УДК 34
DOI https://doi.org/10.32782/2524-0374/2021-6/32

АКТУАЛЬНІ ПИТАННЯ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

CURRENT ISSUES OF LEGAL SECURITY OF CYBER SECURITY OF UKRAINE

Горовий С.С., студент кафедри публічного права факультету соціології та права
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»

Пряміцин В.Ю., старший викладач кафедри публічного права
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»

У статті детально розглядається тлумачення поняття «кібербезпека», «кіберпростір» і суміжних із ними понять, спираючись на чинне законодавство України, адже науковці світу дотепер не дійшли спільної думки щодо визначення цих важливих понять. Також розглядаються позитивні й негативні фактори доступності до інформації будь-кому через глобальну інтернет-мережу. Доведено необхідність розгляду питання, особливо в сучасному світі, мало того, проаналізовано актуальну ситуацію системи кібербезпеки України, зокрема в період прихованої війни від сусіда-агресора. Для кращого розуміння можливих труднощів у галузі інформаційної безпеки визначено ролі кожної ланки в цій системі, хоча в чинному законодавстві такий аспект досить розмитий і не містить чіткої інформації. Автори аналізують публікації сучасних науковців із проблеми, а також чинне законодавство України. Автори порівнюють та аналізують відповідність чинного законодавства України з питань кібербезпеки з міжнародними правовими актами. Викладено актуальні проблеми й прогалини в українському законодавстві. У результаті проведеного дослідження головною проблемою виділено відсутність конкретики в законодавстві України та його неузгодженість із міжнародно-правовими актами, що не лише гальмує розвиток, але і є причиною гострих проблем, хоча незначні кроки на шляху покращення ситуації були втілені. Визначено, що наявний рівень кібербезпеки є недостатнім і потребує значних внесків і поправок, а чинна система може виступати лише фундаментом для відбудови повноцінної структури кібербезпеки Україні. Її зовсім не можна назвати абсолютною та повноцінною, це більше план і схема, ніж чіткий функціонал. Авторами запропоновані методи ліквідації недоліків і прогалин із питань кібербезпеки, або хоча б мінімізації їх негативного впливу на державу.

Ключові слова: кіберпростір, кібербезпека, інформаційна безпека.

The article examines in detail the interpretation of the concept of “cyberspace”, “cyberspace” and related concepts, based on current legislation of Ukraine, because scientists around the world have not yet come to a consensus on the definition of these important concepts. Also considers the positive and negative factors access to information for anyone through the global Internet. The necessity of considering this issue, especially in the modern world, is proved, moreover, the current situation of the cybersecurity system of Ukraine is analyzed, especially during the hidden war from the aggressor neighbor. To better understand the possible difficulties in the field of information security, the role of each link in this system is defined, although in the current legislation this aspect is rather vague and does not contain clear information. The author analyzes the publications of modern scientists on this issue, as well as current legislation of Ukraine. The author compares and analyzes the compliance of the current legislation of Ukraine on cyber security with international legal acts. Current problems and gaps in Ukrainian legislation are highlighted. As a result of the study, the main problem was the lack of specifics in the legislation of Ukraine and its inconsistency with international legal acts, which not only slows down development, but is the cause of acute problems, although minor steps to improve the situation have been implemented. It is determined that the current level of cybersecurity is insufficient and requires significant contributions and amendments, and the existing system can only serve as a foundation for rebuilding a full structure of cybersecurity in Ukraine and it can not be called absolute and complete, it is more a plan than a clear functionality. The author proposes methods to eliminate shortcomings and gaps in cybersecurity or at least minimize their negative impact on the state.

Key words: cyberspace, cybersecurity, information security.

Постановка проблеми. Світова мережа Інтернет вже давно стала повсякденністю, надаючи доступ до широкого обсягу інформації, але водночас і легким і доступним способом управління та контролю за людьми зі сторони держави. І навпаки, населення багатьох країн тепер має можливість контролювати діяльність влади через звіти на онлайн-платформах. Крім того, сучасний громадянин має можливість отримувати інформацію майже безконтрольно зі сторони держави, що докорінно відрізняється від тих часів, коли все проходило через цензуру.

Кіберпростір – це нова система управління суспільством, засіб міжнародного співробітництва, й мало того, – нова форма державного суверенітету.

Актуальність дослідження зумовлена новими загрозами для України зі сторони кіберзлочинності, в той час, як країна має недостатній рівень захисту у формі законодавчого забезпечення, особливо в період гібридної війни.

