АДМІНІСТРАТИВНЕ ПРАВО І ПРОЦЕС; ФІНАНСОВЕ ПРАВО; ІНФОРМАЦІЙНЕ ПРАВО
ADMINISTRATIVE LAW AND PROCESS; FINANCE LAW; INFORMATION LAW

https://doi.org/10.26565/2075-1834-2024-37-17
УДК 34.342.5

В. В. ГОРУЛЬКО
аспірант юридичного факультету
E-mail: vl.gorulko@karazin.ua ORCID:https://orcid.org/0000-0001-5921-6066
Харківський національний університет імені В.Н. Каразіна
м. Харків, 61022, майдан Свободи 4

ЗНАЧЕННЯ ПРАВОВОГО РЕГУЛЮВАННЯ У ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ В УМОВАХ ВІЙНИ: ДОСВІД ДЛЯ УКРАЇНИ

АНОТАЦІЯ. *Вступ.* У переважній більшості країн спостерігається постійна тенденція до значного збільшення кількості та розширення спектру кібератак з метою порушення конфіденційності, цілісності та доступності державних інформаційних ресурсів, зокрема тих, що поширюються в мережі Інтернет та об'єкти критичної інформаційної інфраструктури.

Короткий зміст основних результатів. Широкомасштабне розгортання гібридної війни проти нашої держави серйозно впливає на всі аспекти суспільного життя. Значною мірою стратегічний успіх протидії викликам гібридної війни залежить від ефективності та якості правового реагування. Забезпечення належного рівня кібербезпеки важко уявити без чітко спланованих спільних дій та заходів, розроблених відповідальними суб'єктами, які мають бути синхронізовані та реалізовуватися згідно з єдиним стратегічним планом та вектором розвитку національної системи кібербезпеки декларативного характеру. Саме тому кібербезпека у більшості країн світу визнається важливою складовою національної безпеки, забезпечення якої неможливе без формування та функціонування національної системи у сфері кібербезпеки, яка базується на таких принципах, як повага до принципів і норм міжнародного права, захист основоположних цінностей, визначених чинним законодавством, захист національних інтересів у кіберпросторі. Наголошується, що національна безпека держави значною мірою залежить від стану кібербезпеки. Доведено, що гібридна війна значно посилює вплив кіберзагроз на українське суспільство та актуалізує небезпеку цілеспрямованих кібератак як інструменту агресії проти нашої держави в контексті глобальних тенденцій щодо загроз у кіберпросторі.

Висновки. У процесі проведення дослідження нами сформульовано висновки, в яких особливу увагу приділено особливостям сучасного стану функціонування законодавства з кібербезпеки та розглянуто перспективні напрями його вдосконалення у майбутньому, що, у свою чергу, стане основою для удосконалення адміністративно-правового регулювання кібербезпеки в Україні.

КЛЮЧОВІ СЛОВА: *національна безпека, інформаційна безпека, кібербезпека, кіберпростір, воєнний стан, правове регулювання.*

Як цитувати: Горулько В. В. Значення правового регулювання у забезпеченні кібербезпеки в умовах війни: досвід для України. Вісник *Харківського національного університету імені В.Н. Каразіна, серія «Право».* 2024. Вип. 37. С. 150-155. https://doi.org/10.26565/2075-1834-2024-37-17

In cites: Horulko V.V. (2024). The significance of legal regulation in ensuring cyber security in the conditions of war: experience for Ukraine. *The Journal of V.N. Karazin Kharkiv National University, Series "Law"*, (37), P. 150-155. https://doi.org/10.26565/2075-1834-2024-37-17 (in Ukrainian)

Вступ. Актуальність теми визначається масштабами інформаційної війни, яку Росія веде проти України, та зростанням ролі захисту кіберпростору України у військовій сфері. Сьогодні, особливо у відношенні військових дій, можна вважати, що «кіберпростір є новою площиною створення та розповсюдження різноманітної інформації, який став новою рушійною силою економічного зростання, новою платформою соціального управління, новою формою міжнародного співробітництва та, крім того, абсолютно новою сферою державного суверенітету. Проте кіберпростір не лише забезпечує нас ресурсами та можливостями, але й містить загрози.

Посилення цифровізації та зв'язку збільшує ризики кібербезпеки, роблячи суспільство в цілому більш вразливим до кіберзагроз, посилюючи небезпеки, з якими стикаються люди, особливо під час дії воєнного стану.

Огляд праць з даної проблематики. Організаційно-правові проблеми забезпечення кібербезпеки в Україні у своїх наукових працях досліджували С. Гуржій, В. Петров, А. Тарасюк, Н. Ткачук та ін. Проте на сьогодні бракує суттєвих досліджень щодо забезпечення кібербезпеки в умовах воєнного стану, що свідчить про актуальність обраної теми.

Мета статті полягає у з'ясуванні правового регулювання у забезпеченні кібербезпеки в умовах війни для України.

Основні результати дослідження. Розвиток ІТ-законодавства в Україні, що регулює всі відносини всередині і навколо сектора високих технологій, ще не досягнув високої ефективності його функціонування в такому масштабі, як у розвинених західних країнах і деяких країнах Азії. Якщо правове регулювання високотехнологічного сектору в розвинутих країнах дозволяє як громадянам, так і державі отримувати значні прибутки та переваги, то в Україні все ще спостерігається слабке правове регулювання цих процесів. Сучасна система забезпечення інформаційної безпеки та кібербезпеки в Україні має бути єдиною та ефективною системою, що складається з обов'язкових компонентів, таких як: правовий, освітній та технічний [1, с. 34].

Війна в Україні стала сигналом глобального розвитку кіберзахисту та необхідності зміцнення кібербезпеки у світі. Війна ведеться і на полі бою, і в кіберпросторі. Фактично зараз відбувається перша у світі цифрова війна, на хід якої безпосередньо впливають високі технології. У 2022 році РФ втричі збільшила кількість кібератак проти України. В основному вони спрямовані на цивільну інфраструктуру, зокрема енергетику та логістику, а також державні реєстри.

Сьогодні ризик кібератак як на українські системи, так і на системи європейських партнерів залишається досить високим. Кібербезпека в даний час є ключовим і стратегічним питанням в економічному, політичному, соціальному та військовому аспектах.

Зауважимо, що ця сфера є публічною, тому темою нашої уваги буде адміністративне регулювання кіберпростору в контексті ведення військових дій.

Враховуючи законодавчі визначення цього поняття, Є.А. Рижкова формулює власне трактування адміністративно-правового регулювання кібербезпеки. За її твердженням, це стан захищеності життєво важливих інтересів особи, суспільства і держави, за якого унеможливлюється заподіяння шкоди шляхом негативного інформаційного впливу шляхом несанкціонованого створення, використання інформації з певною метою; неповна, несвоєчасна, недостовірна та необ'єктивна інформація; негативний вплив кібертехнологій; несанкціоноване порушення режимів доступу до інформації з подальшим її розповсюдженням та використанням [2, с. 5].

А. Тарасюк наголошує, що адміністративно-правове регулювання кібербезпеки гарантує інформаційну безпеку, що слід трактувати як правове поняття. Мається на увазі стан захищеності національних інтересів у кіберпросторі, який визначається сукупністю збалансованих інтересів особи, суспільства та держави [3, с. 171].

В Україні формується власна модель зміцнення стану кібербезпеки в умовах війни, що вимагає, насамперед, прискорення розробки та затвердження відповідних нормативних актів, що відповідають сучасним умовам.

Відповідно до Закону України «Про основні засади кібербезпеки України» кібербезпека – це захист життєво важливих інтересів особистості і громадянина, суспільства і держави при використанні кіберпростору, який забезпечує сталий розвиток інформаційного суспільства та цифрового комунікаційного середовища, своєчасне виявлення, запобігання та нейтралізацію реальних та потенційних загроз до національної безпеки України в кіберпросторі [4].

Суттєвим кроком у розвитку кіберправа є прийняття 12 січня 2023 року Верховною Радою України у першому читанні законопроєкту щодо невідкладних заходів посилення спроможностей із кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури, яким пропонується внести зміни до ряду законів України, що спрямовані на нормативне забезпечення захищеності від кібератак державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури, на створення належної правової основи для здійснення заходів з попередження, виявлення та припинення актів агресії у кіберпросторі в умовах війни російської федерації проти України, а також на загальне удосконалення нормативно-правової бази у сфері кібербезпеки та захисту інформації задля посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам.

На початку квітня 2023 року Кабінет Міністрів України видав постанову, яка визначає процедуру реагування на кіберінциденти

та кібератаки. Нова постанова Уряду України дозволить вчасно реагувати та планувати заходи з кіберзахисту. Мова йде про Постанову Кабінету Міністрів України від 04.04.23 р. № 299 «Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі» [5]. Цією постановою затверджено Порядок реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі. Нормативно встановлено, що реагування на кіберінциденти/кібератаки здійснюється суб'єктами забезпечення кібербезпеки шляхом вжиття заходів до кіберзахисту, спрямованих на швидке виявлення та захист від кіберінцидентів/кібератак, належне інформування про них, запобігання негативним наслідкам, їх мінімізації та усунення, виправлення вразливостей, а також відновлення сталості і надійності функціонування інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем та інших об'єктів кіберзахисту.

Алгоритм реагування суб'єктами забезпечення кібербезпеки на кіберінциденти/ кібератаки розпочинається з етапу підготовки, під час якого здійснюються заходи з дослідження сучасних видів кіберінцидентів/кібератак, розроблення методів і механізмів запобігання та протидії можливим кіберінцидентам/кібератакам. На етапі виявлення та аналізу суб'єкти забезпечення кібербезпеки здійснюють виявлення кіберінциденту/ кібератаки та визначають їх критичність для забезпечення пропорційності та/або співрозмірності подальших заходів з кіберзахисту реальним та потенційним ризикам.

Окрім зазначеної постанови у 2022 році була ухвалена низка важливих законів та підзаконних актів, зокрема законодавчі зміни стосуються активної протидії агресії у кіберпросторі [6], Хмарних послуг та розміщення у «хмарах» державних інформаційних ресурсів [7], посилення захисту критичної інфраструктури України [8], регламентований механізм забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану [9] тощо.

До того ж в Україні діє Стратегія забезпечення кібербезпеки, яка набула чинності рішенням РНБО України від 14 травня 2021 року [10]. Стратегія кібербезпеки України розрахована до 2025 року як основоположний документ загальнодержавного значення, що регулює вектор подальших кроків розвитку національної системи кібербезпеки нашої держави, системні заходи щодо надійного захисту національного сегменту простору кібербезпеки, зовнішньополітичну діяльність у сфері посилення кібербезпеки тощо. Загалом Стратегія кібербезпеки України складається з дев'яти взаємопов'язаних розділів і детально визначає пріоритети, цілі та завдання забезпечення кібербезпеки України з метою створення передумов для побудови безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

Стратегія кібербезпеки України враховує попередній досвід і проблеми, поточний і майбутній стан середовища кібербезпеки на національному та міжнародному рівнях, а також положення Стратегії кібербезпеки ЄС на цифрове десятиліття, стратегії безпеки окремих держав-членів ЄС і країн-членів НАТО. Стратегія кібербезпеки України визначає пріоритети національних інтересів у сфері кібербезпеки, існуючі та потенційно можливі кіберзагрози, цілі та завдання щодо забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтереси особи, суспільства і держави. Цією Стратегією визначено, що забезпечення кібербезпеки є одним із пріоритетів системи національної безпеки України. Реалізація зазначеного пріоритету здійснюватиметься шляхом зміцнення спроможностей національної системи кібербезпеки щодо протидії кіберзагрозам у сучасному безпековому середовищі.

У положеннях Стратегії наголошується, що саме кіберпростір разом з іншими фізичними просторами визнано одним з можливих театрів воєнних дій. Окреслено тенденцію зі створення власних кібервійськ, до завдань яких належить не лише забезпечення захисту критичної інформаційної інфраструктури від кібератак, а й проведення превентивних наступальних операцій у кіберпросторі. Враховуючи масштаби військової агресії проти України, вважаємо, що деякі положення зазначеної Стратегії потребують уточнення, оскільки не в повній мірі відображають поточну реальну ситуацію у сфері кібербезпеки.

Зокрема, важливим завданням держави в умовах воєнного стану залишається створення та оптимізація ефективної національної системи кібербезпеки з урахуванням тенденцій динаміки змін безпекового середовища та кращих практик у сфері кібербезпеки. провідних країн світу; набуття суб'єктами

кібербезпеки необхідних можливостей для виконання поставлених оперативних завдань у кібердомені; створення передумов для опанування сучасних форм та способів підготовки та проведення заходів забезпечення кібербезпеки; нарощування потужностей щодо підготовки та ведення кібербезпеки (у т. ч. кіберзахисту, кібероборони) відповідно до зростання рівня кіберзагроз; вчасне реагування на поточні загрози кібербезпеки шляхом запобігання, завчасного виявлення, випереджувального реагування на них, усунення (мінімізації, ліквідації наслідків) їх впливу; створення ефективних систем управління для забезпечення кібербезпеки; налагодження ефективної співпраці у межах повноважень із суб'єктами забезпечення національної безпеки держави, а також з НАТО, ЄС, державами-партнерами в частині спільного виконання завдань кібербезпеки.

Висновки. Отже, під час війни проблема забезпечення інформаційної безпеки стає питанням національної безпеки, як кожного громадянина, так і суспільства в цілому, що робить її стратегічною проблемою держави, яка потребує комплексної підтримки кібербезпеки та інформаційного суверенітету, налагодити стратегічну комунікацію суб'єктів національної системи кібербезпеки, підвищити можливості протидії кіберзагрозам, сформувати відповідну інфраструктуру інформаційного простору України.

Законодавець зобов'язаний здійснювати політику передбачення та негайного реагування на динамічні зміни, що відбуваються в кіберпросторі, розробляти та впроваджувати ефективні засоби та інструменти можливої відповіді на агресію в кіберпросторі, які можуть бути використані як засіб стримування конфліктів військового характеру та загроз в кіберпросторі. В умовах глобалізації кіберзагроз доцільно уніфікувати підходи до адміністративно-правового регулювання у сфері кібербезпеки та стандартизувати заходи безпеки для ефективної взаємодії та координації зусиль на національному та міжнародному рівнях.

Прагнення України до євроінтеграції вимагає вдосконалення національного законодавства у сфері кібербезпеки з урахуванням умов Угоди про асоціацію між Україною, з одного боку, та ЄС та його державами-членами, з іншого. Слід зазначити, що проблему ефективної кібербезпеки можна буде вирішити лише скоординованими діями на національному, регіональному та міжнародному рівнях, тому, на нашу думку, беззаперечним фактом є те, що чинне законодавство має відповідати вимогам сучасного рівня розвитку технологій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1.Казанчук І. та Яценко В. Особливості правового регулювання діяльності Національної поліції України у сфері забезпечення інформаційної безпеки в Україні. Закон і безпека. 2020. № 79 (4). С. 32–38

2.Рижкова Є. Актуальні проблеми правового регулювання цифрової революції. Юридичні дослідження. 2021. № 8. С. 1–10

3.Тарасюк А. Актуальні проблеми забезпечення кібербезпеки на глобальному та національному рівнях. Visegrad Journal on Human Rights. 2020. № 1, С. 167–172

4.Закон України «Про основні засади кібербезпеки України» від 5 жовтня 2017 року. URL: https://zakon.rada.gov.ua/laws/show/2163-19

5.Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі: Постанова Кабінету Міністрів України від 04.04.23 р. № 299. URL: https://zakon.rada.gov.ua/laws/show/299-2023-п#Text

6.Про внесення змін до Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» щодо забезпечення формування та реалізації державної політики у сфері активної протидії агресії у кіберпросторі: Закон України від 28.07.22 р. № 2470. URL: https://zakon.rada.gov.ua/laws/show/2470-20#Text

7.Про хмарні послуги: Закон України від 17.02.22 р. № 2075. URL: https://zakon.rada.gov.ua/laws/show/2075-20#Text

8.Про внесення змін до деяких законів України щодо повноважень уповноваженого органу у сфері захисту критичної інфраструктури України: Закон України від 18.10.22 р. № 2684. URL: https://zakon.rada.gov.ua/laws/show/2684-20#Text

9.Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану: Постанова Кабінету Міністрів України від 12.03.22 р. № 263. URL: https://www.kmu.gov.ua/npas/deyaki-pitannya-zabezpechennya-funkcionuvannya-informacijno-komunikacijnih-sistem-elektronn ih-komunikacijnih-sistem-publichnih-elektronnih-reyestriv-v-umovah-voyennogo-stanu-263

10. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 р. «Про Стратегію кібербезпеки України»: Указ Президента України від 26.08.21 р. № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013

Стаття надійшла до редакції 22.01.2024
Стаття рекомендована до друку 27.03.2024

V. V. HORULKO
PhD student, Faculty of Law
E-mail: vl.gorulko@karazin.ua ORCID::https://orcid.org/0000-0001-5921-6066
V. N. Karazin Kharkiv National University
Kharkiv, 61022, Svobody square, 4

THE SIGNIFICANCE OF LEGAL REGULATION IN ENSURING CYBER SECURITY IN THE CONDITIONS OF WAR: EXPERIENCE FOR UKRAINE

ANNOTATION. *Introduction.* In the vast majority of countries, there is a constant trend towards a significant increase in the number and expansion of the spectrum of cyber-attacks with the aim of violating the confidentiality, integrity and availability of state information resources, in particular those distributed on the Internet and objects of critical information infrastructure.

Summary of main results. The large-scale deployment of a hybrid war against our state seriously affects all aspects of social life. To a large extent, the strategic success of countering the challenges of hybrid warfare depends on the effective and quality of the legal response. Ensuring an adequate level of cyber security is difficult to imagine without clearly planned joint actions and measures developed by responsible entities, which must be synchronized and implemented according to a single strategic plan and development vector of the national cyber security system of a declarative nature. That is why cyber security in most countries of the world is recognized as an important component of national security, the provision of which is impossible without the formation and functioning of a national system in the field of cyber security, which is based on such principles as respect for the principles and norms of international law, protection of fundamental values defined by current legislation, protection national interests in cyberspace. It is emphasized that the state's national security largely depends on the state of cyber security. It has been proven that hybrid war significantly increases the impact of cyber threats on Ukrainian society and actualizes the danger of targeted cyber attacks as a tool of aggression against our state in the context of global trends regarding threats in cyberspace.

Conclusions. In the process of conducting the research, we formulated conclusions in which special attention was paid to the peculiarities of the current state of functioning of the legislation on cyber security and considered promising directions for its improvement in the future, which, in turn, will become the basis for improving the administrative and legal regulation of cyber security in Ukraine.

KEY WORDS: *national security, information security, cyber security, cyberspace, martial law, legal regulation.*

REFERENCES:

1.Kazanchuk I., Yatsenko V. Peculiarities of legal regulation of the National Police of Ukraine in the field of ensuring information security in Ukraine. Law and security. 2020. No. 79 (4). P. 32–38 (in Ukrainian).

2.E. Ryzhkova. Actual problems of legal regulation of the digital revolution. Legal studies. 2021. No. 8. P. 1–10 (in Ukrainian).

3.Tarasyuk A. Actual problems of ensuring cyber security at the global and national levels. Visegrad Journal on Human Rights. 2020. No. 1, pp. 167–172 (in Ukrainian).

4.Law of Ukraine "On the Basic Principles of Cyber Security of Ukraine" dated October 5, 2017. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (in Ukrainian).

5.Some issues of response by cyber security entities to various types of events in cyberspace: Decree of the Cabinet of Ministers of Ukraine dated 04.04.23 No. 299. URL: https://zakon.rada.gov.ua/laws/show/299- 2023-п#Text (in Ukrainian).

6.On the introduction of amendments to the Law of Ukraine "On the State Service of Special Communications and Information Protection of Ukraine" to ensure the formation and implementation of state policy in the field of active countermeasures against aggression in cyberspace: Law of Ukraine dated 07/28/22 No. 2470. URL: https ://zakon.rada.gov.ua/laws/show/2470-20#Text (in Ukrainian).

7.About useless services: Law of Ukraine dated 02.17.22 No. 2075. URL: https://zakon.rada.gov.ua/laws/show/2075-20#Text (in Ukrainian).

8.On amendments to some laws of Ukraine regarding the powers of the authorized body in the field of protection of critical infrastructure of Ukraine: Law of Ukraine dated 18.10.22 No. 2684. URL: https://zakon.rada.gov.ua/laws/show/2684 -20#Text (in Ukrainian).

9.Some issues of ensuring the functioning of information and communication systems, electronic communication systems, and public electronic registers under martial law: Resolution of the Cabinet of Ministers of

Ukraine dated 03/12/22 No. 263. URL: https://www.kmu.gov.ua/ npas/deyaki-pitannya-zabezpechennya-funkonuvannya-informacijno-komunikacijnih-sistem-elektronn ih-komunikacijnih-sistem-publichnih-elektronnih-reyestriv-v-umovah-voyennogo-stanu-263 (in Ukrainian).

10.On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine": Decree of the President of Ukraine dated August 26, 2021 No. 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013 (in Ukrainian).

The article was received by the editors 22.01.2024
The article is recommended for printing 27.03.2024