УДК 340+342.9
DOI 10.37772/2309-9275-2024-2(23)-8
JEL classification: K 39, H 56

РОЗВИТОК МІЖНАРОДНОГО СПІВРОБІТНИЦТВА У СФЕРІ КІБЕРБЕЗПЕКИ: НОРМАТИВНО–ПРАВОВІ ЗАСАДИ ТА ПЕРСПЕКТИВИ

Андрій ЛИСЕЮК, ORCID 0000-0002-9026-1188[1]
Тетяна СВІНЦИЦЬКА[2]

[1]Навчально-науковий гуманітарний інститут Національної академії Служби безпеки України, Київ, Україна;
[2]Навчально-науковий інститут права Державного податкового університету, Київ, Україна

Автор-кореспондент: Свінцицька Тетяна, електронна пошта t0968121645@gmail.com

Анотація. У статті розглянуто окремі аспекти розвитку міжнародного співробітництва у сфері кібербезпеки України. Наголошено на пріоритетності питань захисту кіберпростору, важливості продовження співпраці з іноземними партнерами у сфері кібербезпеки, запровадження нових ініціатив щодо зміцнення кіберзахисту та поглиблення співробітництва з Європейським Союзом і Північноатлантичним альянсом. Проаналізовано норми чинних нормативно-правових актів та документів стратегічного планування у сфері кібербезпеки, зокрема розглянуті окремі положення Закону України «Про основні засади забезпечення кібербезпеки України», Стратегії кібербезпеки України та Стратегії кібербезпеки ЄС на цифрове десятиліття. Встановлено, що головним стратегічним аспектом розвитку міжнародного співробітництва України в галузі кібербезпеки є забезпечення активної участі у діалозі в рамках міжнародних організацій щодо спільного вироблення норм поведінки у кіберпросторі та вдосконалення відповідної нормативно-правової бази. Доведено важливість побудови ефективної національної системи кібербезпеки, поглиблення міжнародного співробітництва в цій сфері, яке повинно мати системний та послідовний характер. Зазначено, що кібербезпека наразі є критичною проблемою, яка потребує підвищеної уваги, в тому числі з боку дослідників. Перспективними напрямами подальшого розвитку міжнародного співробітництва виокремлено: співпрацю з міжнародними партнерами у сфері кібербезпеки шляхом взаємодії та активної участі у нових ініціативах щодо зміцнення кіберзахисту, протидії кіберзагрозам та кібератакам; систематичний обмін дослідженнями та інноваціями, досвідом побудови та ефективного функціонування національних систем кібербезпеки; вдосконалення національного законодавства в сфері кібербезпеки.

Ключові слова: воєнний стан, кібербезпека, кіберзахист, кіберпростір, міжнародне співробітництво, правове регулювання, перспективи розвитку.

Внесок авторів

Автори підготували статтю самостійно. Авторами було самостійно підібрано літературу, проведено її аналіз та сформульовані висновки.

Заява про розкриття інформації

Автори не мають жодних конкуруючих фінансових, професійних чи особистих інтересів щодо інших осіб.

ВСТУП

У сучасних умовах, які характеризуються збільшенням кількості кібератак та кіберінцидентів, що впливають на стан національної безпеки та оборони країни, актуальним завданням

є формування державної політики забезпечення кібербезпеки як засобу посилення безпеки та надійності інформаційних систем, адекватних сучасним викликам і реаліям, спрямованої на своєчасне виявлення, запобігання та нейтралізацію реальних і потенційних кібервтручань і загроз приватним, корпоративним, національним інтересам на основі комплексного підходу та участі усіх суб'єктів (Sozanskyy, T., Krasnytskyi, I, Lutsyk, V, Yaremko, G., Tuz, N., 2020). Тож виклики воєнного стану в Україні зумовили пріоритетність питань забезпечення кібербезпеки, зокрема питань міжнародного співробітництва щодо важливих аспектів захисту кіберпростору. Україна бере активну участь у міжнародних ініціативах щодо зміцнення кіберзахисту отримуючи цінний досвід для подальшого розвитку зазначеної сфери. Тому вкрай важливим є продовження співпраці з іноземними партнерами у сфері кібербезпеки, запровадження нових ініціатив щодо зміцнення кіберзахисту та поглиблення співробітництва з Європейським Союзом (далі – ЄС) та Північноатлантичним альянсом (North Atlantic Treaty Organization). Обрана проблематика набуває особливої актуальності, становить науковий інтерес та потребує здійснення відповідних напрацювань та додаткових досліджень. Метою статті є розгляд питань розвитку міжнародного співробітництва у сфері кібербезпеки України в аспекті перспективізації.