Аналіз останніх досліджень. Аналізоване питання було викладено такими дослідниками, як В. Панін, О. Довгань, В. Бутузов, А. Танасюк, М. Бунчук, О. Баранов, А. Марущак і багато інших.

Метою статті є тлумачення терміну «кібербезпека», його принципів і складових частин, аналіз сучасного стану правового забезпечення кібербезпеки в Україні й визначення прогалин і недоліків із пошуком методів їх усунення чи мінімізації негативних наслідків.

Виклад основного матеріалу. Роль кібербезпеки зростає з кожним днем, проте необхідно досить чітко розуміти тлумачення терміну. Науковці України дотепер сперечаються у визначення поняття «кібербезпека» й суміжних йому, тому доцільно використовувати визначення, подане в Законі України (далі – ЗУ) «Про основні засади забезпечення кібербезпеки України». Інформаційна безпека – це стан захищеності життєво важливих інтересів людини, суспільства й держави, за якого запобігається заподіяння шкоди через: неповноту, невчасність і невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання та порушення цілісності, конфіденційності й доступності інформації [2].

З кожним днем роль кібербезпеки стає все більшою, що змушує чимало держав створювати власні законодавчі норми, адаптовані до сучасних умов, які змінюються дуже швидко, тому створюються стратегії, спрямовані на довгостроковий період. Тому нині 27 країн-членів НАТО, Європейський Союз, 12 країн Європи, які не є членами НАТО, а також інші 38 країн з інших частин світу мають і вдосконалюють власні стратегії кібербезпеки [5].

Проте стратегією все не обмежується, постійно проводяться розробка й ухвалення актуального посилення безпеки інформаційних систем.

Натепер Стратегія кібербезпеки України (рішення Ради національної безпеки й оборони України від 27 січня 2016 року) та ЗУ від 05 жовтня 2017 року «Про основні засади забезпечення кібербезпеки України» визначають організаційну й правову основу протидію кіберзлочинності, яка полягає у визначенні суб'єктів, сфер їх діяльності й напрямів взаємодії [4].

Аналізуючи закордонний досвід із питань кібербезпеки, М. Гребенюк виділяє 3 моделі правового регулювання. На прикладі Китайської Народної Республіки (далі – КНР) ми бачимо тотальний, жорсткий контроль держави над мережею Інтернет. Другу модель ілюструє Франція – передбачення відповідальності провайдера за всі дії користувача, крім того, існує спеціальна комісія, яка контролює, щоб інформація в мережі не порушувала права й свободи людей. Третя – звільняє провайдерів від відповідальності, якщо він виконує всі вимоги, що стосуються надання послуг (наприклад, досвід Японії) [3].

Для забезпечення кібербезпеки в США були створені:

- Electronic Crimes Task Forces ECTF – Секретна служба США для розслідування та запобігання фальшивомонетництва, а нині й для боротьби з економічними й комп'ютерними злочинами;
- Федеральне агентство США є взаємодійною ланкою між службами, правоохоронними органами й приватними сектором для виявлення та запобігання кіберзлочинів;
- US Cyber Command – військовий підрозділ у сфері кібербезпеки;
- United States Computer Emergency Readiness Team – національний відділ кібербезпеки від Департаменту внутрішньої безпеки;
- Computer Crime and Intellectual Property Section – відділ комп'ютерної злочинності й інтелектуальної власності;
- Internet police – інтернет-поліція, мережева поліція [7].

Цікавим є досвід республіки Східної Африки, а саме Уганди. Там було прийнято закон про податок за користування соціальними мережами. Кошти, які сплачуються, використовуються для посилення кібербезпеки й захисту інформаційного простору, а також для покращення електропостачання, щоб громадяни могли без перерв користуватися соціальними мережами [3].

Естонія – одна з перших країн у світі, яка ухвалила стратегію забезпечення інформаційної безпеки. Був розроблений Міністерством оборони не лише сам Документ, а й план впровадження. Створено міжвідомчу координаційну робочу групу, яка займається моніторингом і координацією виконання цілей, що узгоджуються зі стратегією, а також створюють звіт для Ради кібербезпеки. Основним сегментом відповідальності є RIA, яка здійснює нагляд за безперервним застосуванням заходів безпеки, а також захистом критичної інформаційної структури, а особливо за аналізом сучасного стану потенціальних ризиків і підготовкою заходів безпеки. Якщо відбувається порушення вимог безпеки, RIA може чинити провадження поза суду, наприклад, використовуючи систему штрафів [6].

