DOI: 10.18372/2307-9061.59.15603
УДК 342.95:004.056.5(045)

І. М. Сопілко,
доктор юридичних наук, професор
ORCID ID: https://orcid.org/0000-0002-9594-9280

ІНФОРМАЦІЙНА БЕЗПЕКА ТА КІБЕРБЕЗПЕКА: ПОРІВНЯЛЬНО-ПРАВОВИЙ АСПЕКТ

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

Мета: *дослідити особливості та сутність кібербезпеки й інформаційної безпеки, зробити їх порівняльно-правовий аналіз.* ***Методи дослідження:*** *дослідження було проведене із застосуванням загальновизнаних методів наукового пізнання, таких як: аналітичний, порівняльно-правовий, системно-структурний та інші.* ***Результати:*** *досліджено поняття, суть, характеристики кібербезпеки та інформаційної безпеки, вказано на проблеми забезпечення їх функціонування, надано пропозиції щодо подолання таких проблем шляхом вдосконалення чинної законодавчої бази та гармонізації вітчизняного законодавства із міжнародними стандартами.* ***Обговорення:*** *дискусія у статті ведеться щодо відмежування поняття кібербезпеки від поняття інформаційної безпеки та особливостей їх правового регулювання у провідних країнах світу в порівнянні з нашою державою.*

Ключові слова: *кібербезпека; інформаційна безпека; кіберпростір; кіберзлочин; кібератака.*

Постановка проблеми та її актуальність. Роль інформаційної та кібербезпеки у сучасному світі є досить істотною. Сьогодні ми більше, ніж будь-коли, покладаємося на технології. У результаті цього збільшився обсяг створення цифрових даних. Сьогодні компанії та уряди зберігають велику частину важливої інформації на комп'ютерах і передають їх через Інтернет на інші комп'ютери. Пристрої і системи, що лежать у їх основі, мають вразливості, які при експлуатації підривають діяльність організацій і навіть цілих урядів.

Варто відзначити, що витік даних, викликаний проломами у кібербезпеці і недобросовістю систем інформаційної безпеки, може мати руйнівні наслідки для будь-якого бізнесу. Адже вказане може підірвати репутацію компанії через втрату довіри споживачів і партнерів. Також витік критично важливих даних може коштувати організації її конкурентних переваг. Надалі ж зазначена проблема може вплинути на корпоративні доходи через недотримання правил захисту конфіденційної інформації. Саме тому розуміння суті інформаційної та кібербезпеки, а також їх достатня правова врегульованість сьогодні є ключовим аспектом під час здійснення діяльності будь-якої організації.

Аналіз останніх досліджень і публікацій. Цій проблемі були присвячені роботи таких дослідників і вчених як Д. Шац, Д. Пушман, М. Барнетте, А. Сулайман, Р. Башроушу та інших.

Мета статті. В даному науковому дослідженні автор хоче розкрити суть і особливості понять «інформаційна безпека» та «кібербезпека», зробити їх порівняльно-правовий аналіз та надати критичну оцінку пов'язаних із ними прогалин у регулюванні.

Виклад основного матеріалу. Сьогодні терміни «інформаційна безпека» і «кібербезпека» у багатьох на слуху. Але далеко не кожен знає їх значення, а деякі люди, навіть працівники ІТ-галузі, взагалі використовують їх як синоніми, що є невірно.

Для початку необхідно надати визначення кожному із зазначених понять. Так, під інфор-

маційною безпекою (від англ. Information security, також InfoSec), Л. Ірвін розуміє те, як організації та окремі особи захищають свої цінні активи, в т.ч. бізнес-записи, особисті дані, результати інтелектуальної творчої діяльності тощо. Розглянуті дані зберігаються в різному вигляді і на різних носіях інформації (наприклад, на серверах і жорстких дисках, у хмарі або на особистих пристроях) [5].

Інформаційна безпека (далі – ІБ), на думку провідного технічного фахівця Дж. Фрулінгера, це набір методів, призначених для захисту даних від несанкціонованого доступу або змін, як при зберіганні, так і при передачі з одного приладу або фізичного розташування на інше. Іноді під ІБ також розуміють безпеку даних (від англ. Data security) [3].

Варто відзначити, що обговорювана захищена інформація може приймати будь-яку форму, в т.ч. електронну або фізичну; матеріальну (документація) або нематеріальну (знання). Саме збалансований захист конфіденційності, цілісність і доступність даних – це об'єкти захисту інформаційної безпеки. При цьому основний акцент зроблено на ефективній реалізації політики певної організації, без зниження продуктивності такого суб'єкта.

Найчастіше для забезпечення ІБ використовується структурований процес управління ризиками, який включає в себе:

– безпосередню оцінку потенційних ризиків і наступне прийняття рішення про методи боротьби із ними;

– виявлення потенційних загроз і вразливостей;

– відстеження активності, внесення правок при необхідності із метою врегулювання спірних моментів, а також для поліпшення наявних InfoSec-показників;

– розробку і подальше впровадження заходів безпеки з метою зниження обговорюваних ризиків.

Таким чином, можна сказати, що інформаційна безпека – це набір інструментів і методик, розроблених і використовуваних для захисту конфіденційної інформації від зміни, порушення, знищення і перевірки.

Тепер варто визначитися із поняттям кібербезпеки.

Згідно з Д. Шацом, Дж. Волл і Р. Башроушу, кібербезпека (вона ж комп'ютерна безпека і безпека інформаційних технологій) – це захист комп'ютерних систем і комп'ютерних мереж від розкриття даних, пошкодження та крадіжки їх обладнання, програмного забезпечення або електронної інформації, а також від порушення або неправильного спрямування наданих ними послуг [8, с. 56-57].

Також можна говорити і про те, що кібербезпека – це використання сучасних технологій, процесів і засобів контролю з метою захистити комп'ютерні системи та мережі, програми, пристрої і дані від кібернетичних атак, а також з метою зниження ризику здійснення кібератаки [9].

Система кібербезпеки складається із декількох елементів, координація яких всередині організації має вирішальне значення для успіху всієї програми кібербезпеки. Ці елементи включають наступне: безпеку додатків; безпеку даних; безпеку критично важливої інфраструктури; мережеву і операційну безпеку; хмарну безпеку; планування аварійного відновлення, а разом із ним і забезпечення безперервності бізнесу; фізичну охорону; навчання кінцевих користувачів.

Підтримка кібербезпеки в світлі появи все нових і нових загроз – важливе завдання для кожної організації. Щоб стійко протистояти новим викликам, необхідний більш активний і адаптивний підхід, ніж традиційні заходи, при яких захищеними є основні елементи системи, але ніяк не допоміжні.

Таким чином, обидві зазначені категорії мають своєю метою захист інформації та попередження загроз у комп'ютерних та мережевих системах. Далі порівняємо їх та надамо правовий аналіз вказаним поняттям.

Важливо відзначити те, що поведінка співробітників може мати великий вплив на інформаційну безпеку в організаціях. Саме тому нам особливо важливою вбачається культура ІБ, тобто такі моделі поведінки в компанії, які сприяють захисту інформації усіх видів. Так, на думку К. Реймерс і Д. Андерссона, співробітни-

ки організації зазвичай не вважають себе частиною зусиль своєї компанії щодо забезпечення інформаційної безпеки, а також досить часто вчиняють дії, які перешкоджають організаційним змінам [7, с. 1790].

У зв'язку із вищезазначеним варто вказати на результати дослідження, проведеного Verizon Wireless, найбільшим оператором стільникового зв'язку США. Згідно з його звітом із розслідування витоків даних за 2020 рік, 30% інцидентів порушення кібербезпеки пов'язані із внутрішніми суб'єктами всередині компанії. Відзначимо, що дослідження включало в себе вивчення 3950 порушень [1]. Таким чином, культура ІБ виходить на перший план.

Отже, розглянуті терміни не ідентичні. Кожен із них націлений на різний тип безпеки. Так, кібербезпека (далі – КБ) сприяє захисту використання кіберпростору від кібератак, тобто вона пов'язана із атаками ззовні компанії. Як вказує Ф. Фасуло, КБ – це структура захисту всього, що вразливе для злому, кібератаки та несанкціонованого доступу, тобто комп'ютерів, пристроїв, мереж, серверів та програм. При цьому розглянута категорія відноситься виключно до захисту даних, які існують у цифровій формі. І саме це, в першу чергу, відрізняє її від інформаційної безпеки [2].

У свою чергу ІБ відноситься саме до захисту конфіденційності, цілісності та доступності інформації, незалежно від її форми. Таким чином ІБ може стосуватися в рівній мірі і захисту картотеки особливих документів, і захисту бази даних компанії. Як підсумовує Ф. Фасуло, ІБ у широкому розумінні являє собою практику захисту даних організації, незалежно від їх форми.

Фахівці з кібербезпеки несуть відповідальність за запобігання порушень, з метою чого беруть участь у захисті серверів, баз даних, мереж, виявляють «діри» і вразливості. Фахівці з ІБ також стурбовані запобіганням втрати даних, але можуть вести більш широко направлену діяльність, ніж їх колеги з відділу КБ, наприклад, визначивши собі першочерговим пріоритетом складання плану відновлення системи після злому [4].

У розглянутих понять є і певні подібності, через що, ймовірно, і виникає плутанина у застосуванні термінів. А саме:

обидва типи безпеки припускають використання методів, спрямованих на забезпечення безпеки і захист комп'ютерних систем від витоку даних та інших зловмисних дій;

ІБ і КБ включають у себе аналогічні й взаємодоповнюючі процеси, обидві мають компонент, який займається фізичною безпекою інформації;

обидва типи оцінюють цінність інформації, яку прагнуть захистити, тобто зосереджуються на найважливішій інформації [6].

На нашу думку, розумним було б розглядати кібербезпеку в якості форми інформаційної безпеки, як її складового елементу на рівні з криптографією і подібними категоріями.

Відзначимо, що і інформаційна, і кібербезпека є предметом правового регулювання у законодавствах більшості країн. Далі вкажемо на найбільш значущі нормативно-правові акти у сфері регулювання відповідних відносин.

ЄС – Директива Європейського Союзу про захист даних (EUDPD). Відповідно до неї, країни-члени ЄС зобов'язуються розробити і прийнятий національні правила для стандартизації захисту конфіденційності даних для громадян на всій території Союзу.

США – Закон про права сім'ї на освіту і недоторканність приватного життя 1974 р (захищає конфіденційність записів про освіту учнів), Закон про переносимості та підзвітності медичного страхування (HIPAA) 1996 р. (зобов'язує приймати національні стандарти для електронних транзакцій у сфері охорони здоров'я і медичного страхування), Закон Гремма-Ліча-Блайлі (GLBA) 1999 р. (забезпечує конфіденційність і безпеку приватних фінансових даних, отриманих фінансовими установами), Стандарт безпеки даних індустрії платіжних карт (PCI DSS) (націлений на підвищення безпеки даних платіжних рахунків).

Канада – Закон про захист особистої інформації та електронної документації (захищає особисті дані при використанні електронних засобів для передачі або запису інформації або транзакцій).

Великобританія – Закон про захист даних 1998 р. (регулює обробку даних по фізичних особах у контексті отримання інформації, її зберігання та розкриття такої інформації) та Закон про неправомірне використання комп'ютерів 1990 р. (кваліфікує комп'ютерні злочини як кримінальні).

Греція – Закон 165/2011 в Управління з безпеки і конфіденційності зв'язку (вказує на мінімальні заходи контролю інформаційної безпеки, які повинні застосовуватися кожною організацією в сфері електронного зв'язку), Закон 205/2013 (захищає цілісність і доступності послуг місцевих телекомунікаційних компаній).

Розглянувши світовий досвід правового регулювання відносин з приводу інформаційної та кібернетичної безпеки, варто вказати й на українські нормативно-правові джерела у цій галузі:

Закон України «Про основні засади забезпечення кібербезпеки України» визначає особливості і напрямки забезпечення захисту прав та інтересів у кіберпросторі;

Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» дає визначення поняттю ІБ;

Закони України «Про національну безпеку України» і «Про концепцію національної програми інформатизації» містять положення про специфіку забезпечення національної інформаційної безпеки;

Закони України «Про інформацію» та «Про захист економічної конкуренції» дають визначення поняттю інформації;

Указ Президента України Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». Документ націлений на протидію інформаційній агресії РФ. Дано визначення терміну «наратив», що важливо для успішної діяльності суб'єктів забезпечення ІБ. В Акті також чітко простежуються спроби встановити і гармонізувати повноваження відповідних органів і силових структур при виконанні ними зобов'язань щодо захисту інтересів українців і країни в цілому в інформаційній сфері.

М.Т. Гаврильців надає власну класифікацію норм з приводу державного впливу в інформаційній сфері, яка заснована на їх призначенні:

1) норми, що закріплюють завдання і напрямки діяльності країни в інформаційному середовищі та визначають особливості її розвитку (норми Конституції України – статті 3, 10, 17, 31, 32, 34, ЗУ «Про інформацію» (ст. 6), ЗУ «Про Концепцію Національної програми інформатизації» (розділи 4-6);

2) норми про порядок взаємодії органів влади із суб'єктами інформаційних та інформаційно-інфраструктурних відносин, про процедури державного регулювання в даній сфері (ЗУ «Про телебачення і радіомовлення» (ст. 23-37), ЗУ «Про друковані засоби масової інформації ...», ЗУ «Про державну таємницю» (ст. 22), ЗУ «Про доступ до публічної інформації» та інші);

3) норми щодо адміністративно-правового статусу суб'єктів інформаційних відносин (ЗУ «Про телекомунікації» (ст. 39);

4) норми щодо системи органів державного регулювання в інформаційному середовищі та їх адміністративно-правового статусу (зазначені раніше положення Конституції, ЗУ «Про КМУ» (ст. 20) та інші [10, с. 202].

Висновки. Отже, нами були надані визначення інформаційної та кібербезпеки, а також зроблено порівняння та правовий аналіз обох категорій. Можна зробити висновок про те, що ці терміни мають різне значення, але вони однаково важливі як для окремих компаній, так і для держави в цілому. І хоча КБ можна розглядати як підмножину ІБ, обидва цих типи безпеки своєю основною метою мають захист даних. Інформаційна безпека орієнтована на захист від будь-яких загроз важливих даних, як у цифровій, так і в аналоговій формі. А кібербезпека, зосереджена на цифровій інформації, також нерозривно пов'язана із такими категоріями як кіберзлочини, кібератаки тощо.

Наше дослідження також дає можливість говорити про те, що культура інформаційної безпеки, так само як і кібербезпеки, вимагає безперервного поліпшення. Персонал організації повинен усвідомлювати масштаби і спільну місію щодо забезпеченню безпеки у своїй роботі.

Також з боку влади важливо приділяти достатню увагу розробці нових і поліпшенню наявних методів протидії порушенням у даній сфері, чому, безсумнівно, буде сприяти запозичення досвіду провідних країн світу і гар-

монізація чинного законодавства із нормативними актами ЄС.

Література

1. 2020 Data Breach Investigations Report. *Verizon*. 2020. URL: https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf.

2. Fasulo P. Cybersecurity vs Information Security: What's the difference? *Security Scorecard*. 2020. URL: https://securityscorecard.com/blog/ information-security-versus-cybersecurity.

3. Fruhlinger J. What is information security? Definition, principles, and jobs. *CSO United States*. 2020. URL: https://www.csoonline.com/article /3513899/what-is-information-security-definition-principles-and-jobs.html.

4. Information Security and Cyber Security: The Key Differences and Similarities. *Simplilearn*. 2021. URL: https://www.simplilearn.com/ information-security-vs-cyber-security-article.

5. Irwin L. What's the difference between information security and cyber security? *IT Governance*. 2020. URL: https://www.itgovernance.eu/blog/en/whats-the-difference-between-information-security-and-cyber-security.

6. It Security vs Cyber Security - What is the Difference? *Logsign*. 2020. URL: https://www.logsign.com/blog/it-security-vs-cyber-security-what-is-the-difference/.

7. Reimers K., Andersson D. Post-secondary education network security: the end user challenge and evolving threats. *ICERI2017 Proceedings*. 2017. Pp. 1787-1796. DOI: https://doi.org/ 10.21125/iceri.2017.0554

8. 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. С. 54-74. DOI: https://doi.org/ 10.15394/jdfsl.2017.1476

9. What is Cyber Security? Definition and Best Practices. *IT Governance*. 2020. URL: https://www.itgovernance.co.uk/what-is-cybersecurity.

10. Гаврильців М.Т. Інформаційна безпека держави в системі національної безпеки України. *Юридичний науковий електронний журнал*. 2020. № 2. С. 200-203.

References

1. 2020 Data Breach Investigations Report. *Verizon*. 2020. URL: https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf.

2. Fasulo P. Cybersecurity vs Information Security: What's the difference? *Security Scorecard*. 2020. URL: https://securityscorecard.com/ blog/ information-security-versus-cybersecurity.

3. Fruhlinger J. What is information security? Definition, principles, and jobs. *CSO United States*. 2020. URL: https://www.csoonline.com/ article/ 3513899/what-is-information-security-definition-principles-and-jobs.html.

4. Information Security and Cyber Security: The Key Differences and Similarities. *Simplilearn*. 2021. URL: https://www.simplilearn.com/ information-security-vs-cyber-security-article.

5. Irwin L. What's the difference between information security and cyber security? *IT Governance*. 2020. URL: https://www.itgovernance.eu/blog/en/whats-the-difference-between-information-security-and-cyber-security.

6. It Security vs Cyber Security - What is the Difference? *Logsign*. 2020. URL: https://www. logsign.com/blog/it-security-vs-cyber-security-what-is-the-difference/.

7. Reimers K., Andersson D. Post-secondary education network security: the end user challenge and evolving threats. *ICERI2017 Proceedings*. 2017. Pp. 1787-1796.

8. 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. С. 54-74.

9. What is Cyber Security? Definition and Best Practices. *IT Governance*. 2020. URL: https://www.itgovernance.co.uk/what-is-cybersecurity.

10. Gavryl'civ M.T. Informacijna bezpeka derzhavy v systemi nacional'noi' bezpeky Ukrai'ny. *Jurydychnyj naukovyj elektronnyj zhurnal*. 2020. № 2. S. 200-203.

I. Sopilko

INFORMATION SECURITY AND CYBER SECURITY: A COMPARATIVE LEGAL ASPECT

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

The role of information security and cybersecurity in the modern world is very significant. Today we rely more on technology than ever before. As a result, the volume of digital data creation has increased. Today, companies and governments store most of the important information on computers and transfer it over the Internet to other computers. The devices and systems that underlie them have vulnerabilities that, when exploited, threaten the activities of organizations and even entire governments.

It is worth noting that data breaches caused by holes in cybersecurity and incomplete information security systems can have devastating consequences for any business. After all, this can ruin the company's reputation due to the loss of confidence of consumers and partners. Also, the loss of critical data can cost an organization its competitive advantage. In the future, this problem can affect corporate income due to non-compliance with the rules for protecting confidential information. That is why understanding the essence of information and cybersecurity, as well as their sufficient legal regulation, is now a key aspect in the implementation of the activities of any organization.

***The purpose of the paper** is to study the features and essence of cybersecurity and information security and to make their comparative legal analysis. **Research methods:** the research was carried out using generally recognized methods of scientific knowledge, such as analytical, comparative-legal, systemic, and structural, and others. **Results:** the concept, essence, characteristics of cybersecurity and information security are studied, the problems of ensuring their functioning are indicated, recommendations are given to overcome such problems by improving the current legislative framework and harmonizing national legislation with international standards. **Discussion:** the discussion in the article is conducted on the delimitation of the concept of cybersecurity from the concept of information security and the peculiarities of their legal regulation in the leading countries of the world in comparison with our state.*

***Keywords:** cybersecurity; information security; cyberspace; cybercrime; cyberattack.*