ТЕОРЕТИЧНА ОСНОВА

Питання правового забезпечення кібербезпеки та розвитку міжнародного співробітництва в цій сфері розглядалися багатьма вченими. Серед наукових публікацій останніх років окремо слід виділити праці українських вчених-правників. Так, В. П. Кононенко вивчав проблеми зміцнення кібербезпеки, безпеки інформаційно-комунікаційних технологій, національної та міжнародної інформаційної безпеки (Кононенко, 2023). Тарасюк А. В. в своїх наукових дослідженнях провела аналіз стану забезпечення кібербезпеки в Україні та визначила перспективи його подальшого розвитку (Тарасюк, 2020). Р. Ф. Черниш розглядав питання міжнародного організаційного досвіду у сфері забезпечення кібербезпеки (Черниш, 2024). Наведені та інші праці безумовно становлять значну наукову цінність і мають високий науковий рівень, разом з цим окреслена проблематика потребує постійного наукового аналізу.

МЕТОДОЛОГІЯ

Для досягнення мети наукового дослідження були використані загальні та спеціальні наукові методи пізнання. Так, застосування методів абстрагування й узагальнення, дедуктивного та індуктивного методів, методів аналізу та синтезу, структурно-системного та формально-логічного методів дали змогу в повному обсязі опрацювати необхідні наукові та нормативно-правові джерела та виконати комплексне наукове дослідження визначених питань. При застосуванні вищевказаних наукових методів складові обраної проблематики розглядалися системно, з урахуванням їх взаємозв'язку та взаємовпливу.

РЕЗУЛЬТАТИ

Розвиток міжнародного співробітництва у сфері кібербезпеки та кіберзахисту наразі є критично важливим, потребує реалізації ефективної державної політики та відповідного нормативно-правового забезпечення. Нормативно-правове регулювання вказаної сфери повинно бути адаптованим до реалій воєнного стану та відповідати європейським стандартам згідно з міжнародними зобов'язаннями України щодо імплементації актів права ЄС.

Основним нормативно-правовим актом, який визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі є Закон України «Про основні засади забезпе-

чення кібербезпеки України», який визначає кібербезпеку як захищеність 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. В умовах глобальних викликів зазначені складові відіграють вирішальну роль щодо забезпечення національної безпеки держави, яку намагається підірвати країна-агресор, здійснюючи чисельні кібератаки. Отже, наразі пріоритетними завданнями є забезпечення захисту держави, незалежності та територіальної цілісності України та ефективне функціонування національної системи кібербезпеки, зокрема розвиток міжнародного співробітництва.

ОБГОВОРЕННЯ РЕЗУЛЬТАТІВ

Забезпечення безпеки кіберпростору сьогодні є ключовим викликом для світу, що глобалізується, щоб забезпечити гармонійний, сталий розвиток світової економіки, а також забезпечити мир і безпеку у світі, виникла необхідність визначити нові загрози, пов'язані з кібервійною, кібертероризмом і, нарешті, звичайною комп'ютерною злочинністю, що неможливо без універсальної, тісної співпраці всіх суверенних утворень та їх організацій на міжнародній арені (Milik, 2021). Закон України «Про основні засади забезпечення кібербезпеки України» нормативно закріплює важливість провадження міжнародного співробітництва. Так, норми пункту 9 частини 1 статті 7 встановлюють такий принцип забезпечення кібербезпеки, як міжнародне співробітництво з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в терористичних, воєнних, інших протиправних цілях. Також вказаний Закон у пункті 20 частини третьої статті 8 закріплює, що функціонування національної системи кібербезпеки забезпечується зокрема шляхом розвитку міжнародного співробітництва у сфері кібербезпеки, підтримки міжнародних ініціатив у сфері кібербезпеки, що відповідають національним інтересам України, поглиблення співпраці України з Європейським Союзом та НАТО з метою посилення спроможності України у сфері кібербезпеки, участі у заходах із зміцнення довіри при використанні кіберпростору, що проводяться під егідою Організації з безпеки і співробітництва в Європі. Враховуючи значимість стратегічного планування розвитку сфери кібербезпеки, слід вказати, що Стратегія кібербезпеки України закріплює подальшу розбудову національної системи кібербезпеки на засадах стримування, кіберстійкості, взаємодії, для чого необхідним є: розвиток стратегічних відносин у сфері кібербезпеки із ключовими іноземними партнерами, передусім з Європейським Союзом, Сполученими Штатами Америки та іншими державами - членами НАТО, співробітництво у цій сфері з іншими державами та міжнародними організаціями на основі національних інтересів України (взаємодія). Водночас Стратегія кібербезпеки України фокусує увагу на чинниках, які формують загрози кібербезпеці України, серед яких недосконаліть нормативно-правової бази у сфері кібербезпеки, її застарілість у сфері захисту інформації, повільна імплементація положень європейського законодавства, недостатня врегульованість цифрової складової розслідування кримінальних правопорушень, а також низький рівень правової відповідальності за порушення вимог законодавства у цій сфері. Варто зазначити, що Стратегія кібербезпеки України встановлює стратегічну ціль: «Прагматичне міжнародне співробітництво», для досягнення якої необхідно спрямування відносин з міжнародними партнерами на розвиток взаємної довіри для спільної відповіді на кібератаки і подолання кризових ситуацій у кібербезпеці та на практичну співпрацю, таку, як: обмін інформацією про кібератаки та кіберінциденти, проведення спільних кібероперацій та розслідування міжнародних кіберзлочинів, регулярні кібернавчання та тренінги, обмін досвідом та найкращими практиками. Також важливим аспектом є забезпечення активної участі у діалозі в рамках міжнародних організацій щодо спільного вироблення норм поведінки

у кіберпросторі та вдосконалення відповідної нормативно-правової бази. Відтак прагматичне міжнародне співробітництво передбачає послідовність та систематичність узгоджених дій. У цьому контексті слід погодитись, що кожна держава, включаючи Україну, має створити ефективну національну систему кібербезпеки, посилювати спроможності суб'єктів сектора безпеки й оборони для забезпечення ефективної боротьби з кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом і кіберзлочинністю та поглиблювати міжнародне співробітництво в цій сфері, яке повинно мати системний та послідовний характер, супроводжуватися ґрунтовними дослідженнями, особливо стосовно попередження та усунення загроз кібербезпеки, відповідного успішного іноземного досвіду (Шемчук, 2018). Відтак важливу роль у розвитку міжнародного співробітництва з питань захисту кіберпростору повинні відігравати участь приватного сектора та впровадження сучасних наукових досліджень у зазначеній сфері. Дійсно, кібербезпека стала дуже критичною проблемою, яка потребує уваги дослідників, академіків та організацій для конфіденційного забезпечення захисту та безпеки інформаційних систем (Admass, Munaye, Diro, 2024).

При цьому головним зовнішньополітичним фарватером України у сфері кібербезпеки є: поглиблення євроінтеграційних процесів шляхом уніфікації підходів, методів і засобів забезпечення кібербезпеки з усталеними практиками НАТО; вжиття інших узгоджених з іноземними партнерами заходів, спрямованих на посилення кіберстійкості України; розвиток спроможностей національної системи кібербезпеки та захист національних інтересів у кіберпросторі (Поляков, 2021).

Щодо стратегічних орієнтирів ЄС у сфері кіберзахисту та кібезбезпеки, необхідно зазначити, що Стратегія кібербезпеки Євросоюзу на цифрове десятиліття спрямована на зміцнення колективної стійкості Європи проти кіберзагроз та забезпечення всім громадянам та бізнесу Європейського Союзу повної вигоди від надійних послуг та цифрових інструментів (Гавриляк, 2021). Ця Стратегія також повинна дати змогу Євросоюзу зміцнити лідерство в галузі міжнародних норм та стандартів у кіберпросторі, а також розвивати співпрацю з партнерами по всьому світу для сприяння глобальному, відкритому, стабільному та безпечному кіберпростору. Так, Стратегія кібербезпеки ЄС на цифрове десятиліття наголошує на тому, що ЄС і надалі сприятиме співпраці між державами-членами в галузі досліджень, інновацій та розвитку потенціалу у сфері кібербезпеки, заохочуючи держави-члени використовувати весь потенціал Постійного структурованого співробітництва (PESCO). Водночас ЄС посилить і розширить свій кібердіалог із третіми країнами, щоб просувати свої цінності та бачення кіберпростору, обмінюючись найкращими практиками та прагнучи до більш ефективної співпраці, також акцентовано увагу на посиленні захисту інформаційної галузі (The EU's Cybersecurity Straegy, 2020). Зазначений досвід стратегічного планування свідчить про приділення уваги важливим факторам, які забезпечують ефективний розвиток системи кібербезпеки, тому цей досвід доцільний до імплементації в Україні. В цьому контексті доречно згадати про розробку проекту Закону України «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури» № 11290 від 27.05.2024 р., яким пропонуються оновлення чинного законодавства та внесення відповідних змін, спрямованих на нормативне забезпечення захищеності від кібератак інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем (проект Закону «Про внесення змін...», 2024)

В умовах новітніх викликів, зумовлених повномасштабною агресією росії проти України, загальним погіршенням міжнародної безпекової ситуації та підвищенням рівня зовнішньої загрози держави-члени ЄС краще розуміють спільні інтереси, до яких належать територіальна цілісність, безпека зовнішніх кордонів Союзу, стійкість до пандемій, продовольча, водна та енергетична безпеки, екологічна стійкість, цілісність і належне функціонування єдиного ринку, безпечні та захищені мережі зв'язку, кібербезпека, боротьба з організованою злочинністю, тероризмом і екстремізмом тощо (Дорош, 2023). Зазначене підкреслює важливість реалізації заходів

із підтримки спільних безпекових інтересів країн-партнерів. Тож слушною є думка про те, що ключовими напрямками розвитку державної політики у сфері інформаційної безпеки є вдосконалення правового регулювання діяльності в кіберпросторі та боротьби з кіберзлочинністю; посилення інтеграції міжнародних стандартів у внутрішнє законодавство України; розробка та вдосконалення існуючих та створення нових стандартів щодо кібербезпеки; посилення захисту критичних об'єктів інфраструктури, які є найбільш вразливими до кіберзагроз; посилення міжнародного співробітництва у боротьбі з кіберзлочинністю та участь у відповідних глобальних ініціативах і форумах тощо (Горєлова, Вихрист, 2024).

ВИСНОВКИ

Проведене дослідження дало змогу розглянути особливості міжнародного співробітництва у сфері забезпечення кібербезпеки України, простежити динаміку його правового забезпечення і стратегічного планування та дійти висновку щодо необхідності продовження імплементації міжнародного досвіду та вдосконалення норм чинного законодавства у сфері зміцнення захисту кіберпростору. Серед основних перспективних напрямів подальшого розвитку міжнародного співробітництва доцільно виокремити: продовження співпраці з міжнародними партнерами у сфері кібербезпеки шляхом взаємодії та активної участі у нових ініціативах зміцнення кіберзахисту, протидії кіберзагрозам та кібератакам; систематичний обмін дослідженнями та інноваціями, досвідом побудови та ефективного функціонування національних систем кібербезпеки; вдосконалення законодавства в сфері кібербезпеки шляхом імплементації досвіду найкращих практик країн ЄС і стандартів НАТО. Отже, створення ефективної національної системи кібербезпеки та захисту кіберпростору неможливо без активізації міжнародного співробітництва в цій сфері, яке повинно супроводжуватися проведенням комплексних наукових досліджень і мати системно-динамічний, послідовний характер.

REFERENCES

Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications, 2,* 100031. Retrieved from https://doi.org/10.1016/j.csa.2023.100031.

Chernysh, R. (2023). International organizational experience in the sphere ensuring cyber security. *Herald of Criminal Justice, 3-4,* 112–121. [in Ukrainian].

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].

Dorosh, L. (2023). Evolution of regulatory and law ensuring of the EU security: Search and determination of key priorities. *Visnyk of the Lviv University. Series Philos.-Political Studies, 46,* 262–270. [in Ukrainian].

Draft Law "On Amendments to Certain Laws of Ukraine on Information Protection and Cyber Protection of State Information Resources and Critical Information Infrastructure Objects" No. 11290 (2024, May 27). Retrieved from https://itd.rada.gov.ua/billInfo/Bills/Card/44275. [in Ukrainian].

Havryliak, V. B. (2021). The EU's cybersecurity strategy for the digital decade: Perspectives for Ukraine. *Herald of the National Academy for Public Administration under the President of Ukraine. Series «Public Administration, 1,* 46–52. [in Ukrainian].

Horielova, V. Y., & Vikhryst, S. M. (2024). Legal support and prospects for the development of state policy in the field of information security. *Legal Bulletin, 3(13),* 79–85. [in Ukrainian].

Kononenko, V., Zdorovko, S., & Korol'eva, A. (2023). Information security as a special state. *Uzhhorod National University Herald. Series Law, 2(76),* 244–250. [in Ukrainian].

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].

Milik, P. (2021). International legal regulations in the area of cybersecurity. *Cybersecurity and Law, 2019(1),* 115–141. Retrieved from https://www.researchgate.net/publication/360421905_International_legal_regulations_in_the_area_of_cybersecurity.

Poliakov, O. M. (2021). Activation of international cooperation in the field of cybersecurity: The ways of improvement in today's realities. *Information and Law, 2,* 129–138. Retrieved from http://jnas.nbuv.gov.ua/article/UJRN-0001253594 [in Ukrainian].

Shemchuk, V. (2018). Main directions of international cooperation in the field of cybersecurity. *Scientific Notes of V. I. Vernadsky Taurida National University. Series: «Legal Sciences, 2,* 125–130. [in Ukrainian].

Sozanskyy, T., Krasnytskyi, I., Lutsyk, V., Yaremko, G., & Tuz, N. (2020). International practice of legal support of cyber security of the country. *Journal of Legal, Ethical and Regulatory Issues, 23(2),* 1–8.

Tarasyuk, A. V. (2020). Cyber security priorities of legal support in Ukraine at the present stage. *Subcarpathian Law Herald, 1(30),* 133–136. [in Ukrainian].

The EU's Cybersecurity Strategy for the Digital Decade. (2020). Joint Communication to the European Parliament and the Council. European Commission. Document 52020JC0018. (Brussels, 16.12.2020). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020JC0018

