DOI: 10.18372/2307-9061.61.16356
УДК 342.95:004.056.5(045)

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

ОСОБЛИВОСТІ ПРОТИДІЇ КІБЕРЗАГРОЗАМ ПРАВОВИМИ МЕТОДАМИ ТА ЗАСОБАМИ

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

Мета: *дослідити особливості та сутність кіберзагроз та надати рекомендації з приводу правового забезпечення кібербезпеки на підприємствах та в державі загалом.* ***Методи дослідження:*** *дослідження було проведено із застосуванням загальновизнаних методів наукового пізнання, таких як: аналітичний, формальний, порівняльно-правовий, системно-структурний та інші.* ***Результати:*** *досліджено поняття, суть, характеристики кіберзагроз та відповідних їм категорій, вказано на проблеми забезпечення протидії ним, надано пропозиції щодо подолання таких проблем шляхом вдосконалення чинного законодавства та його гармонізації зі стандартами, прийнятими в країнах Євросоюзу.* ***Обговорення:*** *дискусія у науковому дослідженні ведеться щодо особливостей правового врегулювання загроз та ризиків, які виникають під час взаємодії суб'єктів у кіберпросторі.*

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

Постановка проблеми та її актуальність. Українське суспільство за останні декади пройшло період повної трансформації і стало тим, що сьогодні прийнято називати інформаційним суспільством. Дійсно, ми виробляємо, використовуємо, накопичуємо інформацію, переробляємо її з метою наступної трансформації отриманих даних у якісно новий продукт – знання. Сьогодні роль інформації та інформаційних технологій у житті соціуму не просто велика, вона величезна, адже ми не тільки поглинаємо дані, але й створюємо з них відповідні інформаційні продукти і послуги, тим самим забезпечуючи розвиток економіки країни.

Глобальний інформаційний простір як середовище віртуального «проживання» великої кількості людей по всьому світу дало нам багато, одночасно ставши об'єктом постійних ризиків і різноманітних кібернетичних загроз. Зазначене здатне істотно дестабілізувати роботу не тільки окремих індивідів, а й цілих соціальних груп, а також всієї держави в цілому, якщо буде порушена цілісність такої категорії як інформаційна безпека. Остання, у свою чергу, є важливим елементом безпеки національної. Саме тому протидія можливим і реальним кіберзагрозам, а також приборкання потенційних ризиків у вказаній сфері сьогодні стало першочерговим завданням як для окремих організацій, так і для держави загалом. І забезпечити таке можливо, в першу чергу, правовими методами та інструментами, про що й піде мова далі.

Аналіз досліджень і публікацій з проблеми. Цій проблемі були присвячені роботи таких дослідників і вчених як Л. Бєлкін, П. Біленчук, Ю. Кунєв, С. Лихова, В. Мороз, Ю. Юринець, В. Філінович та інших.

Мета статті. Автор даного наукового дослідження хоче розкрити суть і особливості поняття «кіберзагроза» та інших, пов'язаних із ним термінів, зробити їх порівняльно-правовий аналіз та надати критичну оцінку і рекомендації щодо подолання пов'язаних із цим прогалин у правовому регулюванні.

Виклад основного матеріалу. Сьогодні ми маємо можливість спостерігати активний розви-

ток «електронних» сфер взаємодії, а саме: економіки, уряду, соціальних, господарюючих мереж тощо. Все це вимагає забезпечення достатнього рівня кібербезпеки, адже ми щодня взаємодіємо саме в кіберпросторі, який став об'єктом загроз й атак. А тому правове співтовариство також намагається внести свою лепту у врегулювання зазначеної проблеми, чому і присвячена дана стаття.

