.

Нині питання інформаційної безпеки фактично відноситься до окремої міждисциплінарної галузі знань, які є складовими компонентами загальної проблеми інформаційного забезпечення розвитку людини, суспільства і держави. При цьому зміст поняття розкривається у сучасній практиці забезпечення інформаційної безпеки, наукових дослідженнях і нормативно-правових актах, які базуються, насамперед, на розвитку сучасних технологій створення, зберігання та поширення інформації, технологічних і соціальних аспектах глобального інформаційного простору.

Виходячи з позиції професійної спрямованості організації підготовки майбутніх фахівців з інформаційної та кібернетичної безпеки у вищих навчальних закладах, яка орієнтована на сучасні потреби суспільства і держави, а також із метою обґрунтування концептуальних

основ професійної підготовки розглянемо ґенезу основних понять інформаційної безпеки.

Складність висвітлення проблем забезпечення інформаційної безпеки пов'язана, передусім, із тлумачення багатьох термінів, які використовуються для опису цієї предметної області. У зв'язку з цим розглянемо такі родові поняття, як «безпека», «загроза», «ризик», а також «інформація».

У більшості наукових джерел під «безпекою» розуміється стан захищеності життєво важливих інтересів людини, суспільства і держави (системи) в різних сферах життєдіяльності від внутрішніх і зовнішніх, навмисних і випадкових загроз. При цьому основними завданнями безпечного існування системи вважається її самозбереження та розвиток. Безумовно, до базових понять безпекознавства відносять і такі складові, як «загроза» та «ризик». У більшості наукових і практичних джерел вони мають такі тлумачення:

Загроза – це сукупність умов і факторів, які створюють небезпеку в межах певної системи (наприклад, для людини, суспільства та держави).

Ризик – функція ймовірності здійснення певної загрози, а також виду і величини збитків за результатами її реалізації. У свою чергу, управління ризиком – сукупність заходів щодо оцінки ризику, вибору, реалізації та впровадження заходів забезпечення безпеки, спрямованих на досягнення прийнятного рівня залишкового ризику, де залишковий ризик – це ризик, який залишається після впровадження заходів забезпечення безпеки.

На основі здійсненого системного аналізу базове поняття «інформація» необхідно визначати як сукупність відомостей про стан будь-якої матеріальної системи (особи, організації, предмета, процесу, події тощо), призначеної для розповсюдження (передачі, отримання), обробки, зберігання або безпосереднього використання. При цьому з точки зору інформаційної безпеки основною властивістю інформації можна вважати її вплив на людину (а потім громадянина, суспільство і державу), що безпосередньо стосується процесів прийняття рішень. У якості ж основної характеристики визначимо цінність інформації, яка зумовлює рівень впливу та відповідні втрати (шкоду) при успішній реалізації загроз інформаційній безпеці.

Загальновідомо, що людина отримує інформацію через зір, слух, відчуття і дотик, причому найбільший обсяг – через зір і слух. Тому *повідомлення* – це форма представлення інформації: текст; мова; рухоме та нерухоме зображення (далі під інформацією буде розумітися

саме повідомлення). Відповідно *носій інформації* – це об'єкт, який зберігає повідомлення: матеріально-речовинні носії (паперові документи, носії електронної інформації, вироби, речовини, матеріали тощо); сигнали (цифрові чи аналогові); фізичні поля та випромінювання (електромагнітні й акустичні); людина.

Контент – це семантичне наповнення інформаційних ресурсів У інформаційній інфраструктурі, насамперед, *засобах масової комунікації* (преса, радіо, телебачення, інформаційні сервіси мобільного та стаціонарного зв'язку, мережі Інтернет) і *засобах масового впливу* (театр, кіно, література, масові зібрання).

Далі перейдемо до визначення загроз інформаційній безпеці. З технологічної точки зору загрози в інформаційному просторі можна класифікувати таким чином:

– загрози порушення конфіденційності, цілісності, автентичності (авторства) і доступності [1; 8] інформаційних ресурсів у інформаційному просторі – загрози застосування деструктивних інформаційно-технологічних впливів;

– загрози використання контенту [2; 3; 5; 9] інформаційних ресурсів і технічних можливостей інформаційної інфраструктури для прихованого деструктивного впливу на свідомість і підсвідомість людини та громадянина з метою примусу до вчинення непритаманних для нього дій (або бездіяльності) – загрози застосування деструктивних інформаційно-психологічних і психофізичних впливів.

