РОЗДІЛ 7. АДМІНІСТРАТИВНЕ ПРАВО І ПРОЦЕС; ФІНАНСОВЕ ПРАВО; ІНФОРМАЦІЙНЕ ПРАВО

УДК: 340.1
DOI https://doi.org/10.24144/2307-3322.2024.85.3.1

ПРАВОВІ ОСНОВИ РЕГЛАМЕНТАЦІЇ КІБЕРБЕЗПЕКИ

Мазур Я.П.,
аспірант кафедри конституційного, адміністративного
та фінансового права
Хмельницького університету управління та права
імені Леоніда Юзькова
ORCID: 0009-0003-2057-1732
e-mail: yarmazur54@gmail.com

Мазур Я.П. Правові основи регламентації кібербезпеки.

Стаття присвячена комплексному та цілісному аналізу законодавчої бази України у сфері кібербезпеки. На основі систематичного огляду нормативно-правових актів виявлено основні тенденції розвитку законодавства, проаналізовано їх відповідність сучасним викликам та міжнародним стандартам. Окрім того, необхідно зазначити, що увага приділяється впливу російської агресії, яка триває з анексії Криму та окупації Луганської та частини Донецької областей, а також з дня повномасштабного вторгнення рф на територію нашої суверенної держави на зміни в законодавстві. Дослідження дозволяє оцінити ефективність чинного законодавства та сформулювати пропозиції щодо його вдосконалення та поліпшення. Результати дослідження можуть бути використані органами державної влади, підприємствами та організаціями для підвищення рівня кіберзахисту та забезпечення національної безпеки України в цілому. Процес формування та становлення правового поля для забезпечення кібербезпеки в Україні не припиняється, а триває й досі, оскільки це нешвидкісний процес. Незважаючи на те, що основні та головні вектори державної політики в цій сфері вже визначені й окреслені, все ж законодавство потребує подальшого вдосконалення для адекватного та повного реагування на сучасні кіберзагрози. Виклики цифрового світу вимагають постійного оновлення нормативно-правової бази. Ми вважаємо, що для подальшого розвитку та покращення законодавства у сфері кібербезпеки необхідно: удосконалити нормативно-правову базу з урахуванням постійної динаміки кіберпростору, також впровадити ефективні механізми правового захисту від кіберзагроз, які постійно існують, особливо через агресію з боку російської федерації, окрім того, варто підвищити рівень кіберзахисту критично важливої інфраструктури. Також, на наш погляд, вагомим та важливим є забезпечення гармонізації національного законодавства з міжнародними стандартами. Також рахуємо за доцільне, розробити інноваційні, сучасні правові інструменти для захисту інформаційних ресурсів, які існують у нашій державі в цілому. Тобто глибокий аналіз цих питань сприяє комплексному розумінню проблем кібербезпеки та дозволяє розробити ефективні заходи для захисту інформаційного простору України.

Ключові слова: кібербезпека, кіберпростір, кіберзагрози, захист даних, інформація.

Mazur Ya.P. Legal basis of regulation of cyber security.

The article is devoted to a comprehensive and holistic analysis of the legislative framework of Ukraine in the field of cybersecurity. On the basis of a systematic review of normative legal acts, the main trends in the development of legislation have been identified, their compliance with modern challenges and international standards has been analyzed. In addition, it should be noted that attention is paid to the impact of Russian aggression, which continues from the annexation of the Crimea and the occupation of Luhansk and part of Donetsk regions, as well as from the day of the full-scale invasion of

the Russian Federation into the territory of our sovereign state to changes in the legislation. The study allows to assess the effectiveness of the current legislation and formulate proposals for its improvement and improvement. The results of the study can be used by state authorities, enterprises and organizations to increase the level of cyber defense and ensure the national security of Ukraine as a whole. The process of formation and formation of the legal framework for ensuring cybersecurity in Ukraine does not stop, but continues to this day, as it is a slow process. Despite the fact that the main and main vectors of state policy in this area have already been defined and outlined, the legislation still needs further improvement to adequately and fully respond to modern cyber threats. The challenges of the digital world require constant updating of the regulatory framework. We believe that in order to further develop and improve legislation in the field of cybersecurity, it is necessary: to improve the regulatory framework taking into account the constant dynamics of cyberspace, also to introduce effective mechanisms of legal protection against cyber threats that constantly exist, especially due to aggression by the Russian Federation, in addition, it is necessary to increase the level of cyber defense of critical infrastructure. Also, in our opinion, it is important and important to ensure the harmonization of national legislation with international standards. We also consider it appropriate to develop innovative, modern legal tools to protect information resources that exist in our country as a whole. That is, a deep analysis of these issues contributes to a comprehensive understanding of cybersecurity problems and allows us to develop effective measures to protect the information space of Ukraine.

Key words: cybersecurity, cyberspace, cyber threats, data protection, information.

Постановка проблеми. У сучасних умовах збройної військової агресії рф проти незалежної та суверенної України, питання законодавчої регламентації забезпечення кібербезпеки в нашій державі має надзвичайно важливе та актуальне значення. Кібербезпека є досить критичною проблемою в наш час, оскільки кіберзагрози стають все більш складними, особливо в умовах війни з росією. Для вирішення цих проблем необхідні інноваційні підходи до кібербезпеки. Зростаюча складність кібератак робить захист інформації дуже вагомим для всіх людей та організацій. Необхідно дати визначення поняттю кібербезпека. Кібербезпека – це комплекс заходів, які є спрямованими на захист комп'ютерного обладнання, програмного забезпечення та даних від кібератак. Основна та головна мета кібербезпеки – запобігти несанкціонованому доступу до інформації та забезпечити її цілісність, а також конфіденційність. Кібербезпека держави має вплив на всі складові частини її політики.

Мета дослідження. Проведення дослідження особливостей формування законодавства України у сфері кібербезпеки, а також які проблеми воно вирішує та визначити шляхи його вдосконалення для забезпечення більш надійного захисту інформаційного простору держави в цілому.

Стан опрацювання проблематики. Питання кібербезпеки набуло надзвичайної актуальності, тому що сучасне життя неможливо уявити без використання інформаційних технологій, а отже, кожний з нас стикається з ризиками, які пов'язані з кіберзагрозами. Серед науковців необхідно виділити праці: Бакалінської О.О., Бакалинського О. О., Веселевої Л.Ю.

Виклад основного матеріалу. Кібербезпека має дуже вагоме значення, адже вона здійснює захист від деяких з найсерйозніших проблем в галузі кібербезпеки, а саме: крадіжка та знищення великої кількості типів даних. Це включає конфіденційну інформацію, особисту інформацію, захищену медичну інформацію, персональні дані, дані про інтелектуальну власність та інформаційні системи, що використовуються урядом та підприємствами.

Зростання кількості та складності кіберзагроз потягло за собою створення нормативної бази і стандартів щодо кібербезпеки. Парламент нашої держави мав прийняти ряд законодавчих актів, які спрямовані на підвищення рівня кібербезпеки в Україні в цілому. До прийняття Закону України «Про основні засади забезпечення кібербезпеки України» правову основу кібербезпеки України становили Основний закон нашої держави, закони України «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах» та інші закони, Конвенція Ради Європи про кіберзлочинність [1], а також інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, Доктрина інформаційної безпеки України й інші нормативно-правові акти.

Як вже раніше зауважувалось про Закон України «Про основні засади забезпечення кібербезпеки України», то доцільно та важливо підкреслити, що він є одним із найголовніших та досить значних, адже вищезазначений закон встановлює головні принципи й норми забезпечен-

ня кібербезпеки в Україні та визначає відповідальність за захист інформації в кіберпросторі, окрім того визначає вагомі аспекти, що є тісно пов'язаними з кібербезпекою, а саме: захист персональних даних громадян, реагування на кібератаки, регулювання діяльності в галузі кібербезпеки [2].

Окрім того, звертаємо увагу на те, що дія Закону України «Про основні засади здійснення кібербезпеки України» не поширюється на відносини та послуги, що є пов'язаними із змістом інформації, яка обробляється в комунікаційних та/ або в технологічних системах, соціальних мережах, приватних електронних інформаційних ресурсах у мережі Інтернет (включаючи блог-платформи, відеохостинги, інші веб-ресурси), а також не стосується інформаційно-телекомунікаційних систем, у яких циркулює інформація, що відноситься та утворює державну таємницю. Проте запровадження положень Закону у даній сфері може розглядатися як істотне порушення прав людини відповідно до положень Європейської конвенції про захист прав людини і основних свобод, а саме ст. 10 Конвенції [3].

Національна система кібербезпеки являє в собі комплексну систему взаємодії між Державною службою спеціального зв'язку та захисту інформації України, Національною поліцією України, Службою безпеки України, Міністерством оборони України та Генеральним штабом Збройних Сил України, розвідувальними органами. Їхня діяльність має на меті забезпечити кібербезпеку та взаємопов'язані заходи політичного, науково-технічного, інформаційного, освітнього характеру, а також кіберзахисту об'єктів критичної інформаційної інфраструктури.

Основним суб'єктом національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України [4], остання здійснює забезпечення реалізації державної політики щодо захисту в кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлюється законодавством.

Необхідно зазначити, що Закон України «Про основні засади забезпечення кібербезпеки України» визначив, хто і за що відповідає в сфері захисту від кібератак, розподіливши повноваження між різними державними органами та іншими суб'єктами.

Також потрібно згадати й Закон України «Про захист персональних даних» від 01.06.2010 року, який був узгоджений з загальним регламентом ЄС про захист даних (GDPR). Вищезазначений закон встановлює вимоги щодо обробки особистих даних та відповідальність за їх захист [5]. Щоб протистояти кіберзагрозам, Україна досить активно наближає своє законодавство до міжнародних стандартів та посилює міжнародне співробітництво. Саме тому співробітництво між країнами в сфері кібербезпеки стає тільки потрібнішим та важливішим.

Не менш вагомим є також Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР. Останній був прийнятий з ціллю забезпечити захист інформації в інформаційно-телекомунікаційних системах (ІТС). Також він визначає порядок доступу до інформації в інформаційно-телекомунікаційній системі, умови обробки інформації в системі, забезпечення захисту інформації в інформаційно-телекомунікаційній системі, права та обов`язки забезпечення захисту інформації в інформаційно-телекомунікаційних системах, повноваження державних органів у сфері захисту інформації в інформаційно-телекомунікаційних системах, а також відповідальність за порушення законодавства про захист інформації в інформаційно-телекомунікаційних системах [6].

Хочемо підкреслити про міжнародну діяльність в галузі захисту інформації в автоматизованих системах, тому що вищезгаданий Закон дозволяє іноземним державам, іноземним фізичним та юридичним особам:

- бути власниками автоматизованих систем в Україні;
- бути власниками інформації, яка розповсюджується та обробляється в автоматизованих системах України;
- засновувати спільні підприємства, для того щоб створити автоматизовані системи, а також постачати інформацію до автоматизованих систем України, обмінюватись інформацією між автоматизованими системами України та автоматизованими системами інших держав.

Цей Закон є надзвичайно важливим, адже забезпечення безпеки інформації в інформаційно-телекомунікаційних системах є одним із провідних та основних факторів національної безпеки. Наше переконання грунтується на тому, що інформаційні атаки можуть бути інструментом для того, щоб втручатись у різні політичні процеси, а також економічного шпигунства та створення інших загроз для держави в цілому.

Доцільно також зауважити, що в 2016 році Україна прийняла національну стратегію кібербезпеки, що була введена в дію рішенням Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України», та затверджену указом Президента України № 96/2016. Вона зазначала головні та основні цілі й завдання у сфері захисту кіберпростору. Дана стратегія є дуже вагомим кроком для нашої держави в зміцненні захисту кіберпростору в умовах постійно зростаючих кіберзагроз. Вважаємо за потрібне зазначити головні напрямки вищезгаданої стратегії:

Основні напрямки цієї стратегії включали:

– Утворення правової бази: розвиток та поліпшення законодавства у сфері кібербезпеки для забезпечення цілісного захисту надзвичайно вагомих інформаційних інфраструктур та особистої інформації громадян.

– Інституційну підтримку: Утворення спеціальних структур для координації дій у сфері кібербезпеки, включаючи Національний координаційний центр кібербезпеки.

– Підвищення обізнаності: Збільшення рівня обізнаності населення та фахівців у сфері кібербезпеки завдяки навчальним програмам, вебінарам, тренінгам.

– Міжнародне співробітництво: Стрімке збільшення співпраці з міжнародними партнерами у сфері кібербезпеки з ціллю обміну сучасним досвідом та інформацією [7].

Важливо підкреслити, що указом Президента України від 26 серпня 2021 року № 447/2021 визнано такою, що втратила чинність, статтю 2 Указу Президента України від 15 березня 2016 року № 96 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України», та введено в дію рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України», тобто виходячи з цього можна зазначити, що було затверджено нову стратегію кібербезпеки в нашій державі в цілому. Хочемо зауважити, що в Стратегії окреслено головні напрями зовнішньополітичної діяльності України у сфері кібербезпеки, а саме зазначається, що наша держава у сфері кібербезпеки обов'язково має забезпечити поглиблення євроінтеграційних процесів, здійснивши уніфікацію підходів та засобів забезпечення кібербезпеки з усталеними практиками Європейського союзу і НАТО [8].

24 лютого 2022 року російська федерація розпочала повномасштабне вторгнення на територію суверенної та незалежної України, це дуже негативно вплинуло на життя всіх українців та держави в цілому. Змін зазнали всі сфери. Не оминуло це й кіберпростір. Для протидії зростаючій кіберзагрозі, яка постійно існує, через країну-агресорку рф, українське законодавство було доповнено новими нормами, які стосуються відповідальності за кіберзлочини. Ці зміни дозволяють правоохоронним органам ефективніше та швидше розслідувати кіберзлочини та притягувати винних до відповідальності. Хочемо зазначити, що зміни містяться у двох законах:

– Закон України «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам» № 2137-IX від 15.03.2022 [9];

– Закон України «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» № 2149-IX від 24.03.2022 [10]. Головні завдання та мета вищезазначених нормативно-правових актів можна зазначити оптимізацію національної системи кібербезпеки для протидії кіберзагрозам, впровадження швидких та доцільних кримінально-правових механізмів боротьби з кіберзлочинністю, яка особливо часто виникає в період дії воєнного стану на території нашої держави.

Цілком та повністю розділяємо думку, що Україна зацікавлена у впровадженні міжнародного досвіду у сфері правового забезпечення кібербезпеки, оскільки він необхідний у якості позитивного прикладу у формуванні відповідної політики і побудові власної системи правового забезпечення кібербезпеки [11, с. 360].

Також погоджуємося з тим, що забезпечення безпеки в кіберпросторі не закінчується тільки заходами державного регулювання та контролю, а навпаки в багатьох випадках цілком залежить від відповідальної, виваженої та адекватної поведінки учасників правовідносин [12].

Висновки. Важливо зауважити, що попри те, що законодавство України у сфері кібербезпеки ще розвивається, наша держава вже подолала досить складний етап визначення стратегічних напрямів державної політики саме в цій галузі. Тому можна вважати це значним кроком вперед, хоча, звісно, й залишаються невирішені й проблемні питання. Попереду нас чекає ще немаленький обсяг роботи, який буде спрямований на нормативно-правове врегулювання у сфері кібербез-

пеки. Досліджуючи перспективи розвитку та вдосконалення законодавчого регулювання кібербезпеки в Україні, на наш погляд вагомим є: розробка цілісного законодавства з кібербезпеки, яке включатиме в себе цілком усі моменти цієї проблематики, а саме: захист інформації, кіберзлочинність, критично важливі об'єкти, особисті дані та приватність; також вважаємо, що важливим є зміцнення механізмів реагування на кіберзагрози, а також поліпшення та модернізація співпраці між правоохоронними органами та іншими державними установами; не можна обійти стороною й зарубіжний досвід та співпрацю з міжнародними організаціями у сфері кібербезпеки з метою обміном досвіду.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Про кіберзлочинність. Конвенція Ради Європи від 21.11.2001. *Офіційний вісник України* від 10.09.2007 р. № 65. С. 107. Ст. 2535, код акту 40846/2007.
2. Про основні засади забезпечення кібербезпеки України. Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 03.10.2024).
3. Про захист прав людини і основних свобод. Європейська конвенція. від 04.11.1950. *Офіційний вісник України* від 16.04.1998. № 13 / № 32 від 23.08.2006. С. 270.
4. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 07.11.2018, № 2155-VIII. *Відомості Верховної Ради України* (ВВР). 2006. № 30. Ст. 258.
5. Про захист персональних даних. Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 03.10.2024).
6. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР. *Відомості Верховної Ради України* (ВВР), 1994, № 31, ст. 286. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 03.10.2024).
7. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про стратегію кібербезпеки України»: Указ Президента України; Стратегія від 15.03.2016 № 96/2016. URL: https://zakon.rada.gov.ua/laws/show/96/2016#Text (дата звернення: 03.10.2024).
8. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України; Стратегія від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 03.10.2024).
9. «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам»: Закон України від 15.03.2022 № 2137-IX. URL: https://zakon.rada.gov.ua/laws/show/2137-20#Text (дата звернення: 03.10.2024).
10. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану: Закон України від 24.03.2022 № 2149-IX. URL: https://zakon.rada.gov.ua/laws/show/2149-20#Text (дата звернення: 03.10.2024).
11. Веселова Л.Ю. Адміністративно-правові основи кібербезпеки в умовах гібридної війни: дис. …д-ра юрид. наук : 12.00.07. Одеса, 2021. 500 с.
12. Бакалінська О.О., Бакалинський О.О. Правове забезпечення кібербезпеки в Україні. Підприємництво, господарство і право. *Адміністративне право і процес.* 2019. № 9. С. 100–108. URL: http://pgp-journal.kiev.ua/ archive/2019/9/18.pdf (дата звернення: 03.10.2024).