CERT-EE – підрозділ RIA – займається реагуванням на комп'ютерні надзвичайні ситуації, забезпечує запобігання кіберінцидентам, першим дізнається про загрози й інформує про них, а також організовує профілактичні заходи.

Система національної безпеки Іспанії складається з:

- Прем'єр-міністра;
- Ради національної безпеки;
- Департаменту національної безпеки;
- Органів підтримки національної безпеки.

Національний криптологічний центр (CCN) забезпечує безпеку інформаційно-комунікаційних технологій у різних органах державного управління та системах, які відповідають за секретну інформацію [6].

CCN-CERT – команда, яка реагує на випадки в напрямі кібербезпеки, особливо актуальна їхня діяльність у випадку кібератак.

Національний центр захисту інфраструктури й кібербезпеки (CNPIC) відповідає за захист критичної інфраструктури, а також за секретаріат із питань безпеки. Основна мета – координація механізмів, які необхідні для забезпечення безпеки.

Іспанський національний інститут кібербезпеки (INCIBE) займається просуванням і розвитком інноваційних процесів у галузі кібербезпеки.

Іспанський кластер інновацій у кібербезпеці (AEI Ciberseguridad у Tecnologías Avanzadas) сприяє відкриттю бізнесів і впровадженню технологічних послуг у сфері кібербезпеки, співпраці й стимулюванню нових стратегій для конкурентоспроможності, заохоченню обміну досвідом та ідеями в процесі впровадження інновацій у сфері кібербезпеки [6].

Кожна країна обирає свою стратегію в області кібербезпеки. Доречно розглянути також систему Казахстану. Ця країна має чітко сформовану концепцію, яка визначає напрями реалізації політики в галузі забезпечення безпечного користування інтернет-ресурсам [3]. Під час формування правової структури був урахований міжнародний досвід, що є чудовим прикладом і для України, адже нема потреби вигадувати щось нове, досить проаналізувати інші країни, оцінити ті чи інші способи забезпечення кібербезпеки, «приміряти» їх до правової системи України й за можливості запровадити.

Не заважаючи на чималі кроки на шляху до забезпечення інформаційної безпеки, присутня багата кількість недоліків, основним із них є неузгодженість національного законодавства з міжнародними стандартами. Законодавство України не передбачає визначення «користувач послуг», «дані про рух інформації», «електронні докази».

Експерти визначають проблемні моменти правового забезпечення інформаційної безпеки України [1]:

– нелогічність використання термінології, адже Закон України «Про основні засади забезпечення кібербезпеки України» вносить цілий ряд дефініцій, які не відповідають тим, що були узаконені раніше;

– відсутність системного національного захисту критичної інфраструктури як наслідок того, що немає законодавчого акту, де ця структура була б описана, хоча й існують певні регуляторні правила захисту, проте вони не є вичерпними й послідовними;

– невідповідність міжнародним стандартам Європейського Союзу й НАТО щодо інформаційної безпеки об'єктів критичної інфраструктури;

– повторення підпорядкованості (основними органами, які відповідають за контроль кібербезпеки України, є Служба безпеки України, Міністерство оборони України, Національна поліція України, Державна служба спецзв'язку й захисту інформації, Національний банк України й розвідувальні органи).

Присутня юридична невизначеність повноважень, завдань і функціональних обов'язків агенцій держави, які мають здійснювати захист критичної інфраструктури. Як приклад, Закон України «Про основні засади забезпечення кібербезпеки України» регламентує повноваження Служби безпеки України стосовно кіберінцидентів, проте такий момент не відбитий у решті нормативно-правових актів;

– не зарегламентовані вимоги про належне інформування та безпеку для операторів і провайдерів об'єктів критичної інфраструктури. За директивою NIS [1] усі країни мають визначити й регламентувати вимоги щодо безпеки й інформування для операторів суттєвих послуг і для провайдерів цифрових послуг. Що стосується України, ЗУ «Про основні засади забезпечення кібербезпеки України» робить перші кроки на шляху регламентації, проте, оскільки законопроєкт про критичну інфраструктуру зна-

ходиться на стадії розгляду, ця норма не є повноцінною та залишається декларативною. Постанова Кабінету Міністрів України № 518 від 19 червня 2019 р. [9] визначає обов'язки власника й / або керівник об'єкта критичної інфраструктури, проте сама процедура й терміні надання інформації не встановлені. Окрім того, не визначено місце провайдерів у системі об'єктів критичної інфраструктури й чи взагалі належать вони до цієї категорії; існує прогалина в стратегічному плануванні на довгостроковий період, а точніше, його повна відсутність, не говорячи про проміжні результати й наслідки в разі невиконання плану; обмежений бюджет країни, в результаті чого відсутні спеціалісти з кібербезпеки, тому що заробітна плата не конкурентоспроможна [8].

