

ЛИСЕЮК АНДРІЙ МИКОЛАЙОВИЧ

кандидат юридичних наук, доцент, професор кафедри фінансово-економічної безпеки Навчально-наукового гуманітарного інституту Національної академії Служби безпеки України
ORCID 0000-0002-9026-1188

СВІНЦИЦЬКА ТЕТЯНА ВОЛОДИМИРІВНА

здобувач вищої освіти Навчально-наукового інституту права Державного податкового університету

УДК 340+342.9

DOI 10.37772/2518-1718-2024-4(48)-4

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ ТА ЄВРОІНТЕГРАЦІЇ

Стаття присвячена розгляду питань правового забезпечення кібербезпеки України в умовах правового режиму воєнного стану та необхідності продовження євроінтеграції. У процесі наукового дослідження визначено, що захист кіберпростору виступає стратегічно важливим пріоритетом у системі національної безпеки України. Наголошено, що Україна під час широкомасштабного вторгнення росії зустрічається з кібератаками та кіберзлочинами з боку держави-агресора. Підкреслено, що в умовах тривання воєнних дій на території України питання захисту національних інтересів та критичної інформаційної інфраструктури набувають особливо гострої актуальності. Зазначено, що для відвернення кіберзагроз та захисту території й інформаційного простору держави наразі потрібна концентрація всіх видів ресурсів та впорядкування повноважень відповідних суб'єктів забезпечення кібербезпеки у поєднанні з ефективною державною політикою та відповідним нормативно-правовим забезпеченням зазначеної сфери. Розглянуті положення чинних нормативно-правових актів та документів стратегічного планування в сфері кібербезпеки. Так, проаналізовані окремі норми Закону України «Про основні засади забезпечення кібербезпеки України», положення Стратегії національної безпеки України та Стратегії кібербезпеки України. Встановлено, що важливими завданнями також постають поглиблення співпраці з міжнародними партнерами у сфері кібербезпеки, запровадження нових ініціатив щодо зміцнення кіберзахисту, а також співпраця в сфері протидії та попередження кіберактивності злочинців. Зроблені висновки, що для забезпечення захисту кіберпростору в Україні необхідно вдосконалювати нормативно-правову базу у сфері кібербезпеки, впроваджувати заходи щодо поглиблення євроінтеграційних процесів шляхом забезпечення ефективної імплементації положень європейського законодавства.

Ключові слова: воєнний стан, євроінтеграція, кібербезпека, кіберзахист, кіберпростір, правове регулювання.

Постановка проблеми. Питання нормативно-правового регулювання сфери кібербезпеки зберігають значну актуальність в умовах правового режиму воєнного стану та необхідності поглиблення євроінтеграційних процесів. Україна під час широкомасштабної агресії зустрічається з різними видами кібератак та кіберзлочинів, країна-агресор прагне заблокувати надання електронних послуг наслідком чого є непоодинокі випадки порушення прав громадян, порушуються цілісність та конфіденційність персональних відомостей, здійснюються фішингові атаки, провокується інформаційно-психологічний натиск на людей [1]. Тож, захист кіберпростору в умовах зазначених викликів ви-

ступає стратегічно важливим пріоритетом у системі національної безпеки України.

Метою статті є розгляд особливостей та проблематики правового регулювання кібербезпеки України в сучасних умовах.

Аналіз останніх досліджень і публікацій. Дослідженню питань забезпечення кібербезпеки присвячено чимало наукових праць вчених з різних наукових сфер.

Вчені В. Ліпкан та І. Діордіца досліджували національну систему кібербезпеки як складову частину системи забезпечення національної безпеки України та акцентували увагу на тому, що одним із ключових питань організації ефективної роботи національних

систем кібербезпеки залишається налагодження взаємодії між компетентними державними органами, які є суб'єктами кібернетичної безпеки, та здійснення координації з такої діяльності [2].

Ю. О. Загуменна розглядала актуальні питання кібербезпеки в контексті сучасних проблем правознавства та визначила шляхи вдосконалення правового регулювання боротьби з кіберзлочинністю в Україні, в тому числі виявила тенденції щодо універсалізації підходів законодавців різних країн у напрямі боротьби з кіберзлочинністю [3].