Але, перш ніж перейти до розгляду правових методів забезпечення захисту інформаційної сфери, необхідно ознайомитися із основними використовуваними поняттями і категоріями. Першим вивченню підлягає концепт згаданого раніше кіберпростору. Фахівці NIST (Національний інститут стандартів і технологій Міністерства торгівлі США) пропонують такі його визначення:

- це глобальна область в інформаційному середовищі, сформована із взаємозалежної мережі інфраструктур інформаційних систем, а саме телекомунікаційних мереж, комп'ютерних систем і подібного (про що свідчать стандарти NIST SP 800-30 Rev.1, NIST SP 800-39, NIST SP 800-53);

- це взаємозалежна мережа інфраструктур інформаційних технологій ... у найважливіших галузях промисловості (CNSSI 4009-2015, NIST SP 800-160);

- це складне середовище, яке виникло завдяки людській взаємодії із програмами в мережі Інтернет за допомогою підключених до неї високотехнологічних пристроїв. При цьому таке середовище не має фізичної форми (NISTIR 8074 Vol. 2.) [1].

Якщо звернутися до законодавства України, то Закон № 2163-VIII «Про основні засади забезпечення кібербезпеки України» в статті 1 дає визначення кіберпростору як віртуального простору, завдяки якому можливо встановлювати комунікацію і реалізовувати суспільні відносини. Таке середовище було утворене як результат функціонування спільних комунікаційних систем і всесвітньої мережі Інтернет або інших глобальних мереж передачі інформації [2].

Далі розглянемо суть інформаційної та кібернетичної безпеки як одних із основних цілей загроз і ризиків у кіберпросторі. Якщо звернемося до статті 17 Конституції України, то дізнаємося, що «захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу. Захист України, захист її суверенітету, територіальної цілісності і недоторканності покладені на Збройні Сили України» [3]. Зазначене дає нам можливість зробити висновок про те, що досягнення інформаційної безпеки країни поставлено в один ряд із її захистом як такої.

Згідно Дж. Фрулінгеру, інформаційна безпека (також infosec, від англ. Information security) – це сукупність різних методів, за допомогою яких здійснюється захист даних від несанкціонованого доступу або змін під час їх зберігання або передачі з одного пристрою на інший. І все ж таке визначення не охоплює розглянутий концепт повною мірою. Тому автор пропонує використовувати більш широке визначення, надане Інститутом SANS: infosec – це процеси і методи, розроблені й реалізовані з метою захистити друковану, електронну, а також інформацію, представлену в іншій формі від несанкціонованого доступу, використання тощо [4].

На наш погляд, найбільш повне визначення містить підхід В. Мороза, згідно з яким інформаційна безпека, з одного боку, являє собою стан, коли, з урахуванням реальних і потенційних загроз, інформаційна сфера зберігає свій сталий розвиток, а з іншого боку – це безперервний процес діяльності компетентних осіб із метою запобігти або протидіяти загрозам в інформаційній сфері, пов'язаний із використанням активних заходів інформаційного впливу [5, с. 97].

Нерідко інформаційну безпеку плутають із кібернетичною. І все ж остання зазвичай розуміється як практика захисту мереж і систем, даних, а також обладнання від цифрових (кібернетичних) атак. Раніше згаданий Закон № 2163-VIII у ст. 1 визначає кібербезпеку як захищеність життєво важливих інтересів людини і громадянина, суспільства і держави при використанні кіберпростору, при якій забезпечуються сталий розвиток інформаційного суспільства та

цифрового комунікаційного середовища, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національній безпеці України в кіберпросторі [2].

Розуміючи суть основних термінів, можемо переходити до визначення кіберзагрози. Під нею прийнято розуміти будь-яку зловмисну атаку з метою отримання незаконного доступу до даних, порушення цифрових операцій чи інші дії з інформацією, що мають негативні наслідки. Український закон про кібербезпеку під кібернетичною загрозою розуміє існуючі або потенційно вірогідні явища і чинники, небезпечні для життєво важливих національних інтересів країни у кіберпросторі. Такі явища будуть мати негативний вплив на стан кібербезпеки України [2].

Варто розуміти, що кіберзагрози можуть походити від різних суб'єктів, наприклад, терористичних угруповань, вороже налаштованих держав, так само як і від поодиноких зловмисників, на кшталт хакерів і навіть невдоволених співробітників. Особливо часто ціллю кібератаки стають персональні дані у розпорядженні іменитих компаній. Конфіденційна інформація їх клієнтів може бути використана зловмисниками для отримання фінансової вигоди. Нерідко жертвами подібних зловмисних дій стають звичайні люди як учасники світу Інтернету речей (Internet of Things). В. Філінович під таким розуміє певну технологічну концепцію підключення пристроїв («гаджетів») по всій земній кулі за допомогою Інтернету, метою чого є управління цими пристроями віддалено. Як запевняє дослідниця, світ Інтернету речей вельми небезпечний, адже якщо хакер отримає несанкціонований доступ хоча б до одного з ваших технологічних пристосувань, то зможе впровадити у нього віруси, а після – отримати через нього доступ до інших пристроїв, підключених до мережі [6, с. 123].

Таким чином, однією з основних функцій кожної держави (і особливо «держави у смартфоні») залишається забезпечення безпеки її громадян. Відповідно Україна в особі своїх органів повинна захищати дані її людей, реєстри і ресурси у кібернетичному просторі на тому ж рівні, на якому захищає фізичне майно. І хоча держава активно впроваджує нові політики і методики підтримки кібербезпеки на належному рівні, але проблема до кінця ще не вирішена, адже кількість загроз зростає з кожним днем.

Сьогодні суб'єкти стикаються з наступними перешкодами:

- відсутня єдина якісно пропрацьована програма кібербезпеки. І хоча вже введено в дію Закон «Про основи забезпечення кібербезпеки» і Доктрина інформаційної безпеки, але цього недостатньо як з точки зору всеосяжного законодавчого регулювання, так і з позиції реалізації відповідної програми;

- не впроваджено транспарентну політику інтеграції реєстрів і технічної архітектури прийняття рішень на рівні держави;

- не розроблено набір сучасних вимог щодо захисту баз даних із метою контролю їх виконання та накладення покарання за порушення;

- має місце нестача професійно підготовлених кадрів, експертів у галузі кібербезпеки.

І це далеко не весь перелік наявних проблем. Проте ми можемо запропонувати рекомендації, які, за належної реалізації, допоможуть протистояти кіберзагрозам.

Так, з метою захисту персональних даних, крім уже діючого Закону № 2297-VI, варто інкорпорувати в національне законодавство норми європейського Загального регламенту захисту персональних даних (англ. The General Data Protection Regulation) від 25.05.2018 р. Їх дія повинна поширюватися на всіх суб'єктів, які з комерційною метою збирають і обробляють дані.

Що стосується вразливостей в Інтернеті речей, то варто підтримати позицію про необхідність забезпечення дотримання і поваги прав людини в Інтернеті, особливо у частині недопущення будь-яких проявів дискримінації користувачів; впроваджувати і використовувати інструменти для забезпечення конфіденційності комунікації і надати користувачам можливість контролювати використання сторонніми суб'єктами їх персональних даних [6, с. 125].

Не менш важливим ми вважаємо забезпечення правової визначеності, прозорості та просто-

ти у розумінні нормативно-правових документів кожним українцем.

Як вказує Ю. Кунєв, проблема забезпечення інформаційної та кібернетичної безпеки істотно загострюється під час зовнішніх загроз, особливо, інформаційних війн. При цьому використовуються звичайні (стандартні) засоби і способи інформаційної діяльності. Вчений наполягає на необхідності віднесення і регулювання зазначеної проблеми до відання інформаційно-адміністративного права. Під ним Ю. Кунєв розуміє сукупність правових норм і юридичних принципів для врегулювання інформаційно-адміністративної діяльності, пов'язаної із юридичним регулюванням інформаційної діяльності приватних суб'єктів і органів публічної адміністрації щодо реалізації основних державних функцій; а також формування і використання публічних інформаційних ресурсів. Таким чином для правового забезпечення інформаційної безпеки необхідна трансформація змісту інформполітики в якості інформаційного законодавства [7, с. 101].

Також, як вважає О. Макеєва, важливу роль у даному питанні відіграє правове виховання українців. Адже саме правова культура є загальним критерієм для визначення якісного стану сучасного інформаційного суспільства. При гідному правовому вихованні людина не буде прагнути зловживати правом, порушуючи чужі інтереси, в тому числі, в інформаційній сфері. Це особливо важливо в умовах пандемії COVID-19, коли права людини порушуються досить часто, наприклад, внаслідок дискримінації. Правова культура ж зможе допомогти забезпечити транспарентність і повагу до людської гідності, що, в свою чергу, стане каталізатором ефективного реагування в умовах кризової ситуації дезорганізації [8, с. 58].

Зрозуміло, що цей список ще можна продовжити, але і вказаного на перший час повинно вистачити для значного посилення готовності нашої держави активно і цілковито захищати своє інформаційне суспільство, так само як і свідомість кожного окремого індивіда від інформаційної агресії, а персональні дані, іншу важливу інформацію, реєстри і системи – від витоків і зломів. Так масштабна діджиталізація перестане бути джерелом постійних ризиків і загроз.

Висновки. Отже, в 2019-2021 роках кібербезпека стала як ніколи важливою. Адже загрози в сфері діджиталізації не тільки не зменшуються, але й виходять на новий, більш високотехнологічний рівень. Постраждати від дій кіберзлочинців сьогодні може кожен – починаючи від індивіда і закінчуючи державними структурами. Існує вкрай багато кіберзагроз, щоб можна було ігнорувати ризики, а тому запобігання їм є ключовою метою, в першу чергу, уряду і нормотворців.

Єдиного готового рішення по протидії кіберзагрозам не існує, як не існує і підходу в правовому регулюванні, який би однаково застосовувався для всіх суб'єктів інформаційних правовідносин. У першу чергу необхідно опрацювати чинне законодавство і доповнити його новими нормативно-правовими актами спеціального призначення, а також гармонізувати його з європейським законодавством. Не менш важливим автор вважає розвиток культури безпеки, і в першу чергу саме правової. Необхідно вести просвітницьку діяльність, щоб кожен громадянин знав, чим загрожує порушення прав учасників кіберпростору і як уберегти себе від кіберзагроз. На підприємствах і в організаціях потрібно розробляти і впроваджувати особливі політики і процедури щодо поводження із інформаційними активами, тобто певні встановлені правила роботи в інформаційній системі компанії.

Це лише невеликий перелік рекомендацій щодо протидії і усунення кіберзагроз, на які далеко не завжди звертають увагу як власники бізнесу, так і керівники державних організацій. При цьому загрози здатні завдати непоправної шкоди всій кіберсистемі не тільки окремо взятого підприємства, але й цілих структур (згадаємо, наприклад, випадок 2017, коли вірус Petya (NotPetya) паралізував роботу об'єктів критичної інфраструктури держави. При цьому сховатися за технологіями не вдасться, важливо працювати з людьми, впроваджувати основи кібергігієни і не забувати про правовий інструментарій і засоби примусу.

Література

1. Cyberspace. *NIST Information Technology Laboratory.* 2019. URL: https://csrc. nist.gov/ glossary/term/cyberspace.

2. Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовт. 2017 р. № 2163-VIII. *Відомості Верховної Ради України.* 2017. № 45. Ст. 403.

3. Конституція України: Закон України від 28 чер. 1996 р. № 254к/96-ВР. *Відомості Верховної Ради України.* 1996. № 30. Ст. 141.

4. 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.

5. Мороз В. Особливості забезпечення інформаційної безпеки в умовах воєнного стану. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право».* 2021. № 2(59). С. 94-101. DOI: https://doi.org/10.18372/2307-9061.59.15600

6. Філінович В.В. Кібербезпека та Інтернет речей: правовий аспект. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право».* 2020. № 4(57). С. 122–127. DOI: https://doi.org/ 10.18372/2307-9061.57.15074

7. Кунєв Ю.Д. Правове забезпечення інформаційної безпеки як предмет правового дослідження. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право».* 2021. № 1(58). С. 95-102. DOI: https://doi.org/ 10.18372/2307-9061.58.15314

8. Макеєва О.М. Функції правової культури у сучасному інформаційному просторі. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право».* 2021. № 1(58). С. 54-60. DOI: 10.18372/2307-9061.58.15309.