Нещодавно президент України Володимир Зеленський опублікував на своїй сторінці мережі Instagram новину про створення інституту, де будуть готувати фахівців із кібербезпеки, що є чималим кроком на шляху розвитку галузі, головне, щоб задум був реалізований, а не лишився лише проєктом на папері.

Аналізуючи вищевказані недоліки, можна дійти єдиного шляху подолання прогалин – це вдосконалення правової системи через визначення термінів «стан захищеності», «цифрове комунікаційне середовище» й «критерії забезпечення кібербезпеки».

Висновки. Отже, в Україні стратегія кібербезпеки обмежується лише ЗУ «Про основні засади забезпечення кібербезпеки України», який є більшою мірою основою для розробки нормативних актів у майбутньому, але не всеосяжним законом про кібербезпеку, який би врегулював повністю питання кібербезпеки й відповідав би міжнародним стандартам і найвищим позитивним показникам.

Доцільно розглянути досвід інших країн і розробити свою систему на їх прикладі. Уряди провідних країн світу, й зокрема Європейського Союзу, продовжують вживати різноманітних заходів для посилення безпеки кіберпростору як елементу глобальної міжнародної безпеки. Водночас особлива увага приділяється розробкам стратегічних документів із питань кібербезпеки, їх регулярному оновленню та контролю виконання плану заходів реалізації на основі оцінки ефективності й спроможностей.

На нашу думку, є сенс частково перейняти досвід Китаю та Франції, адже наразі інтернет-мережа України досить доступна й неконтрольована. Звісно, впровадження системи КНР неможливе, адже це призведе до масштабного протесту й бунту зі сторони народу, адже ми абсолютно демократична держава, проте жорсткіший контроль буде раціональним і правильним рішенням.

Для своєчасного поновлення таких документів в Україні необхідно розробити критерії оцінки стану кібербезпеки в державі. А після проведення відповідної оцінки визначити ключові напрями формування нової Стратегії кібербезпеки України, розрахованої на 2020–2025 роки.

З огляду на вищевказане, доцільно активно розробляти нормативно-правові акти, які будуть містити всі пропущені визначення термінів, узгодять законодавство України з міжнародно-правовими актами й виведуть державу на новий рівень.

ЛІТЕРАТУРА

1. Directive on security of network and information systems (NIS Directive). *ENISA : European union agency for cybersecurity*. URL: https://www.enisa.europa.eu/topics/nis-directive.

2. Бакалінська О.О., Бакалинський О.О. Правове забезпечення кібербезпеки України. *Адміністративне право і процес*. 2019. № 9. С. 100–108.

3. Гребенюк М.В. Деякі питання організаційно-правового забезпечення кібербезпеки: огляд кращих практик зарубіжного досвіду. *Кримінальне право*. 2019. № 2. С. 203–207.

4. Довгань О.Д., Танасюк А.В. Глобальна культура кібербезпеки в системі запобігання кіберзлочинності в Україні. *Інформація і право*. 2018. № 3. С. 94–103.

5. Камчатний М.В. Історія міжнародно-правового регулювання питань, пов'язаних із застосуванням комп'ютерних технологій. *Проблеми законності*. 2016. Вип 134. С. 199–207.

6. Олексюк Л.В. Кращі практики управління кібербезпекою. Оглядовий звіт. 2019. 130 с. URL: file:///C:/Users/User/Downloads/Report_on_Cybersecurity_04.pdf.

7. Петровський О.М., Лівчук С.Ю. Проблеми боротьби з кіберзлочинністю: міжнародний досвід та Українські реалії. *Молодий вчений*. 2019. № 12.1 (76.1). С. 55–59. URL: http://molodyvcheny.in.ua/files/journal/2019/12.1/13.pdf.

8. Правова база української кібербезпеки: загальний огляд і аналіз. Міжнародна фундація виборчих систем в Україні, 2019. 35 с.

9. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : Постанова Кабінету Міністрів України № 518 від 19 червня 2019 р. / Кабінет Міністрів України. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF.