УДК 342.9:004
DOI https://doi.org/10.32837/pyuv.v0i1(30).532

А. В. Тарасюк
orcid.org/0000-0002-0479-0666
кандидат юридичних наук,
головний науковий співробітник наукової лабораторії
забезпечення інформаційної та кібернетичної безпеки
Науково-дослідного інституту інформатики і права
Національної академії правових наук України

ПРІОРИТЕТИ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ НА СУЧАСНОМУ ЕТАПІ

Постановка проблеми. Головним чинником формування системи кіберзахисту інформації й регулятора людської діяльності в інформаційній сфері у процесі забезпечення кібербезпеки як соціального феномена є правові та морально-етичні принципи, відповідальність кожного суб'єкта, які базуються на загальноприйнятих правилах поведінки в суспільстві й підкріплюються законодавчими заходами. Можна також зазначити, що в теперішній час відчувається нагальна потреба цілеспрямованого формування інформаційної культури суспільства, від чого значною мірою залежить успішне розв'язання проблем кібербезпеки й подолання викликів, котрі виникають у процесі творення світового інформаційного простору.

На зайвим є підкреслити, що лишень на адміністративних, фізичних і технічних засобах ефективну систему кіберзахисту сформувати неможливо, оскільки її дієвість залежить передусім від людини, її професійних та особистісних якостей. Її стійкість зумовлюється професіоналізмом і згуртованістю колективу, а підвищення результативності відбувається за рахунок законодавчих і морально-етичних заходів. Утім, звісно, найдосконаліші правові акти й найефективніша кадрова політика не є гарантією належного розв'язання безпекових проблем.

Формулювання цілей статті. Метою статті є дослідження актуальних питань правового забезпечення кібербезпеки в Україні.

Виклад основного матеріалу. З огляду на зростаючу роль кіберпросторі та кібербезпеки більшість світових держав розробляють власні стратегії кібербезпеки та відповідне національне законодавство. Зокрема, нині 27 країн-членів НАТО, Європейський Союз (ЄС), 12 країн Європи, що не є членами НАТО, а також 38 інших країн затвердили національні стратегії кібербезпеки [1].

На законодавчому рівні необхідність захисту кібернетичного простору вперше передбачено воєнною доктриною США "Concept Force XXI" (1996) [2]. З усвідомленням глобального характеру кібербезпеки зросла роль міжнародних інститутів у розв'язанні цієї проблематики. Приміром, Міжнародний союз електрозв'язку (ITU) сформулював таке визначення кібернетичної безпеки в контексті діяльності цієї організації: сукупність безпекових принципів, стратегій і засобів забезпечення, гарантії безпеки, основні засади управління ризиками, діяльність, підготовка кадрів, практичний досвід, страхування, механізми й технології захисту кібернетичного простору, ресурсів союзу та користувачів. Найбільш загальними завданнями забезпечення кібербезпеки було визначено гарантування цілісності, доступності та конфіденційності інформації [3].

В Україні кібербезпека розглядається як складник національної безпеки. Стратегія кібербезпеки України була затверджена Указом Президента України від 15 березня 2016 р. [4]. Ця Стратегія базується на положеннях Конвенції про кіберзлочинність, ратифікованої Законом України від 7 вересня 2005 р. № 2824-IV [5], законодавства України щодо забезпечення національної безпеки, законодавства з питань засад внутрішньої та зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та іншої захищуваної інформації, а також спрямована на реалізацію до 2020 р. Стратегії національної безпеки України, затвердженої Указом Президента України від 26 травня 2015 р. № 287 «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 р. «Про Стратегію національної безпеки України» [6].

Закон України «Про основні засади забезпечення кібербезпеки України», прийнятий 5 жовтня 2017 р. [6] заклав загальні засади побудови національної системи кібербезпеки, а також визначив основні завдання та компетенцію суб'єктів забезпечення кібербезпеки.

Крім позитивної динаміки розвитку законодавства у сфері забезпечення кібербезпеки, варто зазначити, що необхідно узгодити національне законодавство з міжнародними стандартами. Зокрема, в законодавстві України не наведені визначення таких термінів, як «користувач послуг», «дані про рух інформації» та «електронні докази» і не регулюються «термінове збереження комп'ю-

терних даних, які зберігаються», «термінове збереження та часткове розкриття даних про рух інформації», що заважає ефективному виконанню положень Будапештської конвенції та обмежує можливості взаємодопомоги з іншими країнами у сфері попередження кіберзлочинності та протидії кіберзлочинам.

Крім того, експерти зазначають проблемні моменти правового забезпечення кібербезпеки в Україні [9]:

– непослідовність у термінології, адже Закон України «Про основні засади забезпечення кібербезпеки України» впроваджує низку нових термінів, які не узгоджуються з термінами, які раніше використовувались у законодавстві;

– відсутність закону про критичну інфраструктуру, внаслідок чого нині відсутня єдина національна система захисту критичної інфраструктури, а регуляторні правила щодо її захисту – недостатні та непослідовні;

– відсутність правил щодо проведення аудитів інформаційної безпеки об'єктів критичної інфраструктури, які мають ґрунтуватись на міжнародних стандартах, включаючи стандарти Європейського Союзу і НАТО, і розроблятися з обов'язковим залученням представників основних національних суб'єктів сфери кібербезпеки, наукових установ, незалежних аудиторів, експертів із кібербезпеки тощо;

– дублювання підвідомчості (до числа основних органів, відповідальних за контроль кібербезпеки в Україні, належать Міністерство оборони України, Державна служба спецзв'язку та захисту інформації, Служба безпеки України, Національна поліція України, Національний банк України та розвідувальні органи). Є правова невизначеність щодо повноважень, завдань та обов'язків державних агенцій, відповідальних за захист критичної інфраструктури. Наприклад, хоча Закон України «Про основні засади забезпечення кібербезпеки України» передбачає повноваження Служби безпеки України щодо кіберінцидентів, це не відображено належним чином в інших нормативно-правових актах. Правоохоронні повноваження, на кшталт тих, про які йдеться в Будапештській конвенції, не є чітко визначеними в українському кримінально-процесуальному законодавстві, і це негативно впливає на співробітництво між надавачами правоохоронних послуг, на права конфіденційності, а іноді й на верховенство права;

– відсутність вимог щодо безпеки та інформування для операторів об'єктів критичної інфраструктури та провайдерів цифрових послуг. Директива NIS [9] вимагає, щоб країни встановили вимоги щодо безпеки та інформування для операторів суттєвих послуг і для провайдерів цифрових послуг. Закон України «Про основні засади забезпечення кібербезпеки України» вимагає від операторів об'єктів критичної інфраструктури інформувати CERT-UA про кіберінциденти, однак, оскільки законопроект про критичну інфраструктуру перебуває на розгляді, ця норма залишається декларативною. Постановою Кабінету Міністрів України № 518 від 19 червня 2019 р. [10] визначено, що власник та/або керівник об'єкта критичної інфраструктури зобов'язані організувати невідкладне інформування CERT-UA (у разі наявності – галузевої команди реагування на комп'ютерні надзвичайні події), а також функціонального підрозділу контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Центрального управління Служби безпеки України (Ситуаційний центр забезпечення кібербезпеки Служби безпеки України) або відповідного підрозділу регіонального органу Служби безпеки України про кіберінциденти та кібератаки, які стосуються його об'єкта критичної інформаційної інфраструктури. Водночас процедура та строки такого інформування не встановлені. Крім того, чітко не визначено, чи належать провайдери цифрових послуг до категорії об'єктів критичної інфраструктури;

– відсутність довгострокового стратегічного планування з чітко визначеними проміжними результатами, часовими рамками та відповідальністю за їх досягнення;

– бюджетні обмеження здатності держави платити конкурентоспроможні зарплати для залучення та утримання високопрофесійних фахівців із питань кібербезпеки [8].