Науковці У. М. Ніконенко та О. В. Халіна досліджували організаційно-правовий механізм, який регламентує організацію процесу забезпечення кібербезпеки соціально-економічних систем в правовому полі та зазначили, що метою функціонування організаційно-правового механізму забезпечення кібербезпеки є організація процесу захисту кіберпростору через використання нормативно-правової бази як регулюючого інструменту та ефективне управління ресурсами суб'єкта господарювання [4].

О. А. Алексеєва висвітлювала питання правового забезпечення кібербезпеки об'єктів критичної інфраструктури, в тому числі розглядала понятійний апарат у сфері забезпечення кібербезпеки об'єктів критичної інфраструктури, її наукова праця містить аналіз чинного законодавства України у сфері забезпечення кібербезпеки та відповідного зарубіжного досвіду [5]. М. Tvaronavičienė, T. Plėta, S. D. Casa запропонували модель управління кібербезпекою критичної інфраструктури та дійшли висновку щодо необхідності впровадження комплексної моделі, яку можливо застосувати до будь-якого типу критичної інфраструктури [6]. T. Limba, T. Plėta, K. Agafonov, M. Damkus розглядали теоретичні аспекти моделі управління кібербезпекою, які можна використовувати для забезпечення безпеки критичної інфраструктури в організації або компанії та висловили думку, що головна проблема полягає в тому, що кібербезпека зазвичай розглядається як технічний аспект або технологія, яку можна легко реалізувати всередині організації, і це впровадження гарантуватиме кібербезпеку, втім таке ставлення має змінитися, тому що кібербезпека сьогодні це щось більше, ніж просто технологія [7].

Отже, як вбачається, тематика щодо проблем забезпечення кібербезпеки є актуальною та активно досліджуваною, втім окремі її аспекти не мають наукового розкриття та потребують додаткових наукових опрацювань.

Виклад основного матеріалу. Підкреслимо, що в умовах тривання воєнних дій на території України внаслідок широкомасштабного вторгнення росії питання захисту національних інтересів та критичної інформаційної інфраструктури набувають особливо

гострої актуальності. Тож, для відвернення кіберзагроз та захисту території й інформаційного простору держави наразі потрібна концентрація всіх видів ресурсів та впорядкування повноважень відповідних суб'єктів забезпечення кібербезпеки у поєднанні з дієвою державною політикою та ефективним нормативно-правовим забезпеченням зазначеної сфери.

Закон України «Про основні засади забезпечення кібербезпеки України» [8] встановлює поняття кібербезпеки як захищеності життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. Також норми статті 4 зазначеного закону визначають наступні об'єкти: 1) об'єкти кібербезпеки, якими є: конституційні права і свободи людини і громадянина; суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища; держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність; національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави; об'єкти критичної інфраструктури; 2) об'єкти кіберзахисту, а саме: комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону; об'єкти критичної інформаційної інфраструктури; комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу [8]. Перелічені об'єкти безпосередньо пов'язані з важливими інтересами людини і громадянина, суспільства, держави та національними інтересами України у кіберпросторі.

Слід погодитися, що формування та реалізація державної політики у сфері кібербезпеки, захист прав і свобод людини та громадянина, національних інтересів України у кіберпросторі, боротьба з кіберзлочинністю забезпечується Кабінетом Міністрів України, Уряд України також організовує та забезпечує необхідними силами, засобами і ресурсами функціонування національної системи кібербезпеки; формує вимоги та забезпечує функціонування системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури (крім об'єктів критичної інфраструктури у банківській системі України) [9, с. 120].

Отже, забезпечення кібербезпеки є пріоритетним завданням державної політики, водночас важливу

роль відіграє стратегічне планування в зазначеній сфері.

Так, Стратегія національної безпеки України [10], яка затверджена Указом Президента України від 14 вересня 2020 року № 392/2020, встановлює, що реалізація пріоритетів національних інтересів України та забезпечення національної безпеки забезпечуватиметься зокрема за напрямом посилення спроможностей національної системи кібербезпеки для ефективної протидії кіберзагрозам у сучасному безпековому середовищі. Також Стратегія національної безпеки України визначає основним завданням розвитку системи кібербезпеки – гарантування кіберстійкості та кібербезпеки національної інформаційної інфраструктури, зокрема в умовах цифрової трансформації та для системного захисту України від загроз національній безпеці необхідним вбачається розвиток сектору безпеки і оборони, для цього Україна: завершить створення національної системи кібербезпеки, сформує сучасні спроможності суб'єктів забезпечення кібербезпеки і кібероборони та зміцнить систему їх координації.

Доцільно зауважити, що Стратегія національної безпеки України є основою для розроблення документів щодо планування у сферах національної безпеки і оборони (в тому числі Стратегії кібербезпеки), які визначатимуть шляхи та інструменти її реалізації.

Стратегія кібербезпеки України, яка затверджена Указом Президента України від 26 серпня 2021 року № 447/2021 [11] серед передумов та чинників, які формують загрози кібербезпеці України визначає недосконалість нормативно-правової бази у сфері кібербезпеки, її застарілість у сфері захисту інформації, повільну імплементацію положень європейського законодавства, недостатню врегульованість цифрової складової розслідування кримінальних правопорушень, а також низький рівень правової відповідальності за порушення вимог законодавства у цій сфері.

Водночас зазначена Стратегія регламентує наступні пріоритети забезпечення кібербезпеки України:

- 1) убезпечення кіберпростору задля захисту суверенітету держави та розвитку суспільства;
- 2) захист прав, свобод і законних інтересів громадян України у кіберпросторі;
- 3) європейська і євроатлантична інтеграція у сфері кібербезпеки.

Щодо формування стратегічних цілей Стратегія кібербезпеки України визначає наступні положення:

- 1) для формування потенціалу стримування (С) необхідним є досягнення таких стратегічних цілей: ціль С.1. «Дієва кібероборона»; ціль С.2. «Ефективна протидія розвідувально-підривній діяльності у кіберпросторі та кібертероризму»; ціль С.3. «Ефектив-

на протидія кіберзлочинності»; ціль С.4. «Розвиток асиметричних інструментів стримування»;

для набуття кіберстійкості (К) необхідним є досягнення таких стратегічних цілей: ціль К.1. «Національна кіберготовність та надійний кіберзахист»; ціль К.2. «Професійне вдосконалення, кіберобізнане суспільство та науково-технічне забезпечення кібербезпеки»; ціль К.3. «Безпечні цифрові послуги»;

3) для вдосконалення взаємодії (В) необхідним є досягнення таких стратегічних цілей: ціль В.1. «Зміцнення системи координації»; ціль В.2. «Формування нової моделі відносин у сфері кібербезпеки»; ціль В.3. «Прагматичне міжнародне співробітництво».

Так, для досягнення стратегічної цілі В.3 «Прагматичне міжнародне співробітництво» Україна розвиватиме міжнародне співробітництво у сфері кібербезпеки, спрямоване, передусім, на забезпечення незалежності і державного суверенітету, відновлення територіальної цілісності України, шляхом: продовження співробітництва з Агентством Європейського Союзу з питань мережевої та інформаційної безпеки, зокрема з питань скоординованого розкриття вразливостей та імплементації Директиви Європейського Парламенту і Ради (ЄС) 2016/1148 від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу [12] як елементу євроінтеграції України. У цьому контексті слід зауважити, що вищевказана Директива в своїх положеннях підкреслює важливість міжнародної співпраці з питань кібербезпеки.

Також в Стратегії кібербезпеки України заявлено, що Україна у сфері кібербезпеки забезпечить поглиблення євроінтеграційних процесів шляхом уніфікації підходів, методів і засобів забезпечення кібербезпеки з усталеними практиками ЄС і НАТО, вжиття інших узгоджених із ключовими іноземними партнерами заходів, спрямованих на посилення кіберстійкості України, розвиток спроможностей національної системи кібербезпеки та захист національних інтересів у кіберпросторі.

Отже важливими питаннями постають поглиблення співпраці з міжнародними партнерами у сфері кібербезпеки, запровадження нових ініціатив щодо зміцнення кіберзахисту, а також співпраця в сфері протидії та попередження кіберактивності злочинців. Так, доречно зазначити, що 9 жовтня 2024 року Україна та Республіка Хорватія уклали Угоду про довгострокове співробітництво та підтримку між Україною та Республікою Хорватія [13], яка регламентує, що учасники вивчатимуть можливості зміцнення двосторонньої співпраці у сфері цифрової стійкості та кібербезпеки з метою допомоги Україні у виявленні та протидії зловмисній кіберактивності з боку

росії та будь-яких інших державних і недержавних суб'єктів відповідно до міжнародного права. Відповідно до положень зазначеної Угоди про довгострокове співробітництво Україна та Хорватія обмінюватимуться розвідувальними даними, практиками та набутим досвідом з метою розвитку своїх спроможностей у сфері кібербезпеки й кіберзахисту, а також для підвищення кіберстійкості України та захисту її критичної інфраструктури, зокрема шляхом обміну технічною допомогою.

Співпраця України з міжнародними партнерами, підписання нових домовленостей та угод, що регулюють питання кібербезпеки, зобов'язують нашу країну виконувати їхні норми та стандарти, що стане кроком, який сприятиме виходу України на рівень світових держав з високими показниками кібербезпеки, тому важливо, щоб національне законодавство відповідало міжнародним стандартам, адже зусилля міжнародних партнерів, в наданні додаткової фінансової підтримки для зміцнення кібербезпеки України є важливим кроком у напрямі боротьби із загрозою кібератак та підтримки країни в розвитку її оборонної спроможності [14].

Висновки. Враховуючі стан врегулювання сфери кібербезпеки та вплив відповідних внутрішніх та зовнішніх чинників, доцільно визначити, що наразі

основним завданням державної політики постає посилення спроможностей національної системи кібербезпеки з метою ефективної протидії кіберзагрозам з боку країни-агресора. Для того, щоб гарантувати убезпечення кіберпростору та належний рівень захисту прав, свобод і законних інтересів громадян України у кіберпросторі необхідно вдосконалювати нормативно-правову базу у сфері кібербезпеки, впроваджувати заходи щодо поглиблення євроінтеграційних процесів шляхом забезпечення ефективної імплементації положень європейського законодавства. До того ж важливим є посилення співпраці з міжнародними партнерами у сфері кібербезпеки, запровадження нових ініціатив щодо зміцнення кіберзахисту та попередження кіберактивності злочинців. Тож, проблема ефективного забезпечення кібербезпеки потребує комплексного вирішення і вимагає скоординованих дій на національному, регіональному та міжнародному рівнях для запобігання, підготовки, реагування та відновлення інцидентів з боку органів влади, приватного сектора і громадянського суспільства [15].

Отже, розв'язання наведених проблем щодо належного правового забезпечення кібербезпеки України в умовах воєнного стану та євроінтеграції потребує подальших науково-правових напрацювань.

ЛІТЕРАТУРА

1. Колосовський Є. Ю., Круць Е. М. Сучасний стан кібербезпеки України в умовах воєнного періоду. *Юридичний науковий електронний журнал*. 2023. № 12. С. 402–405.
2. Ліпкан В., Діордіца І. Національна система кібербезпеки як складова частина системи забезпечення національної безпеки України. *Підприємництво, господарство і право*. 2017. № 5. С. 174–180. URL: <http://pgp-journal.kiev.ua/archive/2017/5/40.pdf>.
3. Загуменна Ю. О. Актуальні питання кібербезпеки в контексті сучасних проблем правознавства. *Право.ua*. 2021. № 1. С. 70–82. URL: <https://dspace.univd.edu.ua/server/api/core/bitstreams/b45ebfd0-fd90-48ec-ac3e-1ce5ebb949fd/content>.
4. Ніконенко У., Халіна О. Організаційно-правовий механізм забезпечення кібербезпеки соціально-економічних систем в умовах викликів сучасності. 2024. *Економічний простір*. № 190. С. 108–113. DOI: <https://doi.org/10.32782/2224-6282/190-20>.
5. Алексеева О. А. Правове забезпечення кібербезпеки об'єктів критичної інфраструктури. *Інформація і право*. 2023. №4(47). С. 168–176. DOI: [https://doi.org/10.37750/2616-6798.2023.4\(47\).291633](https://doi.org/10.37750/2616-6798.2023.4(47).291633).
6. Cyber security management model for critical infrastructure protection. Contemporary Issues in Business, Management and Education. International Scientific Conference. Vilnius, Lithuania. Vilnius Gediminas Technical University. (13–14 May 2021). DOI: <https://doi.org/10.3846/cibmee.2021.611>.
7. Limba T., Plėta T., Agafonov, K., Damkus M. Cyber security management model for critical infrastructure, *Entrepreneurship and Sustainability*. 2017. Issues 4(4): P. 559–573. DOI: [https://doi.org/10.9770/jesi.2017.4.4\(12\)](https://doi.org/10.9770/jesi.2017.4.4(12)).
8. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII (в редакції від 28.06.2024). URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>.
9. Тарасюк А. В. Система суб'єктів забезпечення кібербезпеки в Україні. *Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки*. 2020. № 2. С. 119–124. DOI: <https://doi.org/10.32838/2707-0581/2020.2-2/23>.
10. Стратегія національної безпеки України. Безпека людини - безпека країни: затв. Указом Президента України від 14 вересня 2020 року № 392/2020. URL: <https://zakon.rada.gov.ua/laws/show/392/2020#Text>.
11. Стратегія кібербезпеки України «Безпечний кіберпростір - запорука успішного розвитку країни»: затв. Указом Президента України від 26 серпня 2021 року № 447/2021. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#n12>.

12. Директива Європейського Парламенту і Ради (ЄС) 2016/1148 від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу: Міжнародний документ від 06.07.2016 № 2016/1148. URL: https://zakon.rada.gov.ua/laws/show/984_013-16#Text.
13. Офіс Президента. Офіційний сайт. <https://www.president.gov.ua/news/ugoda-pro-dovgostrokove-spivrobotnictvo-ta-pidtrimku-mizh-uk-93733>.
14. Сироватченко М. Правові аспекти забезпечення кібербезпеки в Україні: сучасні виклики та роль національного законодавства. *Вісник Національного університету «Львівська політехніка». Серія: «Юридичні науки»*. 2024. №1 (41). С. 314–320. <https://doi.org/10.23939/law2024.41.314>.
15. Трофименко О., Прокоп Ю., Логінова Н., Задерейко О. Кібербезпека України: аналіз сучасного стану. *Захист інформації*. Том 21 № 3. DOI: 10.18372/24107840/21/13951. С. 150–157.

REFERENCES

1. Kolosovskiy, Ye. Yu., & Kruts, E. M. (2023). The current state of cyber security in Ukraine during the wartime period. *Yurydychnyi Naukovyi Elektronnyi Zhurnal*, 12, 402–405. [in Ukrainian].
2. Lipkan, V., & Diordytza, I. (2017). National cyber security system as part of the national security system of Ukraine. *Pidpriemnytstvo, Hospodarstvo i Pravo*, 5, 174–180. Retrieved from <http://pgp-journal.kiev.ua/archive/2017/5/40.pdf> [in Ukrainian].
3. Zahumenna, Yu. O. (2021). Current issues of cyber security in the context of modern legal problems. *Pravo.ua*, 1, 70–82. Retrieved from <https://dspace.univd.edu.ua/server/api/core/bitstreams/b45ebfd0-fd90-48ec-ac3e-1ce5e-bb949fd/content> [in Ukrainian].
4. Nikonenko, U., & Khalina, O. (2024). Organizational and legal mechanisms for ensuring cyber security of socio-economic systems in modern challenges. *Ekonomichnyi Prostir*, 190, 108–113. <https://doi.org/10.32782/2224-6282/190-20> [in Ukrainian].
5. Alekseeva, O. A. (2023). Legal support for cyber security of critical infrastructure objects. *Information and Law*, 4(47), 168–176. [https://doi.org/10.37750/2616-6798.2023.4\(47\).291633](https://doi.org/10.37750/2616-6798.2023.4(47).291633). [in Ukrainian].
6. Cyber security management model for critical infrastructure protection. (2021, May 13–14). In *Contemporary Issues in Business, Management and Education. International Scientific Conference*. Vilnius, Lithuania: Vilnius Gediminas Technical University <https://doi.org/10.3846/cibmee.2021.611>.
7. Limba, T., Plêta, T., Agafonov, K., & Damkus, M. (2017). Cyber security management model for critical infrastructure. *Entrepreneurship and Sustainability*, 4(4), 559–573. [https://doi.org/10.9770/jesi.2017.4.4\(12\)](https://doi.org/10.9770/jesi.2017.4.4(12)).
8. Law of Ukraine On the basic principles of ensuring cyber security in Ukraine, No. 2163-VIII (2017, October 5) (as amended on 2024, June 28). Retrieved from <https://zakon.rada.gov.ua/laws/show/2163-19#Text> [in Ukrainian].
9. Tarasiuk, A. V. (2020). System of subjects ensuring cyber security in Ukraine. *Scientific Notes of TNU Named After V. I. Vernadskyi. Series: Legal Sciences*, 2, 119–124. <https://doi.org/10.32838/2707-0581/2020.2-2/23> [in Ukrainian].
10. National Security Strategy of Ukraine. Human Security – Country Security: Approved by the Decree of the President of Ukraine, No. 392/2020 (2020, September 14). Retrieved from <https://zakon.rada.gov.ua/laws/show/392/2020#Text> [in Ukrainian].
11. Cyber Security Strategy of Ukraine «Safe Cyberspace – a Guarantee of the Country’s Successful Development»: Approved by the Decree of the President of Ukraine, No. 447/2021 (2021, August 26). Retrieved from <https://zakon.rada.gov.ua/laws/show/447/2021#n12> [in Ukrainian].
12. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Retrieved from https://zakon.rada.gov.ua/laws/show/984_013-16#Text.
13. Office of the President of Ukraine. Official website. Retrieved from <https://www.president.gov.ua/news/ugoda-pro-dovgostrokove-spivrobotnictvo-ta-pidtrimku-mizh-uk-93733> [in Ukrainian].
14. Syrovatchenko, M. (2024). Legal aspects of ensuring cyber security in Ukraine: Modern challenges and the role of national legislation. *Visnyk of the National University «Lvivska Politechnika». Series: Legal Sciences*, 1(41), 314–320. <https://doi.org/10.23939/law2024.41.314>. [in Ukrainian].
15. Trofymenko, O., Prokop, Yu., Lohinova, N., & Zadereiko, O. (2021). Cyber security in Ukraine: Analysis of the current state. *Information Protection*, 21(3), 150–157. <https://doi.org/10.18372/24107840/21/13951> [in Ukrainian].

LYSEIUK ANDRII

Phd in Law, Associate Professor of the National Academy of the Security Service of Ukraine

SVINTSYTSKA TETYANA

graduate of the Educational and Scientific Institute of Law of the State Tax University

LEGAL PROVIDING OF CYBER SECURITY UKRAINE UNDER THE CONDITIONS OF MARTIAL STATE AND EUROPEAN INTEGRATION

Problem setting. The issues of proper normative and legal regulation of the cybersecurity sphere are becoming especially relevant under conditions of the legal regime of martial law and the continuation of the European integration processes. During the large-scale aggression, Ukraine faces various types of cyber-attacks and cybercrimes. The protection of cyberspace in the context of these global challenges is a strategically important priority of state policy.

Analysis of recent researches and publications. Many scientific works by scientists from various scientific fields are dedicated to the study of issues of cybersecurity.

