ПРОБЛЕМИ ФОРМУВАННЯ ТА РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

DOI: 10.18372/2307-9061.64.16893
УДК 342.951:351.82 +32.019.51(045)

Л. М. Бєлкін,
кандидат технічних наук, старший науковий співробітник, адвокат
ORCID ID: https://orcid.org/0000-0001-8672-8147

Ю. Л. Юринець,
доктор юридичних наук, професор
ORCID ID: https://orcid.org/0000-0003-0281-3251

М. Л. Бєлкін,
кандидат юридичних наук, адвокат
ORCID ID: https://orcid.org/0000-0003-0805-9923

Є. В. Криволап,
здобувач вищої освіти третього (освітньо-наукового) рівня
ORCID ID: https://orcid.org/0000-0003-2599-2520

СПІВВІДНОШЕННЯ ПОНЯТЬ «ІНФОРМАЦІЙНА БЕЗПЕКА», «БЕЗПЕКА ІНФОРМАЦІЇ», «КІБЕРБЕЗПЕКА» В КОНТЕКСТІ БЕЗПЕКОВИХ СТРАТЕГІЙ УКРАЇНИ 2020-2021 РОКІВ

Національний авіаційний університет
проспект Любомира Гузара, 1, 03680, Київ, Україна
E-mail: belkinleonid@ukr.net

Метою *статті є комплексний правовий та інформаційно-технологічний аналіз понять «інформаційна безпека», «безпека інформації», «кібербезпека» для обґрунтування підходу до створення центральної дефініції у сфері інформаційної безпеки та удосконалення системи протидії інформаційним загрозам.* ***Методи дослідження:*** *документальний аналіз, узагальнення правової інформації, інформації із сфери створення інформаційно-комунікаційних технологій, а також практики захисту інформації та протидії пропагандистським інформаційно-психологічним впливам.* ***Результати:*** *з урахуванням положень безпекових стратегій України 2020-2021 рр., а також наукової, практичної інформації та міжнародного досвіду запропонована структура «інформаційної безпеки держави» як центральної дефініції у сфері інформаційної безпеки. Доводиться, що поняття «інформаційна безпека» не може зводитися до безпеки окремої сукупності даних чи інформаційних систем чи до кібербезпеки. Забезпечення інформаційної безпеки поділяється на забезпечення безпеки інформації, у тому числі кібербезпеки, та забезпечення когнітивної безпеки. Запропоновано ввести у стабільний науковий і практичний оборот поняття «когнітивна безпека» як стійкість проти інформаційно-психологічних впливів на людину і суспільство. Зворотній зв'язок «кібербезпека» → «когнітивна безпека» пов'язаний із тим, що, кібератаки також активно використовуються державою-агресором як елемент спеціальних інформаційних операцій з метою маніпулятивного впливу на населення.* ***Обговорення:*** *комплексний правовий та інформаційно-технологічний аналіз понять «інформаційна безпека», «безпека інформації», «кібербезпека» дозволяє вибудувати ієрархію цих понять з метою удосконалення протидії інформаційним загрозам та пропагандистським інформаційним операціям.*

Ключові слова: *інформаційна безпека; безпека інформації; кібербезпека; інформаційна загроза; когнітивна безпека.*

Постановка проблеми та її актуальність. Протягом 2020-2021 рр. в Україні прийнята низка безпекових стратегій, зокрема: Стратегія національної безпеки України від 14.09.2020 р., затверджена Указом Президента України від 14.09.2020 р. № 392/2020; Стратегія воєнної безпеки України від 25.03.2021 р. (Указ від 25.03.2021 р. № 121/2021); Стратегія кібербезпеки України від 14.05.2021 р. (Указ від 26.08.2021 р. № 447/2021); Стратегія інформаційної безпеки від 15.10.2021 р. (Указ від 28.12.2021 р. № 685/2021). Однією із цілей прийняття цих Стратегій[1] є інституалізація термінології у цій сфері. Однак це питання до кінця не вирішене, оскільки не усунені певні суперечності у термінології в правових актах, науці та практиці.