Також, виходячи з аналізу базових категорій, які наводяться в Законі України «Про основні засади забезпечення кібербезпеки України», вважаємо за доцільне на законодавчому рівні визначити:

– поняття «стан захищеності»;

– поняття «цифрове комунікативне середовище»;

– критерії забезпечення кібербезпеки.

Визначення терміна «кібербезпека» базується на дефініції терміна «*кіберпростір*», який у Законі «Про основні засади забезпечення кібербезпеки України» визначено як *«середовище (віртуальний простір), яке надає можливості (послуговує) здійсненню комунікацій та/або реалізації суспільних відносин, утворене внаслідок функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій із використанням Інтернету та/або інших глобальних мереж передачі даних»*.

Запропоноване визначення беззаперечно виключає з поля дії автономні автоматизовані системи управління (наприклад, об'єктів атомної енергетики), які, саме з огляду на вимоги безпеки, є автономними.

Надане визначення терміна «кіберпростір» суб'єктно обмежує «простір» лише інформаційни-

ми (автоматизованими), телекомунікаційними та інформаційно-телекомунікаційними системами, тобто автоматизованими системами.

Крім того, у Законі не надано визначення терміна «середовище», що призводить до невизначеності у тлумаченні терміна «кіберпростір».

Кіберпростір – це специфічне інформаційне середовище, якому притаманні особливі просторово-часові властивості транскордонності, екстериторіальності, децентралізованості, багатоканальності, розгалуженості, імітаційності, гіпертекстовості, віртуальності, яке виникло й функціонує за допомогою комп'ютерів та інших електронних пристроїв (супутників, телевізійних пристроїв, засобів стільникового зв'язку, ігрових приставок і т.п.) на базі інформаційно-телекомунікаційних мереж, насамперед Інтернет, а тому має, як правило, параметри глобального інформаційного обсягу й виконує функції комунікації, розміщення й використання інформації, надання інформаційних та інших соціально значущих послуг, взаємодії державних інституцій, громадянського суспільства й окремої особи, яке є імітаційним чинником впливу на індивідуальну, групову та масову свідомість, економічну, соціально-політичну, духовну (культурну, ідеологічну, наукову, освітню, релігійну) та інші сфери життєдіяльності суспільства.

Варто також зазначити, що широко вживані в науковому та професійному вжитку терміни «захист інформації», «захист інформаційних технологій» і «захист кіберпростору» дещо різняться за змістом. Не заглиблюючись у деталі, можна сказати, що захист інформації являє собою сукупність методів і засобів, які забезпечують цілісність, конфіденційність і доступність інформації в разі впливу на неї загроз природного або штучного характеру. Натомість безпека інформаційних технологій передбачає ще й захист технічної частини й забезпечення працездатності, зокрема під час кібератак. Захист кіберпростору – це безпека комунікаційних систем, об'єктів критичної інформаційної інфраструктури, комунікацій та систем керування [11, с. 24].

Дискусійні аспекти законодавчого визначення базових категорій можуть слугувати певними причинами деформацій самої мети та предмета правового регулювання, а також невірного визначення комплексу заходів щодо правового забезпечення кібербезпеки.

Так, вважаємо доцільним у визначенні терміна «*кіберзлочин*» словосполучення «міжнародними договорами» замінити на словосполучення «міжнародним правом». Такий підхід забезпечить єдність термінологічного тлумачення на рівні національного та міжнародного законодавства.

Щодо терміна «*критично важливі об'єкти інфраструктури (критичні інфраструктурні об'єкти)*» зауважуємо, що запропоноване формулювання та розкриття цього терміна не передбачає виділення саме об'єктів такої інфраструктури, а вказує лише на «підприємства, установи та організації незалежно від форм власності».