DEVELOPMENT OF INTERNATIONAL COOPERATION IN THE FIELD OF CYBER SECURITY: REGULATORY AND LEGAL BASIS AND PERSPECTIVES

Abstract. The article considers certain aspects of the development of international cooperation in the field of cybersecurity in Ukraine. It emphasizes the priority of issues of cyberspace protection, the importance of continuing cooperation with foreign partners in the field of cybersecurity and the introduction of new initiatives to strengthen cyber defense and deepen cooperation with the European Union and the North Atlantic Alliance. The norms of current regulatory legal acts and strategic planning documents in the field of cybersecurity are considered. Individual provisions of the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine", the Cybersecurity Strategy of Ukraine and the EU Cybersecurity Strategy for the Digital Decade are analyzed. It is established that an important strategic aspect is ensuring active participation in the dialogue within international organizations on the joint development of norms of behavior in cyberspace and improving the relevant regulatory and legal framework. The importance of building an effective national cybersecurity system and deepening international cooperation in this area, which should be systematic and consistent, has been proven. It is noted that cybersecurity is currently a critical problem that requires increased attention, including from researchers. The need to deepen European integration processes by unifying approaches, methods and means of ensuring cybersecurity with established NATO practices has been emphasized. The following promising areas for further development of international cooperation have been identified: cooperation with international partners in the field of cybersecurity through interaction and active participation in new initiatives to strengthen cyber defense, counter cyber threats and cyber attacks; systematic exchange of research and innovations, experience in building and effective functioning of national cybersecurity systems, and improvement of national legislation in the field of cybersecurity. The conclusions are drawn that the creation of an effective national system of cybersecurity and cyberspace protection is impossible without the activation of international cooperation in this area, which must be accompanied by comprehensive scientific research and have a systemic, dynamic, and consistent nature.

Key words: martial law, cyber security, cyber defense, cyber space, international cooperation, legal regulation, development prospects.

РОЗВИТОК МІЖНАРОДНОГО СПІВРОБІТНИЦТВА У СФЕРІ КІБЕРБЕЗПЕКИ: НОРМАТИВНО–ПРАВОВІ ЗАСАДИ ТА ПЕРСПЕКТИВИ

Анотація. У статті розглянуто окремі аспекти розвитку міжнародного співробітництва у сфері кібербезпеки України. Наголошено на пріоритетності питань захисту кіберпростору, важливості продовження співпраці з іноземними партнерами у сфері кібербезпеки та запровадження нових ініціатив

щодо зміцнення кіберзахисту та поглиблення співробітництва з Європейським Союзом і Північноатлантичним альянсом. Розглянуто норми чинних нормативно-правових актів та документів стратегічного планування у сфері кібербезпеки. Проаналізовані окремі положення Закону України «Про основні засади забезпечення кібербезпеки України», Стратегії кібербезпеки України та Стратегії кібербезпеки ЄС на цифрове десятиліття. Встановлено, що головним стратегічним аспектом розвитку міжнародного співробітництва є забезпечення активної участі у діалозі в рамках міжнародних організацій щодо спільного вироблення норм поведінки у кіберпросторі та вдосконалення відповідної нормативно-правової бази. Доведено важливість побудови ефективної національної системи кібербезпеки, поглиблення міжнародного співробітництва в цій сфері, яке повинно мати системний та послідовний характер. Зазначено, що кібербезпека наразі є критичною проблемою, яка потребує підвищеної уваги, в тому числі дослідників. Наголошено на необхідності поглиблення євроінтеграційних процесів шляхом уніфікації підходів, методів і засобів забезпечення кібербезпеки з усталеними практиками НАТО. Перспективними напрямами подальшого розвитку міжнародного співробітництва виокремлено: співпрацю з міжнародними партнерами у сфері кібербезпеки шляхом взаємодії та активної участі у нових ініціативах щодо зміцнення кіберзахисту, протидії кіберзагрозам та кібератакам; систематичний обмін дослідженнями та інноваціями, досвідом побудови та ефективного функціонування національних систем кібербезпеки; вдосконалення національного законодавства в сфері кібербезпеки. Зроблено висновки, що створення ефективної національної системи кібербезпеки та захисту кіберпростору неможливо без активізації міжнародного співробітництва в цій сфері, яке повинно супроводжуватися проведенням комплексних наукових досліджень і мати системно-динамічний, послідовний характер.

Ключові слова: воєнний стан, кібербезпека, кіберзахист, кіберпростір, міжнародне співробітництво, правове регулювання, перспективи розвитку.

Посилання на статтю: Лисеюк, А., & Свінцицька, Т. (2024). Розвиток міжнародного співробітництва у сфері кібербезпеки: нормативно-правові засади та перспективи. *Право та інноваційне суспільство,* 2 (23), 89-95. doi: https://doi.org/10.37772/2309-9275-2024-2(23)-8.