Разом із тим, як зазначається у статті [1], термінологія займає особливе місце в збереженні та передаванні знань, оскільки саме на неї припадає основне інформаційне навантаження. Як зазначається у статті [2, с. 7], з поняттям «інформаційна безпека» склалася парадоксальна ситуація. З одного боку, термін «інформаційна безпека» широко використовується в наукових публікаціях, навчальній літературі та законодавчих документах різного рівня, з іншого боку, це поняття досі не має однозначного розуміння. Як зазначає D. Schatz (із співавторами), є досить мало розуміння поняття «кібербезпека», що потенційно може викликати значні проблеми в контексті організаційної стратегії, бізнес-цілей або міжнародних угод [3]. Отже, поставлена проблема є актуальною.

Аналіз досліджень і публікацій з проблеми. Згідно ч. 1 ст. 17 Конституції України, захист суверенітету і територіальної цілісності України, забезпечення її економічної та *інформаційної безпеки* є найважливішими функціями держави, справою всього Українського народу.

Разом із тим, в науковій літературі опублікована велика кількість робіт, які, використовуючи поняття «інформаційна безпека», фактично спрямовані на певні локальні питання з цієї сфери, наприклад: «інформаційна безпека» підприємств і безпеки господарської діяльності [4-7 та ін.], «інформаційна безпека» бібліотеки [8], «інформаційна безпека» в органах внутрішніх справ [9], «інформаційна безпека» страхових компаній [10] та ін. Ці види «інформаційних безпек» явно не відповідають конституційному рівню правового регулювання і захисту.

В деяких випадках дослідження «інформаційної безпеки» зводиться до аналізу проблематики «кібербезпеки» [11, 12]. В статті [13, с. 55] розглядається співвідношення понять «безпека інформації» та «інформаційна безпека» в сучасному науковому просторі. Зазначається, що «на перший погляд, «безпека інформації» та «інформаційна безпека» тотожні за змістом, але насправді це далеко не відповідає істині. В статті [14, с. 301] «інформаційна безпека» розглядається на підставі міждисциплінарного підходу: як в контексті «захисту інформації», так і в контексті «захисту від інформації». В.М. Фурашев вважає, що немає особливої різниці, чому споживач отримав неповну, невірогідну, упереджену або спотворену інформацію: чи внаслідок порушення цілісності інформації, чи внаслідок викривлення інформації. Результат один: споживач отримав неповну інформацію, наслідком якої може бути її невірогідність, спотворення її сприйняття та висновків на основі цієї інформації [15].

Отже викладені різноманітні підходи потребують узагальнення.

Виклад основного матеріалу. Відповідно до визначення, наданого у Стратегії від 15.10.2021 р., інформаційна безпека України – складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформацій-

[1] Далі по тексту позначається дата прийняття відповідної Стратегії.

них операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом.

Отже, маємо офіційне визначення поняття «інформаційна безпека України». Це поняття має ознаки комплексності і враховує забезпечення прав і свобод людини на збирання, зберігання, використання та поширення інформації; гарантії перешкоджання поширенню недостовірної, необ'єктивної інформації, перешкоджання негативним інформаційним впливам, деструктивній пропаганді, іншим інформаційним операціям; захист цілісності інформації, перешкоджання її перекрученню та несанкціонованому поширенню.

Варто зазначити, що загрозами інформації у кіберпросторі є кіберзагрози, а відтак засобами протидії цим загрозам є заходи забезпечення кібербезпеки [16]. У цьому сенсі слід зазначити, що в Стратегії від 15.10.2021 р. не заперечується роль кібербезпеки в забезпеченні інформаційної безпеки. Ця роль враховується шляхом відсилання до Стратегії від 14.05.2021 р.

Порівнюючи розуміння «інформаційної безпеки» з міжнародно прийнятим, наприклад, використаним у програмному документі ЮНЕСКО «Інформація для всіх» (IFAP), 2001 рік[2], зазначимо, що у цьому документі вона розглядається в таких аспектах: захист конфіденційної інформації (у тому числі від несанкціонованого доступу); захист інформації від навмисних і ненавмисних дій з метою забезпечення зберігання світової інформаційної спадщини; захист від інформації негативного характеру; безпека даних особистого характеру; сумлінне використання інформації та захист прав інтелектуальної власності (цитується за статтею [8, с. 18]). Аналізуючи ці складові, можемо прийти до висновку, що положення Стратегії від 15.10.2021 р. відповідають позиції ЮНЕСКО. Натомість, з урахуванням поточних реалій, в Стратегії більш чітко наголошено на небезпеках не просто поширення інформації негативного характеру, а небезпеках деструктивного впливу цієї інформації та спеціальних інформаційних операцій.