Тепер розглянемо ці класи загроз та інформаційно-технологічних впливів більш детально та через їх призму визначимо основні складові сучасного поняття «інформаційна безпека».

Деструктивний інформаційно-технологічний вплив – це вплив на технологічні процеси інформаційної інфраструктури (об'єкт захисту) шляхом несанкціонованого втручання у встановлені режими створення, розповсюдження, обробки, зберігання, використання та знищення інформації, що мають на меті порушення конфіденційності, цілісності, автентичності та доступності інформації.

Основними методами реалізації інформаційно-технологічних впливів є: несанкціонований доступ до інформації (порушення заходів фізичної охорони, засобів/заходів розмежування доступу до паперових/електронних носіїв інформації; перехоплення інформації в каналах зв'язку; електромагнітні, акустичні й оптичні технічні канали витоку інформації); підробка та/або несанкціоноване знищення паперових/електронних документів, виведення з робочого стану інформа-

ційної інфраструктури (діловодства, автоматизованих систем, телекомунікаційні мереж, об'єктів інформаційної діяльності), компрометація співробітників; блокування та/або порушення штатних режимів роботи технологічних процесів інформаційної інфраструктури.

Інформаційно-психологічний вплив – це вплив на свідомість і підсвідомість (об'єкти захисту) людини, громадянина і суспільства (суб'єкти захисту) з метою внесення змін у їхню поведінку і світогляд, шляхом маніпулювання контентом інформаційних ресурсів у національному та світовому інформаційному просторі [2; 3; 5; 9].

Основними методами реалізації інформаційно-психологічних впливів є вплив на волю і розум шляхом: переконання, що спрямовується на суб'єктів із власним критичним сприйняттям дійсності; навіювання, що спрямовується на суб'єктів, які некритично сприймають інформацію (розсіювання уваги поданням великої кількості інформації, активна форма її подання, штучне перебільшення престижу джерел).

Зрозуміло, що інформаційно-психологічні впливи будуть ефективними лише за умови відсутності у суб'єкта захисту своєчасного доступу до достовірної, повної та неупередженої інформації, оскільки у цьому випадку він не може адекватно сприймати процеси, які відбуваються, та приймати правильні рішення.

Загалом розглянуті загрози мають певний взаємозв'язок, оскільки ефективність інформаційно-психологічних впливів залежатиме також від рівня безпеки технологічної складової інформаційної інфраструктури: забезпечення доступності інформаційних ресурсів у інформаційній інфраструктурі означає технологічну можливість своєчасного доступу суб'єкта захисту до різних інформаційних ресурсів; забезпечення цілісності й автентичності інформаційних ресурсів у інформаційній інфраструктурі означає достовірність, повноту і неупередженість інформаційних ресурсів, якщо суб'єкт захисту довіряє їх автору; крім того, порушення конфіденційності інформаційних ресурсів суб'єкта захисту дає додаткові можливості потенційному супротивнику для формування неповних та упереджених повідомлень із метою дискредитації їх власника.

Окремо звернемо увагу на поняття «*психофізичного (психогенного) впливу»*, під яким можна розуміти деструктивний вплив на психічний стан людини шляхом застосування фізичних полів (акустичних та електромагнітних, включаючи світловий діапазон). Реалізація зазначених впливів не повною мірою відноситься до категорії інформацій-

ної безпеки, оскільки вплив не завжди має інформаційну складову, однак може розглядатись як одна із загроз кібербезпеки людини.

Зрозуміло, що наведена класифікація загроз інформаційній безпеці (класифікація загроз об'єктам захисту) не дає змоги чітко виокремити ці загрози для людини, суспільства і держави. І це не дивно, оскільки технологічна складова є однаковою. Тому загрози інформаційній безпеці можна класифікувати через призму життєво важливих інтересів у інформаційній сфері людини, суспільства і держави [4; 10]. При цьому в якості ознак класифікації розглядаються сфери національної безпеки (політична, економічна, оборонна та ін.) та джерела загроз, виходячи з практичних можливостей їх реалізації в інформаційному просторі людини, суспільства і держави.

В якості *джерел загроз інформаційній безпеці* традиційно розглядають хакера-одинака, організовані угруповання (у тому числі терористичного й екстремістського характеру), транснаціональні корпорації та фінансово-промислові групи, спеціальні служби іноземних держав і військові формування. При цьому джерела загроз є «мірилом» оцінювання моделі загроз [8] з точки зору ресурсів потенційного супротивника (матеріальних, часових, людських), а також критерієм формування вимог до рівня забезпечення інформаційної безпеки конкретного суб'єкта й об'єкта захисту.

Отже, сучасне поняття інформаційної безпеки включає в себе дві окремі складові – безпеку інформації та інформаційно-психологічну безпеку. Мова йде про два різні об'єкти захисту – інформаційний простір (інформаційні ресурси й інформаційну інфраструктуру), а також свідомість і підсвідомість людини і громадянина (населення).

З урахуванням аналізу визначень науковців [1; 8] розглянемо поняття «безпека інформації». *Безпека інформації* – це стан захищеності інформаційних ресурсів та інформаційної інфраструктури людини, суспільства і держави до застосування реальних і потенційних, внутрішніх і зовнішніх деструктивних інформаційно-технологічних впливів.

У свою чергу, *інформаційно-психологічна безпека* – це стан захищеності свідомості та підсвідомості людини, громадянина і суспільства до застосування реальних і потенційних, внутрішніх і зовнішніх деструктивних інформаційно-психологічних впливів [2; 3; 5; 9].

Безумовно, у першому та другому випадках стан захищеності треба утримувати, тобто забезпечувати достатній рівень захищеності. Тому, враховуючи викладене та відомі підходи до визначення понять захисту в інформаційному просторі [1; 2; 3; 5; 8; 9 та ін.], розглянемо сут-

ність понять «захист інформації» та «інформаційно-психологічний захист».

Захист інформації – це діяльність із забезпечення визначеного (достатнього) рівня захищеності інформаційних ресурсів від загроз порушення конфіденційності, цілісності й автентичності, а також забезпечення доступності інформаційної інфраструктури на протязі життєвого циклу інформаційного простору.

Інформаційно-психологічний захист – це діяльність із забезпечення визначеного (достатнього) рівня переваги над супротивником в інформаційному просторі шляхом створення умов для своєчасного доступу суб'єкта захисту до достовірної, повної та неупередженої інформації (контенту).

Інформаційно-технологічне протиборство – це діяльність, яка передбачає захист власного інформаційного простору та застосування деструктивних інформаційно-технологічних впливів у інформаційному просторі супротивника. *Інформаційно-психологічне протиборство* передбачає застосування позитивних і деструктивних інформаційно-психологічних впливів у інформаційному просторі. Як наслідок, *інформаційне протиборство* – це інформаційно-технологічне й інформаційно-психологічне протиборство, що має за мету отримання інформаційної переваги над супротивником в інформаційному просторі.

У контексті сказаного звернемо увагу на визначення поняття *управління інформаційною безпекою* як діяльності з управління ризиками інформаційної безпеки для зменшення практичних можливостей та/або мотивації джерел загроз до застосування деструктивних інформаційно-технологічних та інформаційно-психологічних впливів, зменшення величини можливих збитків у випадку успішної реалізації цих загроз. І це є організаційна складова забезпечення інформаційної безпеки.

Загалом, поняття «*інформаційна безпека»* необхідно визначити як стан захищеності людини, суспільства та держави від реальних і потенційних, внутрішніх і зовнішніх загроз в інформаційному просторі, що спрямовані на порушення безпеки інформації та інформаційно-психологічної безпеки.

Отже, *забезпечення інформаційної безпеки* – це інформаційне протиборство з метою забезпечення безпеки інформації та інформаційно-психологічної безпеки в національному та світовому інформаційному просторі. І ця діяльність включає в себе правову, організаційну та технологічну складові в технічній і гуманітарній сферах, відповідно, буде ефективною лише при комплексному підході до її реалізації.

З позиції методології діяльності звернемо увагу на поняття *«система забезпечення інформаційної безпеки»*, яка є сукупністю скоординованих заходів державно-приватного партнерства, призначених для створення умов і формування практичних можливостей у людини, суспільства, держави для захисту своїх життєво важливих інтересів у національному та світовому інформаційному просторі.

Таким чином, у статті структуровані та наведені нові конструкції базових понять із забезпечення інформаційної безпеки, які орієнтовані на сучасну практику інформаційного протиборства на рівні людини, суспільства, держави.

Перспективами подальшого розвитку напряму досліджень є наукове осмислення співвідношення між поняттями «інформаційна безпека» та «кібербезпека», визначення основ формування соціального замовлення на підготовку кадрів для державного і приватного секторів забезпечення інформаційної та кібернетичної безпеки в Україні.

Посилання:

1. *Волошина, Н. М.* Поняття «безпека інформації» та «інформаційна безпека» в сучасному науковому просторі / *Н. М. Волошина* // Сучасні інформаційні технології у сфері безпеки та оборони. — 2010. — № 2 (8). — С. 53-56.
2. *Дорош, Л.* Інформаційно-психологічна безпека особи, суспільства та держави: новітні виклики міжнародній безпеці / *Л. Дорош* // Українська національна ідея: реалії та перспективи розвитку. — 2013. — Вип. 25. — С. 107-112.
3. Історія інформаційно-психологічного протиборства : підруч. / *Жарков Я. М., Компанцева Л. Ф., Остроухов В. В.* [та ін.]; за заг. ред. *Є. Д. Скулиша*. — К. : Наук.-вид. відділ НА СБ України, 2012. — 212 с.
4. *Кирилюк, О. В.* Забезпечення інформаційної безпеки в умовах розбудови інформаційного суспільства в Україні / *О. В. Кирилюк* // Актуальні проблеми держави і права. — 2014. — Випуск 74. — С. 159-164.
5. *Кучма, Л. О.* Інформаційно-психологічна безпека: теоретико-методологічні підходи та дискусії / *Л. О. Кучма*. — [Електронний ресурс]. — Режим доступу : http://www.crime-research.ru/library.
6. *Марущак, А.* Щодо поняття «інформаційні ресурси держави» / *А. Марущак* // Інформаційна безпека людини, суспільства, держави. — 2009. — № 1 (1). — С. 11-16.
7. *Наливайко, Л. Р.* Інформаційна безпека та інформаційна політика в Україні: конституційно-правовий аспект / *Л. Р. Наливайко* // Вісник Запорізького державного університету. — 2003. — № 1. — С. 3-5.
8. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. — [Електронний ресурс]. — Режим доступу : http://tzi.com.ua/downloads/1.1-003-99.pdf.
9. *Панченко, В. М.* Гуманітарна та технологічна складові у визначенні поняття «інформаційна безпека» / *В. М. Панченко* // Актуальні проблеми управління інформаційною безпекою держави : зб. матер. наук.-практ. конф., 17 березня

2010 року, м. Київ. — К. : Наук.-вид. відділ НА СБ України. — 2010. — С. 205-206.
10. Указ Президента України від 28 квітня 2014 року № 449 «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України». — [Електронний ресурс]. — Режим доступу : http://zakon5.rada.gov.ua/laws/show/449/2014.

References (transliterated and translated):

1. *Voloshyna, N. M.* Poniattia «bezpeka informatsii» ta «informatsiyna bezpeka» v suchasnomu naukovomu prostori (The concept of «security of information» and «information security» in the modern scientific space) // Suchasni informatsiyni tekhnolohiyi u sferi bezpeky ta oborony (Modern Information Technologies in the Field of Security and Defense), 2010, No 2 (8), P. 53–56 [in Ukrainian].
2. *Dorosh, L.* Informatsiyno-psykholohichna bezpeka osoby, suspilstva ta derzhavy : novitni vyklyky mizhnarodniy bezpetsi (Informational and psychological security of individuals, society and the state : new challenges to international security) // Ukrainska natsionalna ideia : realii ta perspektyvy rozvytku (Ukrainian National Idea : Reality and Prospects), 2013, Issue 25, P. 107–112 [in Ukrainian].
3. Istoriya informatsiyno-psykholohichnoho protyborstva : pidruch. (History of informational and psychological confrontation : A Textbook) / *Zharkov, Ya. M., Kompantseva, L. F., Ostroukhov, V. V.* [et.al.]; under the editorship of *Ye. D. Skulysh*. Kyiv, 2012, 212 p. [in Ukrainian].
4. *Kyryliuk, O. V.* Zabezpechennia informatsiynoi bezpeky v umovakh rozbudovy informatsiynoho suspilstva v Ukrayini (Ensuring information security in terms of information society development in Ukraine) // Aktualni problemy derzhavy i prava (Pressing Problems of State and Law), 2014, Issue 74, P. 159–164 [in Ukrainian].
5. *Kuchma, L. O.* Informatsiyno-psykholohichna bezpeka : teoretyko-metodolohichni pidkhody ta dyskusii (Informational and psychological security : theoretical and methodological approaches and discussions). [Electronic resource]. Available at : http://www.crime-research.ru/library [in Ukrainian].
6. *Marushchak, A.* Shchodo poniattia «informatsiini resursy derzhavy» (On the concept of «State Information Resources») // Informatsiyna bezpeka liudyny, suspilstva, derzhavy (Information security of man, society and the state), 2009, No 1 (1), P. 11–16 [in Ukrainian].
7. *Nalyvaiko, L. R.* Informatsiina bezpeka ta informatsiina polityka v Ukraini : konstytutsiino-pravovyi aspekt (Information security and information policy in Ukraine : constitutional and legal aspect) // Bulletin of Zaporizhzhya State University, 2003, No 1, P. 3–5 [in Ukrainian].
8. ND TZI 1.1-003-99. Terminolohiya v haluzi zakhystu informatsii v kompiuternykh systemakh vid nesanktsionovanoho dostupu (ND TZI 1.1-003-99. Terminology in the field of information security in computer systems from unauthorized access) [Electronic resource]. Available at : http://tzi.com.ua/downloads/1.1-003-99.pdf [in Ukrainian].
9. *Panchenko, V. M.* Humanitarna ta tekhnolohichna skladovi u vyznachenni poniattia «informatsiyna bezpeka» (Humanitarian and technological components in the definition of «information security» concept) // Topical problems of manag-

ing information security of the state : Proceedings of scientific and practical conference, March 17, 2010, Kyiv. P. 205–206 [in Ukrainian].

10. Ukaz Prezydenta Ukrayiny vid 28 kvitnya 2014 roku № 449 «Pro zakhody shchodo vdoskonalennia formuvannia ta realizatsii derzhavnoii polityky u sferi informatsiynoii bezpeky Ukrainy» (Decree of President of Ukraine from April 28, 2014 No 449 «On measures to improve the formation and implementation of state policy in the field of information security of Ukraine). [Electronic resource]. Available at : http://zakon5.rada.gov.ua/laws/show/449/2014. [in Ukrainian].

Стаття надійшла до редакції 25.10.16

С. Мельник

Ґенеза основних понять інформаційної безпеки в контексті професійної підготовки у вищому навчальному закладі

У статті висвітлено ґенезу і сутність основних понять інформаційної безпеки в контексті професійної підготовки фахівців інформаційної безпеки та кібернетичної безпеки у вищому навчальному закладі, запропоновано авторське бачення співвідношення між поняттями «інформаційна безпека», «безпека інформації», «інформаційно-психологічна безпека», «забезпечення інформаційної безпеки», «захист інформації» та «інформаційно-психологічний захист». Розкрито основні складові поняття інформаційної безпеки людини, суспільства і держави в контексті формування професійної компетентності майбутніх фахівців у вищому навчальному закладі, структуровано нові конструкції базових понять із забезпечення інформаційної безпеки, які орієнтовані на сучасну практику інформаційного протиборства на рівні людини, суспільства, держави.

Ключові слова: інформаційна безпека, понятійно-категоріальний апарат, професійна підготовка.

S. Melnyk

Genesis of Basic Concepts of Information Security in the Context of Professional Training in Higher Dducation

The article highlights the origin and nature of the basic concepts of information security in the context of professional training of specialists in the fields of information security and cyber security at higher schools and proposes the copyright vision of the relation between the concepts of «information security», «security of information», «informational and psychological security», «ensuring information security», «protection of information» and «informational and psychological protection». The basic components of the concept of information security of man, society and the

state in the context of future professionals' professional competence formation in higher education are revealed; new designs of basic concepts of information security, which focused on the current practice of information confrontation at the levels of man, society and the state are structured.

Key words: information security, conceptual and categorical apparatus, professional training.

Рецензент – доктор педагогічних наук,
професор А. В. Литвин