УДК 378.016:004.056.5

Мельник Сергій Володимирович
кандидат технічних наук, доцент, докторант
Національна академія Служби безпеки України, м. Київ, Україна
ua.sergii.melnyk@gmail.com

ПОНЯТІЙНО-КАТЕГОРІАЛЬНИЙ АПАРАТ У СИСТЕМІ ПРОФЕСІЙНОЇ ПІДГОТОВКИ МАЙБУТНІХ ФАХІВЦІВ З КІБЕРБЕЗПЕКИ

Анотація. У статті розглянута проблема визначення й обґрунтованості понятійно-категоріального апарату професійної діяльності із забезпечення кібернетичної безпеки в контексті реформування вищої освіти України та впровадження нової спеціальності «Кібербезпека» галузі знань «Інформаційні технології», актуальності завдання організації професійної підготовки для державного і приватного сектору національної системи кібербезпеки тощо. Розглянуті відомі в Україні та закордоном дефініції понять «інформаційна безпека» та «кібернетична безпека», систематизовано та деталізовано їх складові. Проведено порівняння цих понять, визначено зв'язок і розбіжності між ними, спираючись на мету, завдання та технологічні особливості професійної діяльності у цих сферах, а також родові поняття «загроза», «безпека» та «забезпечення безпеки». Обґрунтовано підхід до визначення поняття «кібербезпека» та запропоновано його авторське бачення з урахуванням технічної і гуманітарної складової (комунікативні, політичні, соціологічні та психологічні аспекти).

Ключові слова: інформаційна безпека; кібербезпека; професійна підготовка.

1. ВСТУП

Постановка проблеми. Сучасні світові тенденції свідчать про поглиблення та розширення сфер професійної діяльності й освіти, що пов’язане із значною динамікою розвитку інформаційної складової життєдіяльності людини і суспільства.

Стан розвитку інформаційного суспільства й інформаційної інфраструктури України визначає професійні вимоги державних і приватних структур на підготовку фахівців з питань захисту інформації й інформаційно-психологічного протиборства технічних і гуманітарних спеціалізацій. Зазначені напрями професійної діяльності суттєво розвиваються в останні три десятиліття, а сфера кібербезпеки, починаючи з 2000-х років (при цьому поняття національної системи кібербезпеки в Україні законодавчо визначено лише у 2016 році). Відповідно, понятійно-категоріальний апарат професійної діяльності у сфері кібербезпеки не є остаточно визначеним як на законодавчому, так і практичному і науковому рівнях.

Зрозуміло, що кібербезпека – це не лише технології, а передусім людський ресурс. І на сьогодні більшість представників відомств, задіяних у національній системі кібербезпеки України, відзначають все ж таки незадовільний стан кадрового забезпечення фахівцями відповідних спеціалізацій.

У зв'язку з 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».

При цьому зауважимо, що предметна сфера інформаційної безпеки включає в себе широкий спектр питань відносно іміджу держави, забезпечення інформаційних прав і свобод громадян, забезпечення інформаційного суверенітету, захисту інформації, правоохоронної діяльності, відповідно, можна стверджувати і про адекватну «фахову широту» соціального замовлення на освіту у цій сфері.

Тому виходячи з позиції адекватності освітніх послуг вимогам ринку праці, для визначення змістової частини нової спеціальності «Кібербезпека», обґрунтування можливих спеціалізацій в рамках цієї та інших спеціальностей, набуває особливої ваги питання співвідношення між поняттями «інформаційна безпека» та «кібербезпека».

Аналіз останніх досліджень і публікацій. Наукове осмислення тематики інформаційної і кібернетичної безпеки проведено багатьма науковцями, наприклад [1–8] в межах технічних і гуманітарних наук, що обумовлені завданнями забезпечення громадської, національної і міжнародної безпеки. Натомість серед практиків, науковців і особливо в освітньому середовищі України триває дискусія щодо співвідношення між поняттями «інформаційна безпека» та «кібернетична безпека», є актуальною потреба у визначенні базових і похідних категорій проблеми формування професійних компетентностей майбутніх фахівців із захисту інформації та інформаційно-психологічного протиборства в інформаційному та кібернетичному просторі.

Мета статті полягає у систематизації, деталізації та уточненні понятійно-категоріального апарату професійної діяльності із забезпечення кібернетичної безпеки.

Завданнями статті є розкриття співвідношень між такими поняттями як «інформаційна безпека» і «кібернетична безпека» через призму особливостей професійної діяльності із захисту інформації та інформаційного протиборства в інформаційному та кібернетичному просторах.

2. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

2.1 Сучасні підходи до розуміння інформаційної безпеки

Інформація протягом історії людства була і є основою для прийняття рішень на рівнях людини, суспільства та держави. У сучасних умовах розвитку інформаційного суспільства інформація розглядається як товар, що має цінність і боротьба за який постійно триває. Попри це, інформація є ефективним інструментом керуючого впливу на соціальні системи – людину, суспільні групи, суспільство за схемою «керуючий вплив – бажаний результат».

Як наслідок, інформація є важливим фактором у формуванні безпечного середовища як з точки зору людських відносин, так і забезпечення громадської, національної і міжнародної безпеки. У свою чергу, інформаційне протиборство – це природній стан в умовах конкуренції сучасного глобалізованого світу, а питанням забезпечення інформаційної та кібернетичної безпеки приділяється особлива увага в контексті збереження балансу інтересів на рівнях особи, суспільства, держави та міжнародного правопорядку.

У ст. 17 Конституції України закріплено, що захист суверенітету та територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу.

Інформаційна безпека в загальній системі забезпечення національної безпеки посідає особливе місце. Так у Доктрині інформаційної безпеки України (документ не чинний, підлягає переопрацюванню) зазначено, що інформаційна безпека є невід'ємною складовою кожної зі сфер національної безпеки, водночас є важливою самостійною сферою забезпечення національної безпеки. Тому відповідно до сфер національної

безпеки були визначені реальні та потенційні загрози інформаційній безпеці України у: зовнішньополітичній сфері; сфері державної безпеки; воєнній сфері; внутрішньополітичній сфері; економічній сфері; соціальній та гуманітарній сферах; науково-технологічній сфері; екологічній сфері.

На сьогодні поняття «інформаційна безпека» має чимало визначень, що пов'язано з різними підходами до його розуміння. Розглянемо деякі з них.

Найбільш відомим [1] є з пункту 13 Закону України «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки». «Інформаційна безпека» – це стан захищеності життєво важливих інтересів людини, суспільства й держави, за якого запобігається завдання шкоди через:

- неповноту, невчасність та невірогідність інформації, що використовується;
- негативний вплив;
- негативні наслідки застосування інформаційних технологій;
- несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації.

«Інформаційна безпека» – це захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією умови існування й розвитку людини, всього суспільства та держави [2].

«Інформаційна безпека» – це такий стан інформаційного розвитку та захищеності особи, суспільства, держави (духовного, правового, технічного), за якого сторонні інформаційні впливи не мають вирішального значення в прийнятті рішень, спрямованих на забезпечення власних (особистих, суспільних, державних) інтересів [3].

«Інформаційна безпека» – –це результат управління реальними чи (та) потенційними загрозами (небезпеками) з метою задоволення національних інтересів людини, суспільства та держави в інформаційній сфері [4].

«Інформаційна безпека» – це сукупність умов функціонування суб'єктів в інформаційній сфері та суб'єктивних можливостей їх усвідомлення й контролю [5].

За результатами аналізу наведених визначень доцільно звернути увагу на деякі аспекти побудови їх конструкцій.

По-перше. інформаційна безпека – це «стан захищеності», «захищеність», «стан інформаційного розвитку», «результат управління» та «сукупність умов». Звісно, кожен підхід має рацію, однак звернемо увагу на такі деталі.

На авторську думку, у широкому розумінні твердження «інформаційна безпека – це стан захищеності» є найбільш вдалим, оскільки у цьому випадку є можливість цей стан оцінити (виміряти) у якісних і кількісних показниках. Попри це, існує діяльність (забезпечення інформаційної безпеки), яка цей стан підтримує в умовах застосування реальних та потенційних, внутрішніх та зовнішніх деструктивних впливів. Взагалі безпека та забезпечення безпеки – це різні поняття, тому що безпека виражає характеристику певного стану, а забезпечення безпеки – дієву характеристику, тобто діяльність, спрямовану на підтримання вказаного стану.

По-друге, у наведених визначеннях, окрім першого, не розкривається суть загроз та напрямів забезпечення інформаційної безпеки (не визначені об'єкти захисту). У свою чергу, запропоновані узагальнення у першому з наведених визначень, на суб'єктивний погляд не повною мірою розкривають загрози людині, суспільству та державі через призму їх життєво важливих інтересів. На думку автора, потрібна окрема деталізація загроз інформаційній безпеці, яка навіть в узагальненому вигляді буде занадто громіздкою як для визначення поняття.

Спираючись на сказане, розглянемо наступне загальне визначення інформаційної безпеки.

«*Інформаційна безпека»* – це стан захищеності людини, суспільства та держави від реальних і потенційних, внутрішніх і зовнішніх загроз у інформаційному просторі, що спрямовані на порушення безпеки інформації й інформаційно-психологічної безпеки.