Отже, поняття «інформаційна безпека» не може зводитися до безпеки окремої сукупності даних чи інформаційних систем чи до кібербезпеки, хоча ці поняття і пов'язані між собою. Так, Є.О. Архипова у згаданій вище статті [2] вказує, що «інформаційна безпека» є ширшим за обсягом поняттям, ніж «безпека інформації» і включає в себе останню. Ототожнення цих понять вона пов'язує із тим, що вітчизняні та російські дослідники не враховують, що міжнародні стандарти, з яких запозичується визначення терміну information security, належать до сфери безпеки інформаційних технологій, де об'єктом захисту виступає саме інформація (а не людина, суспільство чи держава). Таке формальне запозичення призводить до суттєвої плутанини в термінологічних визначеннях [2, с. 8].

Так, дослідниця зазначає, що у стандарті BS ISO/IEC 17799 Information security характеризується забезпеченням конфіденційності, цілісності та доступності інформації, а в ISO/IEC 27001 – як «всі аспекти, пов'язані з визначенням, досягненням та підтримкою конфіденційності, цілісності, доступності, невідмовності, підзвітності, автентичності та достовірності інформації чи засобів її обробки». Дж. Фрулінгер (J. Fruhlinger) [17] також звертає увагу на так звану тріаду ЦРУ як основні складові безпеки інформації: конфіденційність, цілісність і доступність. Усі ці міркування стосуються виключно поняття «безпека інформації».

Згідно ч. 1 ст. 1 Закону України «Про інформацію», інформація – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

Отже, захисту підлягає інформація не тільки в електронному вигляді, а на будь-якому носії. Зокрема, Abi Tyas Tunggal та Kaushik Sen наголошують, що «*незалежно від того, як зберігається ваша інформація*, вашій організації потрібні відповідні засоби контролю безпеки, щоб запобігти несанкціонованому доступу» [18]. Отже, кібербезпека є окремим випадком загального поняття безпеки інформації, але такої інформації, яка обертається у кіберпросторі. При цьому причиною підвищеної уваги саме до кі-

[2] https://www.nas.gov.ua/UA/Messages/Pages/View.aspx?MessageID=6522

берзагрозам і кібербезпеки є дедалі зростаюча роль обігу інформації в комп'ютерних системах і електронно-комунікаційних мережах.

Як зазначено в Стратегії від 14.05.2021 р., XXI століття знаменується активним формуванням шостого технологічного укладу та ризиками, з якими стикається цивілізація внаслідок упровадження новітніх технологій. Питома вага кіберзагроз зростає і ця тенденція в міру розвитку інформаційних технологій та їх конвергенції з технологіями штучного інтелекту в найближче десятиліття посилюватиметься… Кіберпростір разом з іншими фізичними просторами визнано одним з можливих театрів воєнних дій.

Засадничим правовим актом в Україні у сфері забезпечення кібербезпеки є Закон України від 05.10.2017 р. № 2163-VIII «Про основні засади забезпечення кібербезпеки України» (далі – ЗУ № 2163-VIII). У пункті 5 ст. 1 ЗУ № 2163-VIII кібербезпека визначена як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. У пункті 6 ст. 1 ЗУ № 2163-VIII кіберзагроза визначена як наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів.

У Стратегії від 14.05.2021 р. загрози кібербезпеці України конкретизовані наступним чином: гібридна агресія РФ проти України у кіберпросторі; кіберзлочинність; організовані та спонсоровані урядами інших держав кібератаки, поєднані з кібершпигунством та здійсненням розвідувально-підривної діяльності; використання терористичними організаціями кіберпростору для вчинення актів кібертероризму, фінансової та іншої підтримки терористичної діяльності.

Із загостренням воєнної ситуації наростають і ризики у кіберпросторі [19]. У своєму виступі 29.12.2016 року на засіданні РНБО, присвяченому розгляду основних засад інформаційної безпеки нашої держави, Президент України зазначив, що тільки за останні два місяці 2016 року на об'єктах п'яти відомств і 31 державного інформаційного ресурсу було здійснено близько 6500 спланованих кібератак[3]. За звітом американської компанії Microsoft, після початку широкомасштабного збройного вторгнення РФ в Україну 24.02.2022 року російські хакери скоїли майже 240 кібератак проти України – підприємств та державних установ. Атаки часто були спрямовані на знищення комп'ютерних систем, але деякі також були спрямовані на збирання розвідувальних даних або поширення дезінформації[4].

Тому держава мусить вживати заходи протидії кіберзагрозам. Як зазначено в Стратегії від 14.05.2021 р., критично зростає роль кібербезпеки в процесах цифрової трансформації держави.

Разом із тим, як наголошує професор Г.Г. Почепцов, усі держави без винятку приділяють багато уваги кібербезпеці і мало тому, що можна позначити терміном «когнітивна безпека». У кібербезпеці захищають кіберресурси, у когнітивній безпеці – розум людини. Ми живемо у світі пропаганди, яка заважає нам бачити реальність [20]. Обробка інформації людиною природно підпорядковується певним когнітивним механізмам. Записані в наших головах схеми дозволяють не виконувати черговий раз аналіз, даючи можливість спиратися на введені раніше схеми [21, с. 521]. Ситуація, коли людина приречена користуватися нав'язаними їй схемами, гарантує переведення людини на іншу картину світу. Зокрема, той же професор Г.Г. Почепцов стверджує, що пропаганда робить ментальну операцію, замінюючи одні сенси на інші, причому робить це непомітно для «пацієнта»… При цьому, іноді цей сенс буде потрібен не сьогодні, а завтра, але для цього його слід запустити вже сьогодні [22]. Тобто, когнітивна

[3] https://www.pravda.com.ua/news/2016/12/29/7131254/mode_amp/

[4] https://www.slovoidilo.ua/2022/04/28/novyna/bezpeka/rosijski-xakery-pochatku-vijny-skoyily-majzhe-240-kiberatak-proty-ukrayiny-microsoft.

операція, безперечно, спрямована на зміну моделі світу людини [21, с. 170].

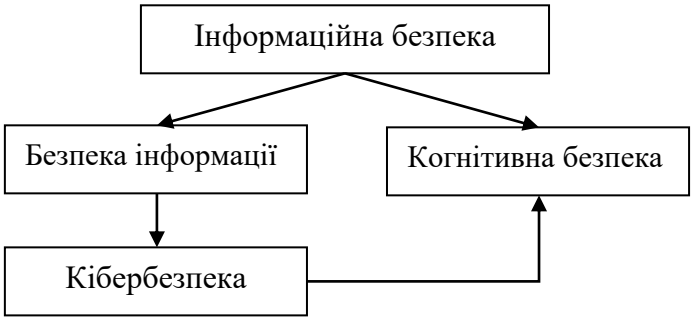
У статті [23] зазначається, що у когнітивній війні людська свідомість стає полем бою. Мета полягає в зміненні не лише того, що думає людина, а й того, як вона думає і діє. При успішному проведенні вона формує і впливає на індивідуальні і групові думки і поведінку на користь тактичних або стратегічних завдань агресора. У доповіді для військового комітету Конгресу США відомий експерт Rand-Corporation Ренд Валтцман (Rand Waltzman) обґрунтовує нагальну потребу у когнітивній безпеці (COGSEC). Пролунало це у контексті інформаційної війни, яку розв'язала Москва проти Заходу з використанням найновіших засобів комунікації та мережевої зброї. Термін когнітивна безпека вживається, аби підкреслити загрози й ризики, які пов'язані з пізнавальною діяльністю, негативними впливами мас-медіа, перебуванням людини у віртуальній реальності [24].

Професор М.В. Маркова [25, с. 7] зазначає, що інформаційно-психологічний вплив може викликати зрушення в цінностях, життєвих позиціях, орієнтирах, світогляді особистості. Такі зміни зумовлюють вияви девіантної антисоціальної поведінки й становлять небезпеку вже для суспільства й держави. Медіа-аналітик Ксенія Ілюк [26] також наголошує, що інформаційно-психологічний вплив завжди здійснюється з метою зміни поведінки. Тобто кожен фейк, провокація чи спекуляція у своїй сукупності має штовхати до дії. У публікації 2014 р. латвійський дослідник Янис Берзиньш (Jānis Bērziņš) наголошував, що «російський погляд на сучасну війну ґрунтується на ідеї, що основним полем бою є погляди, і, як наслідок, у війнах нового покоління має домінувати інформаційно-психологічна війна, з метою… змусити військове та цивільне населення супротивника підтримати нападника на шкоду власному уряду та країні» [27].

Також слід зазначити, що у Стратегії від 15.10.2021 р. надано визначення «інформаційна загроза» – це «потенційно або реально негативні явища, тенденції і чинники інформаційного впливу на людину, суспільство і державу, що застосовуються в інформаційній сфері з метою унеможливлення чи ускладнення реалізації національних інтересів та збереження національних цінностей України і можуть прямо чи опосередковано завдати шкоди інтересам держави, її національній безпеці та обороні». Тобто, додатково наголошується на неприйнятності негативних впливів на свідомість людини і суспільства.

У статті [28] авторка зазначає, що В.О. Голубєв [29] розуміє під інформаційною безпекою людини, суспільства, держави такий стан їхньої інформаційної озброєності (мається на увазі духовної, інтелектуальної, моральноетичної, політичної), за якого ніякі інформаційні впливи на них неспроможні викликати деструктивні думки і дії, що призводять до негативних відхилень на шляху стійкого прогресивного розвитку названих суб'єктів. Цю слушну точку зору можна було б вважати цілком справедливою до визначення стану когнітивної безпеки.

Наведемо схему запропонованої структури інформаційної безпеки.



Зворотній зв'язок «кібербезпека» → «когнітивна безпека» пов'язаний із тим, що, як зазначено у Стратегії від 14.05.2021 р., кібератаки також активно використовуються державою-агресором як елемент спеціальних інформацій-

них операцій з метою маніпулятивного впливу на населення.

Висновки. З урахуванням положень безпекових стратегій України 2020-2021 років, а також наукової, практичної інформації та міжнародного досвіду запропонована структура «інформаційної безпеки держави» як центральної дефініції у сфері інформаційної безпеки. Запропоновано ввести у стабільний науковий і практичний оборот поняття «когнітивна безпека» як стійкість проти інформаційно-психологічних впливів на людину і суспільство.

Література

1. Іленков А. Термінологія та її роль у представленні знань. Вісник Нац. ун-ту «*Львівська політехніка*». Серія «Проблеми української термінології». 2009. № 648. С. 24–29.

2. Архипова Є.О. Соціально-філософське осмислення поняття «інформаційна безпека». *Вісник Нац. технічного ун-ту України «Київський політехнічний інститут». Філософія. Психологія. Педагогіка.* 2011. № 3. С. 7-11.

3. Schatz D., Bashroush R., Wall J. Towards a Mor ds a More Representativ esentative Definition of Cyber Security e Definition of Cyber Security. *Journal of Digital Forensics, Security and Law*. 2017. № 2. P. 54-74.

4. Абакумов В.М. Інформаційна безпека підприємництва як об'єкт адміністративно-правової охорони. *Форум права.* 2012. № 4. С. 10-16.

5. Нечай Л.О. Інформаційна безпека суб'єктів господарювання та фактори її розвитку. *Управління розвитком.* 2013. № 17. С. 145-148.

6. Шопін А.Ю. Інформаційна безпека як фактор забезпечення конкурентоспроможності підприємства. *Управління розвитком.* 2013. № 17. С. 155-157.

7. Северина С.В. Інформаційна безпека та методи захисту інформації. *Вісник Запорізького нац. ун-ту. Економічні науки.* 2016. № 1. С. 155-161.

8. Бобришева О. Інформаційна безпека бібліотеки: проблеми та шляхи формування. *Вісник Книжкової палати.* 2010. № 12. С. 18-20.

9. Гуренко-Вайцман М.М. Рецензія на монографію О.В. Бойченка «Інформаційна безпека в органах внутрішніх справ України (організаційно-правові засади)». *Форум права.* 2009. № 3. С. 738-740.

10. Жабинець О.Й. Захист інформації та інформаційна безпека страхових компаній. *Економічний часопис-XXI.* 2014. № 7-8(2). С. 32-35.

11. Валюшко І.О. Інформаційна безпека України в контексті російсько-українського конфлікту: дис… канд. політичних наук: спец. 23.00.04. Київ, 2018. 210 с.

12. Антонюк В.В. Основні науково-методологічні підходи до дослідження державної політики інформаційної безпеки. *Інвестиції: практика та досвід*. 2013. № 20. С. 143-147.

13. Волошина Н.М. Поняття «безпека інформації» та «інформаційна безпека» в сучасному науковому просторі. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2010. № 2. С. 53-56.

14. Юринець Ю.Л., Сопілко І.М., Бєлкін Л.М., Бєлкін М.Л. Дослідження проблем інформаційної безпеки України на засадах міждисциплінарного підходу: соціологія, психологія, право. *Юридичний науковий електронний журнал. Електронне наукове фахове видання.* 2020. № 7. С. 300-307.

15. Фурашев В.М. Сутність та визначення понять «інформаційна безпека» і «безпека інформації». *Правова інформатика.* 2012. № 2. С. 51-59.

16. Сопілко І.М. Інформаційна безпека та кібербезпека: порівняльно-правовий аспект. *Наукові праці Нац. авіаційного ун-ту. Серія: Юридичний вісник «Повітряне і космічне право».* Київ: НАУ, 2021. № 2(59). С. 110-115. DOI: https://doi.org/10.18372/2307-9061.59.15603

17. Fruhlinger J. What is information security? Definition, principles, and jobs. CSO United States. 17.01.2020. URL: https://www.csoonline.com/ article/3513899/what-is-information-security-definition-principles-and-jobs.html

18. Abi Tyas Tunggal, Kaushik Sen. Cybersecurity Vs. Information Security. What's the Difference? 01.06.2022. UpGuard. URL: https://www.upguard.com/blog/cyber-security-information-security#:~:text=Cybersecurity

%20Vs.-,Information%20Security,integrity%2C%20and%20availability%20of%20information.

19. Сєдая Ю.С. Кібервійна: основні теоретичні положення. У зб.: Українське суспільство в умовах війни: виклики сьогодення та перспективи миротворення: матеріали Всеукр. наук.-практ. конф., м. Маріуполь, 9 чер. 2017 р. Маріуполь. ДонДУУ, 2017. С. 249-252.

20. Почепцов Г. Контр- не всегда плохо, особенно если это контрпропаганда. *Детектор медіа.* 02.06.2019. URL: https://ms.detector.media/mediaanalitika/post/22973/2019-06-02-kontr-ne-vsegda-plokho-osobenno-esly-jeto-kontrpropaganda/

21. Почепцов Г.Г. Теория коммуникации. Киев: Ваклер, 2001. 656 с.

22. Почепцов Г. Метапропаганда как доминирование пропаганды над идеологией, а не наоборот. *Хвиля.* 17.09.2018. URL: https://hvylya.net/analytics/society/metapropaganda-kak-dominirovanie-propagandyi-nad-ideologiey-a-ne-naoborot.html

23. Протидія когнітивній війні: інформованість і стійкість. НАТО Ревю. 20.05.2021. URL: https://www.nato.int/docu/review/uk/articles/2021/05/20/protidya-kogntivnj-vjn-nformovanst-stjkst/index.html

24. Рущенко І.П., Зубар Н.В. Війна інформації. Оборонний вісник. 2017. № 6. URL: https://maidan.org.ua/2017/09/kohnityvna-bezpeka-pohlyady-z-vashynhtonu-moskvy-kyjeva/ (Когнітивна безпека: погляди з Вашингтону, Москви і Києва).

25. Маркова М.В. Інформаційно-психологічна війна: медико-психологічні наслідки та стратегії протидії. *Проблеми безперервної медичної освіти та науки.* 2016. № 4. С. 6-10.

26. Ілюк К. Інформаційна війна – це не тільки фейки. *Детектор медіа.* 31.03.2022. URL: https://ms.detector.media/propaganda-ta-vplivi/post/29264/2022-03-31-informatsiyna-viyna-tse-ne-tilky-feyky/

27. Jānis Bērziņš. Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy. Policy Paper. April 2014. No 02. P. 5-13.

28. Ющук О. Інформаційна безпека користувачів мережі Інтернет. *Наукові записки Нац. ун-ту «Острозька академія». Сер.: Культура і соціальні комунікації.* 2009. Вип. 1. С. 224-231.

29. Голубєв В.О. Інформаційна безпека: проблеми боротьби з кіберзлочинністю. Запоріжжя, 2003. 250 с.

References

1. Ilenkov A. Terminolohiia ta yii rol u predstavlenni znan. Visnyk Nats. un-tu «Lvivska politekhnika». Seriia «Problemy ukrainskoi terminolohii». 2009. № 648. S. 24–29.

2. Arkhypova Ye.O. Sotsialno-filosofske osmyslennia poniattia «informatsiina bezpeka». Visnyk Nats. tekhnichnoho un-tu Ukrainy «Kyivskyi politekhnichnyi instytut». Filosofiia. Psykholohiia. Pedahohika. 2011. № 3. S. 7-11.

3. Schatz D., Bashroush R., Wall J. Towards a Mor ds a More Representativ esentative Definition of Cyber Security e Definition of Cyber Security. Journal of Digital Forensics, Security and Law. 2017. № 2. P. 54-74.

4. Abakumov V.M. Informatsiina bezpeka pidpryiemnytstva yak obiekt administratyvno-pravovoi okhorony. Forum prava. 2012. № 4. S. 10-16.

5. Nechai L.O. Informatsiina bezpeka subiektiv hospodariuvannia ta faktory yii rozvytku. Upravlinnia rozvytkom. 2013. № 17. S. 145-148.

6. Shopin A.Iu. Informatsiina bezpeka yak faktor zabezpechennia konkurentospromozhnosti pidpryiemstva. Upravlinnia rozvytkom. 2013. № 17. S. 155-157.

7. Severyna S.V. Informatsiina bezpeka ta metody zakhystu informatsii. Visnyk Zaporizkoho Nats. un-tu. Ekonomichni nauky. 2016. № 1. S. 155-161.

8. Bobrysheva O. Informatsiina bezpeka biblioteky: problemy ta shliakhy formuvannia. Visnyk Knyzhkovoi palaty. 2010. № 12. S. 18-20.

9. Hurenko-Vaitsman M.M. Retsenziia na monohrafiiu O.V. Boichenka «Informatsiina bezpeka v orhanakh vnutrishnikh sprav Ukrainy (orhanizatsiino-pravovi zasady)». Forum prava. 2009. № 3. S. 738-740.

10. Zhabynets O.I. Zakhyst informatsii ta informatsiina bezpeka strakhovykh kompanii. Ekonomichnyi chasopys-KhKhI. 2014. № 7-8(2). S. 32-35.

11. Valiushko I.O. Informatsiina bezpeka Ukrainy v konteksti rosiisko-ukrainskoho konfliktu: dys… kand. politychnykh nauk: spets. 23.00.04. Kyiv, 2018. 210 s.

12. Antoniuk V.V. Osnovni naukovo-metodolohichni pidkhody do doslidzhennia derzhavnoi polityky informatsiinoi bezpeky. Investytsii: praktyka ta dosvid. 2013. № 20. S. 143-147.

13. Voloshyna N.M. Poniattia «bezpeka informatsii» ta «informatsiina bezpeka» v suchasnomu naukovomu prostori. Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony. 2010. № 2. S. 53-56.

14. Yurynets Yu.L., Sopilko I.M., Bielkin L.M., Bielkin M.L. Doslidzhennia problem informatsiinoi bezpeky Ukrainy na zasadakh mizhdystsyplinarnoho pidkhodu: sotsiolohiia, psykholohiia, pravo. Yurydychnyi naukovyi elektronnyi zhurnal. Elektronne naukove fakhove vydannia. 2020. № 7. S. 300-307.

15. Furashev V.M. Sutnist ta vyznachennia poniat «informatsiina bezpeka» i «bezpeka informatsii». Pravova informatyka. 2012. № 2. S. 51-59.

16. Sopilko I.M. Informatsiina bezpeka ta kiberbezpeka: porivnialno-pravovyi aspekt. Naukovi pratsi Nats. aviatsiinoho un-tu. Seriia: Yurydychnyi visnyk «Povitriane i kosmichne pravo». Kyiv: NAU, 2021. № 2(59). S. 110-115.

17. Fruhlinger J. What is information security? Definition, principles, and jobs. CSO United States. 17.01.2020. URL: https://www.csoonline.com/ article/3513899/what-is-information-security-definition-principles-and-jobs.html

18. Abi Tyas Tunggal, Kaushik Sen. Cybersecurity Vs. Information Security. What's the Difference? 01.06.2022. UpGuard. URL: https://www.upguard.com/ blog/ cyber-security-information-security#:~:text=Cybersecurity%20Vs.-,Information%20Security,integrity%2C%20and%20availability%20of%20information

19. Siedaia Yu.S. Kiberviina: osnovni teoretychni polozhennia. U zb.: Ukrainske suspilstvo v umovakh viiny: vyklyky sohodennia ta perspektyvy myrotvorennia: materialy Vseukrainskoi naukovo-praktychnoi konferentsii, m. Mariupol, 9 chervnia 2017 r. Mariupol. DonDUU, 2017. S. 249-252.