V. Lipkan and I. Diorditsa studied the national cybersecurity system as an integral part of the national security system of Ukraine and emphasized that one of the key issues of organizing the effective work of national cybersecurity systems remains the establishment of interaction between competent state bodies that are subjects of cyber security, and the implementation of coordination in such activities.

Yu. Zahumenna examined the current issues of cybersecurity in the context of modern problems of jurisprudence and identified ways to improve the legal regulation of combating cybercrime in Ukraine, including identifying trends in the universalization of the approaches adopted by legislators from different countries toward combating cybercrime. Scientists U. Nikonenko and O. Khalina studied the organizational and legal mechanism that regulates the organization of the process of ensuring cybersecurity of socio-economic systems in the legal field and noted that the purpose of the functioning of the organizational and legal mechanism for ensuring cybersecurity is the organization of the process of protecting cyberspace through the use of the regulatory and legal framework as a regulatory tool and effective resource management by business entities. O. A. Alekseeva covered the issue of legal support of cybersecurity for critical infrastructure objects, including considering the conceptual apparatus in the field of cybersecurity of critical infrastructure objects. Her research contains an analysis of the current legislation of Ukraine in the field of cybersecurity provision and relevant foreign experience. M. Tvaronavičienė, T. Plėta, S. D. Casa proposed a model of cybersecurity management for critical infrastructure and concluded that a comprehensive model is needed—one that can be applied to any type of critical infrastructure. T. Limba, T. Plėta, K. Agafonov, M. Damkus considered the theoretical aspects of the cybersecurity management model that can be used to ensure the security of critical infrastructure in an organization or company and argued that the main problem is the perception of cybersecurity as purely a technical aspect or technology that can be easily implemented within an organization. They suggested this attitude must change because cybersecurity today is more than just technology.

Purpose of research is to examine the peculiarities and issues of legal regulation of cybersecurity in Ukraine in the current context.

Article's main body. In the conditions of ongoing hostilities on the territory of Ukraine as a result of the large-scale invasion of Russia, the issues of protecting national interests and critically important information are becoming particularly urgent. Therefore, in order to avert cyber threats and protect the territory and information space of the state, the concentration of all types of resources and the clarification of the powers of the relevant subjects of cybersecurity, in combination with an effective state policy and effective regulatory and legal support for the specified sphere are currently required. Deepening of cooperation with international partners in the field of cyber security, introduction of new initiatives to strengthen cyber protection, as well as cooperation in the field of combating and preventing cyber activity of criminals are also important issues. It is also important that national legislation meets international standards, because the efforts of international partners to provide additional financial support to strengthen Ukraine's cybersecurity are an important step towards combating the threat of cyberattacks and supporting the country in developing its defense capabilities.

Conclusions and prospects for the development. Based on the researched aspects of the chosen topic, taking into account the state of regulation of the cybersecurity sphere and the influence of relevant internal and external factors, it is appropriate to determine that currently the main task of state policy is to strengthen the capabilities of the national cyber security system in order to effectively counter cyber threats from the aggressor country. To guarantee the security of

cyberspace and the proper level of protection of the rights, freedoms, and legitimate interests of Ukrainian citizens in cyberspace, it is also necessary to improve the normative legal framework in the field of cybersecurity, to implement measures to deepen European integration processes by ensuring the effective implementation of the provisions of European legislation. In addition, it is important to strengthen cooperation with international partners in the field of cybersecurity, introduce new initiatives to strengthen cyber protection and prevent cybercriminal activity. The solution to the above problems regarding the proper legal provision of cyber security of Ukraine in the conditions of martial law and European integration requires further scientific research.

Key words: martial law, European integration, cybersecurity, cyber defense, cyberspace, legal regulation.

За ДСТУ 8302:2015 цю статтю слід цитувати:

Лисеюк А. М., Свінцицька Т. В. Правове забезпечення кібербезпеки України в умовах воєнного стану та євроінтеграції. *Право та інновації*. 2024. № 4 (48). С. 32–38.