Висновки. Отже, Закон України «Про основні засади забезпечення кібербезпеки України» радше є дорожньою картою для розробки майбутніх нормативних актів, а не всеосяжним законом про кібербезпеку, який регулює повний спектр питань кібербезпеки та відповідає міжнародним стандартам і найкращим практикам. При цьому подальше вдосконалення правового забезпечення кібербезпеки в Україні передбачає виконання таких першочергових кроків:

– проведення аналізу чинного законодавства з метою виявлення норм, які суперечать Директиві NIS, а також неузгодженостей термінологічного характеру, внесення поправок відповідно до рекомендацій, вироблених на основі такого аналізу;

– розробка стратегічної внутрішньої комунікації стосовно кіберінцидентів. Директива NIS вимагає від країн встановлення протоколів безпеки і комунікацій для операторів суттєвих послуг і провайдерів цифрових послуг;

– прийняття закону про критичну інфраструктуру та розробка на його основі відповідних підзаконних нормативно-правових актів;

– розмежування повноважень державних органів у сфері забезпечення кібербезпеки, передусім шляхом внесення змін до законів, що визначають правовий статус та компетенцію Служби безпеки України та Державної служби спецзв'язку та захисту інформації [8].

Упродовж останніх років нашою державою здійснено низку позитивних кроків для виконання своїх міжнародних зобов'язань щодо вдосконалення законодавства у сфері кібербезпеки, однак цей напрям роботи все ще потребує значної уваги та відповідних зусиль.

Оскільки розвиток правового забезпечення кібербезпеки в Україні пов'язаний з євроінтеграційними прагненнями України, дієвою для вдосконалення національного законодавства у сфері кібербезпеки з урахуванням умов Угоди про асоціацію між Україною, з однієї сторони, і ЄС і державами-членами, з іншої сторони (2014), буде імплементація досвіду та кращих практик країн ЄС і стандартів НАТО. Зокрема, найближчим часом Україна має розробити вимоги для операторів об'єктів критичної інфраструктури щодо інформування із зазначенням обставин, за яких вони мають інформувати про інциденти, формату, шаблонів та процедури такого інформування, а також категоризації кіберінцидентів, встановити процедуру інформування інших держав про кіберінциденти, які можуть на них вплинути, з урахуванням вимог конфіденційності та комерційної таємниці, здійснити аудит чинного законодав-

ства на предмет виявлення норм, які суперечать Директиві NIS, а також неузгодженостей термінологічного характеру, а також на законодавчому рівні розмежувати й конкретизувати повноваження та сферу відповідальності суб'єктів забезпечення кібербезпеки.

Література

1. Логінова Н.І. Правові основи кібербезпеки в Україні. *Правові та інституційні механізми забезпечення розвитку держави та прав в умовах євроінтеграції :* матеріали міжнар. наук.-практ. конференції. Одеса, 2016. Т. 1. С. 575–577.

2. Office for the Deputy Director, Acquisition Career Management, 1996. ArmyRD&A., Томи 996&–998.

3. Рекомендация МСЭ-Т X.1205. Обзор кибербезопасности. Женева: МСЕ, 2010. С. 55. URL: www.itu.int/ITU-T/recommendations/rec.aspx?rec=9136&lang=ru; ITU Global Cybersecurity Agenda (GCA) A Framework for International Cooperationin Cybersecurity. URL: https://www.intgovforum.org/Substantive_2nd_IGF/ITU_GCA_E.pdf.

4. Стратегія кібербезпеки України : Указ Президента України № 96/2016 від 15.03.2016 р. URL: http://zakon4.rada.gov.ua/laws/show/96/2016.

5. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 07.09.2005 р. URL: https://zakon.rada.gov.ua/laws/show/994_575.

6. Стратегія національної безпеки України : Указ Президента України № 287 від 26.05.2015 р. URL: https://zakon.rada.gov.ua/laws/show/287/2015#n14.

7. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19.

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

9. Directive on security of network and information systems (NIS Directive). URL: https://www.enisa.europa.eu/topics/nis-directive.

10. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : Постанова Кабінету Міністрів України № 518 від 19.06.2019 р. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF.

11. Савчук М.М. Захист інформаційних технологій та кібербезпека. Стенограма наукової доповіді на засіданні Президії НАН України 25 вересня 2019 року. *Вісник НАН України*. 2019. № 11. С. 23–28.

12. Ткачук Т.Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір : монографія. Київ : ТОВ «Видавничий дім «АртЕк», 2018. 422 с.

Анотація

Тарасюк А. В. **Пріоритети правового забезпечення кібербезпеки в Україні на сучасному етапі.** – Стаття.

В Україні кібербезпека розглядається як складник національної безпеки. В останні роки наша країна здійснила низку позитивних кроків для виконання своїх міжнародних зобов'язань щодо вдосконалення законодавства про кібербезпеку.

Водночас поряд із позитивною динамікою розвитку законодавства у сфері кібербезпеки варто зазначити, що є необхідність надалі узгодити національне законодавство з міжнародними стандартами. Зокрема, Закон України «Про основні засади кібербезпеки України» є радше дорожньою картою розробки майбутніх нормативно-правових актів, а не всеосяжним законом про кібербезпеку, який регулює повний спектр питань кібербезпеки та відповідає міжнародним стандартам та найкращим практикам. Експерти також зазначають проблемні аспекти правового забезпечення кібербезпеки в Україні: непослідовність та неузгодженість термінології; відсутність закону про критичну інфраструктуру; відсутність правил проведення аудиту інформаційної безпеки критично важливих інфраструктурних об'єктів, які мають базуватися на міжнародних стандартах; дублювання повідомлень про кіберінциденти; відсутність вимог щодо безпеки та інформації щодо операторів критичної інфраструктури та постачальників цифрових послуг; відсутність довгострокового стратегічного планування з чітко визначеними проміжними результатами, термінами та відповідальністю за їх досягнення; бюджетні обмеження щодо змоги держави виплачувати конкурентні зарплати для залучення та утримання високопрофесійних фахівців із кібербезпеки.

Оскільки розвиток правової бази кібербезпеки в Україні пов'язаний із прагненнями європейської інтеграції України, буде ефективним вдосконалення національного законодавства про кібербезпеку з урахуванням вимог Угоди про асоціацію між Україною та ЄС та її державами-членами (2014) та впровадженням досвіду і найкращих практик та стандартів країн ЄС.

Ключові слова: кібербезпека, правове забезпечення, законодавство, директива.

Summary

Tarasyuk A. V. **Cyber security priorities of legal support in Ukraine at the present stage.** – Article.

In Ukraine, cybersecurity is seen as a component of national security. In recent years, our country has taken a number of positive steps to fulfill its international obligations to improve cybersecurity legislation.

At the same time, along with the positive dynamics of the development of legislation in the field of cybersecurity, it should be noted that there is a need to further align national legislation with international standards. In particular, the Law of Ukraine "On the Fundamental Principles of Cybersecurity of Ukraine" is rather a roadmap for the development of future regulations rather than a comprehensive cybersecurity law that regulates the full range of cybersecurity issues and meets international standards and best practices. Experts also point out the following problematic aspects of cybersecurity legal support in Ukraine: inconsistency and inconsistency of terminology; lack of a critical infrastructure law; lack of rules for conducting information security audits of critical infrastructure facilities that must be based on international standards; duplication of cyber incident reporting; lack of security and information requirements for critical infrastructure operators and digital service providers; lack of long-term strategic planning with clearly defined interim results, timelines and responsibility for their achievement; budgetary constraints on the ability of the state to pay competitive salaries to attract and retain highly professional cybersecurity professionals.

Accordingly, this area of work still requires considerable attention and efforts. As the development of cybersecurity legal support in Ukraine is linked to Ukraine's European integration aspirations, it will be effective to improve national cybersecurity legislation to take into account the terms of the Association Agreement between Ukraine and the EU and its Member States, on the other hand (2014). implementation of EU countries' experience and best practices and standards.

Key words: cybersecurity, legal support, legislation, directive.