Де «*безпека інформації»* – це стан захищеності від загроз порушення конфіденційності, цілісності, автентичності (авторства) та доступності інформаційних ресурсів, змін штатних режимів роботи, засобів і систем інформаційної інфраструктури. Необхідний рівень (стан) безпеки інформації досягається за рахунок застосування методів, засобів та заходів захисту інформації, насамперед: спеціального діловодства та режиму (пропускного, внутрішньооб'єктового), технічного та криптографічного захисту інформації.

У свою чергу, «*інформаційно-психологічна безпека»* – це стан захищеності від загроз застосування впливів на свідомість та підсвідомість людини, громадянина і суспільства з метою внесення змін у їхню поведінку і світогляд. Як правило, інформаційно-психологічна безпека забезпечується в рамках інформаційно-психологічного протиборства із застосуванням активних заходів у інформаційному просторі, що базуються передусім на комунікативних можливостях *засобів масової комунікації* (преса, радіо, телебачення, інформаційні сервіси мобільного та стаціонарного зв'язку, мережі Інтернет) та *засобів масового впливу* (театр, кіно, література, масові зібрання).

У контексті сказаного звернемо увагу також на достатньо вживане поняття «інформаційний суверенітет». Закон України «Про Національну програму інформатизації» від 4 лютого 1998 р. № 74/98-ВР визначає його як «здатність держави контролювати і регулювати потоки інформації з поза меж держави з метою додержання законів України, прав і свобод громадян, гарантування національної безпеки держави». Зрозуміло, що поняття «інформаційного суверенітету» можна розглядати у якості результату забезпечення інформаційно-психологічної безпеки людини і суспільства як адекватний загрозам стан захищеності.

Розглянуті складові широко вживаного терміну «інформаційна безпека» (безпека інформації та інформаційно-психологічна безпека) поєднані суб'єктами захисту (людиною та суспільством) та інформаційним простором, однак об'єкти, методи, засоби та заходи захисту суттєво різняться, починаючи з визначення мети захисту. При цьому ці дві складові захисту людини і суспільства взаємопов'язані з точки зору комплексного підходу до вирішення проблеми, оскільки є взаємозалежними.

Підсумовуючи зазначимо, що в Україні та на пострадянському просторі «інформаційна безпека» – це широко вживаний термін у засобах масової інформації (особливо з часу проведення АТО), нормативно-правових актах, наукових джерелах та в побуті, який використовують як у розумінні безпеки інформації, так і інформаційно-психологічної безпеки. У країнах євроатлантичної спільноти термін «інформаційна безпека» у більшості пов'язують із безпекою інформації, а інформаційно-психологічну безпеку розглядають в рамках інформаційних війн як окрему тематику. Крім того, доцільно звернути увагу на те, що такі широко вживані та законодавчо закріплені в Україні терміни як «безпека інформації», «технічний захист інформації» та «криптографічний захист інформації» в західних країнах також не вживаються, а використовуються такі аналоги, як «інформаційна безпека», «комп'ютерна та мережева безпека», «ІТ безпека», «криптографія» та ін.

Напевне проблема термінології у сферах інформаційної та кібернетичної безпеки потребує уваги на державному рівні, а враховуючи сталі уявлення суспільства та кількість діючих нормативних документів, що використовують терміни інформаційної безпеки, потребуватиме значного часу на її вирішення. При цьому одним із найбільш

важливих завдань у вирішенні цієї проблеми можна вважати доцільність розмежування понять «інформаційна безпека», «безпека інформації» та «інформаційно-психологічна безпека».

2.2 Змістовий і дефінітивний аналіз поняття «кібербезпека»

На сьогодні термін «кібербезпека» отримав значне поширення в практичній діяльності, перш за все, в завданнях забезпечення громадської та міжнародної безпеки, а також у різних національних та міжнародних документах, включаючи і Україну [9].

Терміни з приставкою «cyber-» ще залишаються предметом відкритої дискусії. Вперше термін «кібернетика» введено в обіг древньогрецьким філософом Платоном для позначення мистецтва кормчого (мистецтва управління). У 1834 французький вчений Андре Марі Ампер використав цей термін для позначення не існуючої ще у той час науки про управління суспільством. Офіційною датою народження кібернетики як окремої науки вважається рік опублікування книги Норберта Вінера «Кібернетика» (1947) у якій він визначив кібернетику як науку «про управління і зв'язок у тварині і машині». У сучасному розумінні кібернетика – це наука про управління, зв'язок і переробку інформації.