20. Pocheptsov G. Kontr- ne vsegda ploho, osobenno esli eto kontrpropaganda. Detektor medIa. 02.06.2019. URL: https://ms.detector.media/mediaanalitika/ post/ 22973/2019-06-02-kontr-ne-vsegda-plokho-osobenno-esly-jeto-kontrpropaganda/

21. Pocheptsov G.G. Teoriya kommunikatsii. Kyiv: Vakler, 2001. 656 s.

22. Pocheptsov G. Metapropaganda kak dominirovanie propagandyi nad ideologiey, a ne naoborot. Hvilya. 17.09.2018. URL: https://hvylya.net/analytics/society/metapropaganda-kak-dominirovanie-propagandyi-nad-ideologiey-a-ne-naoborot.html

23. Protydiia kohnityvnii viini: informovanist i stiikist. NATO Reviu. 20.05.2021. URL: https://www.nato.int/docu/review/uk/articles/2021/05/20/protidya-kogntivnj-vjn-nformovanst-stjkst/index.html

24. Rushchenko I.P., Zubar N.V. Viina informatsii. Oboronnyi visnyk. 2017. № 6. URL: https://maidan.org.ua/2017/09/kohnityvna-bezpeka-pohlyady-z-vashynhtonu-moskvy-kyjeva/ (Kohnityvna bezpeka: pohliady z Vashynhtonu, Moskvy i Kyieva).

25. Markova M.V. Informatsiino-psykholohichna viina: medyko-psykholohichni naslidky ta stratehii protydii. Problemy bezperervnoi medychnoi osvity ta nauky. 2016. № 4. S. 6-10.

26. Iliuk K. Informatsiina viina – tse ne tilky feiky. Detektor media. 31.03.2022. URL: https://ms.detector.media/propaganda-ta-vplivi/post/29264/2022-03-31-informatsiyna-viyna-tse-ne-tilky-feyky/

27. Jānis Bērziņš. Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy. Policy Paper. April 2014. No. 2. P. 5-13.

28. Yushchuk O. Informatsiina bezpeka korystuvachiv merezhi Internet. Naukovi zapysky Nats. un-tu «Ostrozka akademiia». Ser.: Kultura i sotsialni komunikatsii. 2009. Vyp. 1. S. 224-231.

29. Holubiev V.O. Informatsiina bezpeka: problemy borotby z kiberzlochynnistiu. Zaporizhzhia, 2003. 250 s.

Leonid Belkin, Juliya Iurynets, Mark Belkin, Ievgenii Kryvolap

RELATIONSHIPS BETWEEN INFORMATION SECURITY, CYBER SECURITY IN THE CONTEXT OF UKRAINE'S SECURITY STRATEGIES 2020-2021

National Aviation University
Liubomyra Huzara Avenue, 1, 03680, Kyiv, Ukraine
E-mail: belkinleonid@ukr.net

The aim *of the article is a comprehensive legal and information technology analysis of the concepts of «information security», «cybersecurity» to justify the approach to creating a central definition in the field of information security and improving the system of combating information threats.* ***Research methods:*** *documentary analysis, generalization of legal information, information in the field of information and communication technologies, as well as practices of information protection and counteraction to propaganda information and psychological influences.* ***Results:*** *taking into account the provisions of the security strategies of Ukraine 2020-2021, as well as scientific, practical information and international experience, the structure of «information security of the state» as a central definition in the field of information security is proposed. It is argued that the concept of «information security» cannot be reduced to the security of a single set of data or information systems or to cybersecurity. Information security is divided into cybersecurity and cognitive security. It is proposed to introduce into stable scientific and practical circulation the concept of «cognitive security» as resistance to information and psychological influences on man and society. The feedback «cybersecurity» → «cognitive security» is due to the fact that cyber attacks are also actively used by the aggressor state as an element of special information operations to manipulate the population.* ***Discussion:*** *a comprehensive legal and information technology analysis of the concepts of «information security», «cybersecurity» allows you to build a hierarchy of these concepts in order to improve countering information threats and propaganda information operations.*

Key words: *information security; cybersecurity; information threat; cognitive security.*

Стаття надійшла до редакції 22.08.2022