References

1. Cyberspace. *NIST Information Technology Laboratory.* 2019. URL: https://csrc. nist.gov/ glossary/term/cyberspace.

2. Pro osnovni zasady zabezpechennja kiberbezpeky Ukrai'ny: Zakon Ukrai'ny vid 05 zhovt. 2017 r. № 2163-VIII. *Vidomosti Verhovnoi' Rady Ukrai'ny.* 2017. № 45. St. 403.

3. Konstytucija Ukrai'ny: Zakon Ukrai'ny vid 28 cher. 1996 r. № 254k/96-VR. *Vidomosti Verhovnoi' Rady Ukrai'ny.* 1996. № 30. St. 141.

4. 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.

5. Moroz V. Osoblyvosti zabezpechennja informacijnoi' bezpeky v umovah vojennogo stanu. *Naukovi praci Nacional'nogo aviacijnogo universytetu. Serija: Jurydychnyj visnyk «Povitrjane i kosmichne pravo».* 2021. № 2(59). S. 94-101. DOI: https://doi.org/10.18372/2307-9061.59.15600

6. Filinovych V.V. Kiberbezpeka ta Internet rechej: pravovyj aspekt. *Naukovi praci Nacional'nogo aviacijnogo universytetu. Serija: Jurydychnyj visnyk «Povitrjane i kosmichne pravo».* 2020. № 4(57). S. 122–127. DOI: https://doi.org/10. 18372/ 2307-9061.57.15074

7. Kunjev Ju.D. Pravove zabezpechennja informacijnoi' bezpeky jak predmet pravovogo doslidzhennja. *Naukovi praci Nacional'nogo aviacijnogo universytetu. Serija: Jurydychnyj visnyk «Povitrjane i kosmichne pravo».* 2021. № 1(58). S. 95-102. DOI: https://doi.org/10.18372/2307-9061.58.15314

8. Makejeva O.M. Funkcii' pravovoi' kul'tury u suchasnomu informacijnomu prostori. *Naukovi praci Nacional'nogo aviacijnogo universytetu. Serija: Jurydychnyj visnyk «Povitrjane i kosmichne pravo».* 2021. № 1(58). S. 54-60. DOI: 10.18372/ 2307-9061.58.15309.

Iryna Sopilko

PECULIARITIES OF COUNTERING CYBER THREATS BY LEGAL METHODS AND MEANS

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

Over the past decades, Ukrainian society has gone through a period of complete transformation and has become what is now commonly called the information society. Indeed, we produce, use, accumulate information, process it intending to further convert the obtained data into a qualitatively new product – knowledge. Today, the role of information technologies and information itself in the life of society is not just great, it is tremendous because we not only consume data but also produce appropriate information products and services from them, thereby ensuring the development of the country's economy.

The global information space as an environment for the virtual «residence» of a large number of people around the world has given us a lot, while simultaneously becoming an object of constant risks and various cyber threats. This can significantly destabilize the work of not only individuals but also social groups, as well as the entire state as a whole if the integrity of such a category as information security is violated. The latter, in turn, is an important element of national security. That is why counteraction against possible and real cyber threats, as well as curbing potential risks in this area, has today become a priority task both for individual organizations and for the state as a whole. And it is possible to ensure this, first of all, by legal methods and instruments, which are discussed in this study.

Purpose: *to study the features and essence of cyber threats and provide recommendations on the legal support of cyber security at the enterprise and in the state as a whole.* ***Research methods:*** *the research was carried out using generally recognized methods of scientific knowledge, such as analytical, formal, comparative-legal, systemic and structural, and others.* ***The results:*** *the concept, essence, characteristics of cyber threats and their corresponding categories were outlined, the problems of ensuring counteraction to them were pointed out, suggestions to overcome such problems by improving the current legislation and its harmonization with the standards adopted in the EU countries were provided.* ***Discussion:*** *the discussion in the scientific study is about the peculiarities of the legal regulation of threats and risks arising from the interaction of subjects in cyberspace.*

Key words: *cyberthreat; information security; cyberspace; cybersecurity; cyberattack.*

Стаття надійшла до редакції 25.11.2021