Об'єктом дослідження сучасної кібернетики є кібернетичні системи, які розглядаються абстрактно (безвідносно до їх реальної природи), що дозволяє проводити дослідження технічних, біологічних, соціальних систем загальними методами. Кібернетична система представляється у вигляді сукупності взаємопов'язаних об'єктів – елементів системи, що здатні запам'ятовувати, обробляти інформацію та обмінюватись нею з іншими елементами та зовнішнім світом. Комп'ютер розглядається як універсальний перетворювач інформації, що здатний, запам'ятовуючи структуру іншої кібернетичної системи, виконувати її функції як перетворювача інформації. Саме ця якість робить його найфункціональнішою відомою кібернетичною системою та основним технічним засобом моделювання й вивчення інших кібернетичних систем будь-якої природи [6].

Відповідно, значна кількість вітчизняних і західних фахівців вважають, що слово «cyber» пов’язане з використанням інформаційних технологій і комп’ютерів, тобто пов’язане з кіберпростором.

Безмовно, *«кіберпростір»* (або *«кіберсередовище»*) є частиною більш широкого поняття «інформаційний простір», інформаційна інфраструктура якого обмежується комп’ютерними технологіями та телекомунікаційними мережами – *«автоматизованими системами»* (організаційно-технічними системами, що реалізують інформаційну технологію й об'єднують інформаційно-телекомункаційну систему, користувачів, обслуговуючий персонал та інформаційні ресурси), насамперед, мережею Інтернет. При цьому поняття «інформаційні ресурси» достатньо часто визначаються як *«актив»* – все, що представляє цінність для людини, суспільства та держави, наприклад, інформаційні (контент) та програмні ресурси.

Доцільно також звернути увагу на тлумачення поняття «кіберпростір» у широкому і вузькому розумінні [6], що важливо з точки зору практичних можливостей його захисту на рівні людини, суспільства, держави. Так, у вузькому розумінні сучасні дослідники ототожнюють кіберпростір з віртуальним простором (доступним програмним забезпеченням та інформаційними ресурсами), що не враховує його апаратну та мережеву програмну складову, яка в умовах України є «технологічно не прозорою».

Отже, тезаріус кібербезпеки інтегрований з поняттями безпеки інформації та інформаційно-сихологічної безпеки в законодавчому, технологічному та правоохоронному сенсах.

Вважається, що вперше термін «кібербезпека» у сучасному розуміння став використовуватись у 90-х роках минулого століття у США, коли ця проблема стала актуальною для країни. Більшість відомих визначень кібербеспеки [7, 8] ототожнюють це поняття виключно із завданнями забезпечення конфіденційності, цілісності та доступності інформації, тобто захистом інформації у кіберпросторі (кіберзахистом активів), не розглядаючи при цьому аспекти інформаційно-психологічного протиборства у кіберпросторі.

Діюча Рекомендація МСЕ-Т Х.1205 (МСЕ – Міжнародний союз електрозв'язку), прийнята у 2010 році визначає :

Кібербезпека це набір засобів, стратегії, принципи забезпечення безпеки, гарантії безпеки, керівні принципи, підходи до управління ризиками, дії, професійна підготовка, практичний досвід, страхування і технології, які можуть бути використані для захисту кіберсередовища (кіберпростору).

Ресурси організації включають під'єднані комп'ютерні пристрої, персонал, інфраструктуру, додатки, послуги, системи електрозв'язку і всю сукупність переданої та / або збереженої інформації у кіберпросторі. Тому кібербезпека полягає в спробі досягнення і збереження властивостей безпеки ресурсів організації, спрямованих проти реальних і потенційних загроз у кіберпросторі. При цьому загальні завдання забезпечення кібербезпеки передбачають забезпечення конфіденційності, цілісності та доступності інформації.

У міжнародному стандарті ISO/IEC 27032 «Guidelines for cybersecurity» під кібербезпекою розуміють властивість захищеності інформації (активів) також від загроз порушення конфіденційності, цілісності та доступності у кіберпросторі.

Далі розглянемо дефініції поняття «кібернетична безпека», які наведені в деяких національних стратегічних документах [7, 10].

У стратегії Франції, присвяченій питанням кібербезпеки, запропоновано таке визначення: кібербезпека – це бажаний стан інформаційної системи, за якого вона може протистояти подіям з кіберпростору, що можуть поставити під загрозу доступність, цілісність або конфіденційність даних, які зберігаються, обробляються або передаються, і пов’язаних з ними послуг, які ці системи пропонують або роблять доступними.

У німецькій стратегії під кібербезпекою розуміється деяка сукупність необхідних і відповідних заходів, результаті реалізації яких досягається шляхом мінімізації ризиків. При цьому в стратегії стверджується, що кібербезпека повинна базуватися на комплексному підході.

У Канаді стверджують, що з метою забезпечення найсучаснішого використання кіберпростору, який є стратегічним активом, необхідно передбачати і протистояти кіберзагрозам, що виникають. Відповідно до цього документа під кібербезпекою можна розуміти захист киберсистем від шкідливого неправильного використання та від інших деструктивних атак. З іншого боку, надано досить докладне визначення кібератаки (технічної реалізації загрози), а кібербезпека – це стан захищеності від цих атак.

У національній стратегійї кібербезпеки Туреччини міститься таке визначення: кібербезпека – це захист інформаційних систем, що входять до складу кіберпростору від нападів шляхом забезпечення конфіденційності, цілісності та доступності інформації, яка обробляється в цьому просторі, виявленням та протидією атакам.

У Нідерландах у рамках стратегії кібербезпеки запропоноване таке визначення. Кібербезпека – це сукупність зусиль щодо запобігання шкоди, яка може бути заподіяна

внаслідок збоїв у роботі інформаційно-комунікативних технологій (ІКТ) або неправильного їх використання, а також з відновлення ІКТ після реалізації цих загроз. До збоїв у стратегії відноситься зниження надійності ІКТ, обмеження доступності та порушення конфіденційності та/або цілісності інформації, що зберігається в ІКТ.

Стратегія кібербезпеки США 2011 року (перша редакція була у 2003 році) визначає контекст підходу до розуміння пріоритетів держави, способів досягнення безпечного кіберпростору та боротьби з кібератаками. У якості загроз визначено шантаж та вимагання коштів, шахрайство, крадіжки та експлуатацію дітей, крадіжки інтелектуальної власності. Дефініцій понять у документі не наведено.

Цей підхід,у рамках якого розглядаються лише питання забезпечення безпеки інформації (дії із захисту інформації) є зрозумілим, оскільки інформаційно-психологічне протиборство у більшості випадків відноситься до категорії національної, а не міжнародної безпеки, відповідно, стосується сфери компетенції спеціальних служб (соціально-політичної та військової сфери), які не набувають особливого розголосу.

У національній стратегії кібербезпеки України [9] запропоновано визначення не кібербезпеки, а забезпечення кібербезпеки як стану захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, що досягається комплексним застосуванням сукупності правових, організаційних, інформаційних заходів. Водночас дещо розмиті визначення загроз кібербезпеці, однак на авторську думку містять складові безпеки інформації та інформаційно-психологічної безпеки.

У цьому контексті зазначимо, що у стратегічних документах системи кібербезпеки США у військовій сфері [11] соціотехнічний простір розглядається я складова частина кіберпростору у рамках якого ідентифікують інформаційно-психологічні впливи (спеціальні інформаційні операції). Відповідно, інформаційно-психологічний аспект кібербезпеки має право на життя та може бути розглянутий через призму забезпечення безпеки людини, установ, підприємств і організацій усіх форм власності у кіберпросторі.

Так у ратифікованій Законом України від 7 вересня 2005 року №2824-IV Конвенції про кіберзлочинність визначені: правопорушення проти конфіденційності, цілісності та доступності комп’ютерних даних та систем; правопорушення, пов’язані з комп’ютерами; правопорушення пов’язані зі змістом (дитячою порнографією) – які є окремим випадком інформаційно-психологічного захисту людини (дитини) та суспільства; правопорушення, пов’язані з порушенням авторських та суміжних прав.

Підсумовуючи сказане, можна вважати, що поняття кібербезпеки лише трансформує існуючі підходи до визначення інформаційної безпеки, з однієї сторони обмежуючись лише кіберпростором як частиною інформаційного простору, а з іншої – розширюючись завдяки новим можливостям, притаманним лише кіберпростору.

Наприклад, Барановим О. А. у своїй роботі [1] було обґрунтовано дефініцію поняття «інформаційна безпека», яка знайшла в подальшому законодавче закріплення у Законі України «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки». Потім автором розглядається [7] кібербезпека як інформаційна безпека в умовах використання комп’ютерних систем та/або телекомунікаційних мереж (тобто кіберпростору) наступним чином.

Кібербезпека [7] – це такий стан захищеності життєво важливих інтересів особистості, суспільства і держави в умовах використання комп'ютерних систем та/або телекомунікаційних мереж, за якого мінімізується завдання їм шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки функціонування інформаційних технологій;

несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації.

На авторську думку, запропонований підхід є доречним, однак сформульоване визначення є достатньо громіздким і складним для сприймання за рахунок деталізації загроз та формування мети забезпечення кібербезпеки (мінімізація завдання шкоди). Крім того, загрози «використання неповної, невчасної та невірогідної інформації» можуть розглядатися як один із способів реалізації «негативних інформаційних впливів», що свідчить про наявність певного дублювання в запропонованій структурі визначення (дефініції).

Ще одним важливим аспектом, на який доцільно звернути увагу є факт глобальності кіберпростору, інтереси у захисті якого присутні не лише на національному, але і міжнародному рівні. Тому саме цей аспект буде відрізняти дефініції інформаційної і кібернетичної безпеки з точки зору визначення обєктів захисту.

Далі сформулюємо ще одне визначення *кібербезпеки* як стану захищеності людини, суспільства, держави та міжнародної спільноти від реальних і потенційних, внутрішніх і зовнішніх загроз у кіберпросторі, що спрямовані на порушення безпеки інформації й інформаційно-психологічної безпеки.

Звісно це визначення може бути уточнене через призму загроз безпеці людини, суспільства, держави та міжнародної спільноти у кіберпросторі, які потребують окремої деталізації.

Доцільно також звернути увагу на загрозу психофізичного (психогенного) впливу на людину, яка не завжди передбачають використання інформативних сигналів і фізичних полів для реалізації деструктивного впливу, тому відноситься лише до загроз кібербезпеки і не розглядається у випадку інформаційної безпеки.

Таким чином, є всі підстави для твердження, що поняття «кібербезпека» з технологічної точки зору і завдань забезпечення національної безпеки є безумовно складовою частиною поняття «інформаційна безпека», оскільки розглядаються ті ж самі загрози, методи, засоби і заходи захисту, реалізація яких (атаки) обмежується лише технологіями кіберпростору. При цьому ті ж самі технологічні особливості є підставою і для розгляду кібербезпеки як окремої категорії, що відноситься, насамперед, до завдань забезпечення громадської та міжнародної безпеки.

У межах галузевих досліджень інформаційна безпека традиційно розглядається як невід'ємна частина політичної, економічної, оборонної та інших складових національної безпеки. Проте, кібербезпеку як технологічну складову інформаційної безпеки, виходячи з транскордонності кібернетичного простору та можливостей його анонімного використання, доцільно віднести до самостійного наднаціонального виду суспільної безпеки, що стосується життєво важливих інтересів людини та міжнародної спільноти. Оскільки в умовах використання принципу відкритості кіберпростору забезпечити на національному рівні кіберзахист не представляється можливим. Крім того, зрозуміло, що існування відкритого, стабільного і захищеного кіберпростору неможливе без ефективної співпраці з питань забезпечення кібербезпеки за участі громадян, бізнесу, держави, а також міжнародної співпраці у військовій та правоохоронній сфері.

Натомість, широко вживане у світі поняття «кібербезпека» визначає найбільш важливі для міжнародної спільноти проблеми системної координації дій щодо попередження, виявлення та реагування на кіберінциденти (атаки), протидії кіберзлочинності (невійськової сфери) та захисту критичної інформаційної інфраструктури (передусім військової сфери). При цьому поняття забезпечення кібербезпеки не охоплює проблеми перевірки та контролю лояльності та

благонадійності персоналу, організаційних заходів безпеки паперового та електронного спеціального діловодства, захисту мовної інформації на об'єктах інформаційної діяльності, заходів управління інформаційною безпекою, що визначенні в міжнародних стандартах з управління інформаційною безпекою (а точніше управління захистом інформації) серії ISO/IEC 270k «Information technology Security techniques – Information security management systems». Звернемо також увагу на відомий міжнародний стандарт CobiT (Control Objectives for Information and related Technology), який використовує поняття управління інформаційними технологіями (IT), а не управління кібербезпекою.

Тому на авторську думку, поняття кібербезпеки не є сучасним тлумаченням відомого терміна «інформаційна безпека», оскільки навіть у серії діючих стандартів ISO/IEC 270k термін кібербезпека використовується лише в одному стандарті ISO/IEC 27032:2012(E) «Information technology – Security techniques – Guidelines for cybersecurity. Хоча доцільно звернути увагу на те, що у Європейському Союзі в 2004 році було створено Європейське агентство з мережевої та інформаційної безпеки (European Network and Information Security Agency, ENISA), і практично весь спектр питань цієї організації присвячений лише кібербезпеці.

Отже, на сьогодні терміни «інформаційна безпека» та «кібербезпека» використовуються одночасно в сучасній практиці захисту інформації, наукових дослідженнях та освітній діяльності.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

За результатами дослідження питань інформаційної і кібернетичної безпеки можна зробити такі висновки.

1. В умовах становлення і розвитку національних систем інформаційної і кібернетичної безпеки до сьогоднішнього дня\ триває процес формування галузевого понятійно-категоріального апарату.

2. Завдяки здійсненому дослідженню на авторську думку вдалося систематизувати деталізувати та уточнити дефініції понять інформаційної і кібернетичної безпеки.

3. Отримані результати свідчать про необхідність вивчення питання щодо започаткування технічних і гуманітарних спеціалізацій для спеціальності «Кібербезпека», а також доцільності розгляду спеціалізацій «Інформаційна безпека» в рамках інших гуманітарних спеціальностей (наприклад, «Політологія», «Психологія», «Соціологія», «Менеджмент», «Право»). Попри це, здається доречним започаткування нової гуманітарної спеціальності «Інформаційна безпека» в рамках галузі знань «Воєнні науки, національна безпека, безпека державного кордону».

Перспективами подальшого розвитку напряму досліджень є наукове осмислення проблеми визначення соціального замовлення на зміст, якість та кількість майбутніх фахівців з інформаційної та кібернетичної безпеки, дослідження досвіду підготовки фахівців цієї сфери в інших країнах, концептуальних основ організації професійної підготовки майбутніх фахівців з кібербезпеки, неперервної освіти для національної системи кібернетичної безпеки зокрема.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Баранов О.А. Інформаційне право України: стан, проблеми, перспективи / О.А. Баранов. – К: БД "СофтПрес", 2005. – 316 с.

2. Кормич Б.А. Організаційно-правові основи політики інформаційної безпеки України : автореф. дис. на здобуття наук. ступеня докт. юрид. наук : спец. 12.00.07 «Адміністративне право і процес: фінансове право; інформаційне право» Б. А. Кормич. – Х., 2004. – 42 с.
3. Панченко В. М. Гуманітарна та технологічна складові у визначенні поняття «інформаційна безпека» / В. М. Панченко // Актуальні проблеми управління інформаційною безпекою держави: зб. матер, наук.-прак. конф., 17 березня 2010 року, м. Київ. – К.: Наук.-вид. відділ НА СБ України. 2010. С. 205-206.
4. Максименко Ю. Є. Теоретико-правові засади забезпечення інформаційної безпеки України: дис. канд. юрид. наук: 12.00.01 / Ю. Є. Максименко. – К., 2007. – 186 с.
5. Тихомиров О.О. Забезпечення інформаційної безпеки як функція сучасної держави: моногр./ О.О. Тихомиров; заг. ред. Р. А. Калюжний. – Центр навч.-наук. та наук.-практ. вид.НА СБ України. 2014. – 196 с.
6. Мельник С.В. До проблеми формування понятійно-термінологічного апарату кібербезпеки / С.В. Мельник, О.О. Тихомиров, О.С. Лєсков // Збірник наукових праць Київського національного університету імені Тараса Шевченка. – К. : ВІКНУ, 2011. Вип. №30. С. 165-172.
7. Баранов О.А. Про тлумачення та визначення поняття «кібербезпека» / О.А. Баранов // Правова інформатика. – 2014. – №2(42). С. 54-62.
8. Скрипник Л.В. Щодо кібербезпеки / Л.В. Скрипник // СТСЗИ, – 2013р. – вип. 2(24). С. 126-130.
9. Указ Президента України від 15 березня 2016 року «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про стратегію кібербезпеки України».
10. О. Шаховал. Рекомендації щодо розробки стратегії забезпечення кібербезпеки України / О. Шаховал, І. Лозова, С. Гнатюк // Захист інформації. – 2016. – Т. 18 №1. С. 57-65.
11. Даник Ю.Г.. Деякі підходи до формування системи підготовки кадрів для системи кібернетичної безпеки України України / Даник Ю.Г., Супрунов Ю.М. // Збірник наукових праць ЖВІ НАУ «Інформаційні системи». Випуск 5. 2011. С.5-22.

Матеріал надійшов до редакції 24.10.2016 р.

ПОНЯТИЙНО-КАТЕГОРИАЛЬНЫЙ АППАРАТ В СИСТЕМЕ ПРОФЕССИОНАЛЬНОЙ ПОДГОТОВКИ БУДУЩИХ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ И КИБЕРНЕТИЧЕСКОЙ БЕЗОПАСНОСТИ

Мельник Сергей Владимирович
кандидат технических наук, доцент, докторант
Национальная академия Службы безопасности Украины, г. Киев, Украина
ua.sergii.melnyk@gmail.com

Аннотация. В статье рассмотрена проблема определения и обоснования понятийно-категориального аппарата профессиональной деятельности по обеспечению кибербезопасности в контексте реформирования высшего образования Украины и внедрения новой специальности «Кибербезопасность» отрасли знаний «Информационные технологии», актуальности задачи организации профессиональной подготовки для государственного и частного сектора национальной системы кибербезопасности в том числе. Рассмотрены известные в Украине и за рубежом дефиниции понятий «информационная безопасность» и «кибернетическая безопасность», систематизированы и детализированы их составляющие. Проведено сравнение этих понятий, определена связь и расхождения между ними, опираясь на цель, задачи и технологические особенности профессиональной деятельности в этих сферах, а также родовые понятия «угроза», «безопасность» и «обеспечение безопасности». Аргументирован подход к толкованию понятия «кибербезопасность» и предложено его авторское видение с учетом технической и гуманитарной составляющих (коммуникативные, политические, социологические и психологические аспекты).

Ключевые слова: информационная безопасность; кибербезопасность; профессиональная подготовка.

CONCEPTUAL-CATEGORICAL APPARATUS IN THE SYSTEM OF PROFESSIONAL TRAINING OF FUTURE EXPERTS OF INFORMATION AND CYBER SECURITY

Sergii V. Melnik
PhD (technical sciences), associate professor, doctoral candidate
National Academy of the Security Service of Ukraine
ua.sergii.melnyk@gmail.com

Abstract. The article deals with the problem of definition and validity of concepts and categories of professional activities to ensure cyber security in the context of the reform of higher education of Ukraine and introduction of new specialty "Cyber security" field of study "Information technology", the urgency of the problem of training for public and private sector national cyber security system and the like. Considered well-known in Ukraine and abroad the definition of the terms "information security" and "cyber security", systematized and detailed their components. A comparison of these concepts identifies the relationship and differences between them which based on the purpose, objectives and process features of professional activity in these areas as well as generic concepts of "threat", "safety" and "security". Grounded approach to the definition of "cyber security" and suggests its author's vision with regard to the technical and humanitarian aspects (communicative, political, sociological and psychological aspects).

Keywords: information security; cyber security; professional training.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Baranov O. A. Information law of Ukraine: condition, problems, perspective / O. A. Baranov. – K: BD “SoftPress”, 2005. – 316 p. (in Ukrainian).
2. Kormych B.A. Legal and organizational basis of the policy of information security of Ukraine : The studies for the degree of doctor of legal Sciences spec. 12.00.07 "Administrative law and process; financial law; information law" B.A.Kormych. – X., 2004. – 42 p. (in Ukrainian).
3. Panchenko V. M. Humanitarian and technological components in the definition of "information security" / Panchenko V. M. // Actual problems of information security management of the state: compendium, scientifically-practical conference, March 17, 2010, Kyiv. – K.: the scientific publication of the Department of NA SSU. 2010. p. 205-206. (in Ukrainian).
4. Maksymenko Y.Y. Theoretical-legal bases of ensuring of information security of Ukraine: thesis of the Candidate of Legal Sciences, 12.00.01 / Maksymenko Y.Y.– K., 2007. – 186 p. (in Ukrainian).
5. Tykhomyrov O.O. Providing of the information security as a function of the modern state: a monograph. / O.O. Tykhomyrov, general editorship is R.A. Kaliyzhnyi. - ed. & practical dept of the publication of NA SSU 2014. – 196 p. (in Ukrainian).
6. Melnyk S.V. To the problem of formation of the conceptual and categorical framework of cybersecurity / S.V. Melnyk, O.O. Tykhomyrov, O.S. Lienkov // Collection of scientific works of Taras Shevchenko Kyiv national University. – K. : WIKNU 2011. ex. №30. p. 165-172. (in Ukrainian).
7. Baranov O. A. On the interpretation and definition of "cybersecurity" / O. A. Baranov // Legal Informatics. – 2014. – №2(42). p. 54-62. (in Ukrainian).
8. Skrypnyk L.V. Regarding of cybersecurity / L. V. Skrypnyk // STSZI, 2013. – ex. 2(24). p. 126-130. (in Ukrainian).
9. Order of the President of Ukraine from March 15, 2016 "On the decision of the National Security and Defense Council of Ukraine on January 27, 2016" On the cyber security strategy of Ukraine." (in Ukrainian).
10. Shahoval. Guidelines for the development strategy for Ukraine cybersecurity / O. Shahoval, I. Lozova S. Gnatyuk // Information Security. - 2016 - Vol 18 №1. S. 57-65. (in Ukrainian).
11. Y. Danyk Some approaches to the formation of Ukraine system of training for cyber security systems / Y. Danyk, Y. Suprunov // Proceedings of the NAU ZMI "Information systems". Issue 5. 2011. S.5-22. (in Ukrainian).

Conflict of interest. The author has declared no conflict of interest.