Вісник Національного університету "Львівська політехніка". Серія: "Юридичні науки"
№ 1 (41), 2024

УДК 340

Максим СИРОВАТЧЕНКО
Київський національний уверситет внутрішніх справ,
помічник нотаріуса, магістр,
e-mail: m.syrovatchenko@gmail.com
ORCID ID: https://orcid.org/0009-0009-8859-4168

ПРАВОВІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ: СУЧАСНІ ВИКЛИКИ ТА РОЛЬ НАЦІОНАЛЬНОГО ЗАКОНОДАВСТВА

http://doi.org/10.23939/law2024.41.314

У статті наголошено на особливостях сучасного стану кібербезпеки України та підкреслено важливість застосування ефективного законодавства, метою якого є захист кіберструктури. Охарактеризовано також вплив новітніх міжнародних інструментів та механізмів для боротьби із кіберзагрозами у контексті вітчизняного правового забезпечення.

Визначено ключові аспекти законодавства, які безпосередньо впливають на кібербезпеку та захист інформаційних ресурсів України, охарактеризовано актуальні виклики і загрози сучасного кіберпростору. Заходи щодо безпеки даних у кіберпросторі сьогодні доволі ефективні, про що свідчать результати статистичних даних щодо вирішення проблем, пов'язаних із хакерськими атаками на Україну під час воєнних дій 2022–2024 рр. Попри те, що чинні законодавчі акти створюють міцну основу для розвитку системи кібербезпеки України, у статті розглянуто питання запровадження нових інструментів, зокрема, роль використання штучного інтелекту у сфері захисту даних від кібератак. Висвітлено роль міжнародної співпраці у забезпеченні кібербезпеки як одну із необхідних умов забезпечення системи захисту національної безпеки України та його особливостей.

Ключові слова: кібербезпека; кібератака; законодавство; національна безпека; міжнародне співробітництво.

Постановка проблеми. У сучасному інформаційному просторі, який формується під впливом глобалізації та активного розвитку віртуальних технологій, особливу увагу привертають загрози, які можуть зруйнувати конфіденційність приватних чи державних даних. Україна сьогодні є одним із активних учасників світової мережі кіберпростору. Від початку повномасштабної війни, яка розпочалась у 2022 р., здійснено найбільшу кількість кібератак на державні та приватні сектори, що спричинило незначні порушення в роботі українських сайтів. Такі випадки становлять загрозу для українського ринку, який сьогодні залежить від світових мереж та організацій. Тому питання кібербезпеки необхідно розглядати із урахуванням чинного національного та міжнародного законодавства та їх ролі у забезпеченні захисту кіберпростору.

Аналіз дослідження проблеми. Питання кібербезпеки нині є актуальним, адже законодавство та механізми захисту інформаційних ресурсів потребують подальшого вдосконалення, відповідно до

нових викликів та можливих загроз. У цьому контексті набуває особливого значення оцінка міжнародного співробітництва України зі світовими лідерами у галузі кібербезпеки задля ефективного протистояння кіберзагрозам.

Метою статті є оцінка статистичних даних щодо ситуації в кіберпросторі України та світу, а також визначення ролі національного та міжнародного законодавства відповідно до реальних викликів і загроз цієї сфери.

Виклад основного матеріалу. Науковці виділяють декілька визначень кібербезпеки. Зокрема, у французькій документації подано таке визначення кібербезпеки: “це бажаний стан інформаційної системи, за якого вона може протистояти подіям з кіберпростору, що можуть поставити під загрозу доступність, цілісність або конфіденційність даних, які зберігаються, обробляються або передаються, і пов’язаних з ними послуг, які ці системи пропонують або роблять доступними”. У німецькій стратегії це “деяка сукупність необхідних і відповідних заходів, в результаті реалізації яких досягається мінімізація ризиків”. Канадські науковці визначають кібербезпеку як “захист кіберсистем від шкідливого неправильного використання та від інших деструктивних атак”, турецькі вважають, що це насамперед “захист інформаційних систем, що входять до складу кіберпростору, від нападів, забезпечення конфіденційності, цілісності та доступності інформації, яка обробляється в цьому просторі, виявлення та протидія атакам і кіберінцидентам”. Згідно із нідерланською системою визначень, кібербезпека – це “сукупність зусиль щодо запобігання шкоді, що може бути заподіяна внаслідок збоїв у роботі ІКТ або неправильного їх використання, а також з відновлення ІКТ після реалізації цих загроз” [1].

Відповідно до українського законодавства, кібербезпека – це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, за якої забезпечується сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [5].

Як бачимо, кожна із країн має власне визначення поняття кібербезпеки, основу якого становлять такі важливі аспекти, як захист інформаційних систем від небезпеки, що виникає у кіберпросторі. Усі визначення акцентують на необхідності застосування відповідних заходів для мінімізації ризиків і запобігання можливим негативним наслідкам, які пов’язані із неправильним використанням або атаками на інформаційні системи.

Оцінюючи динаміку останніх років, простежуємо позитивну тенденцію у сфері інформаційних технологій (ІТ). Насамперед спостерігається збільшення хмарних обчислень, які використовують майже у всіх сферах діяльності. Окрім цього, зростає складність мереж, що пов’язано із активним розвитком новітніх технологій.

Ці тенденції створюють сприятливі можливості для бізнесу й економіки загалом, проте водночас надають кіберзлочинцям більше можливостей для здійснення кібератак. Глобальний дефіцит кібербезпеки проявляється, насамперед, у кількості вакансій, які неможливо заповнити наявними працівниками у цій галузі. Проблема кіберзахисту є доволі великим ризиком, проте сприяє розвитку ефективних стратегій захисту, використовуючи аналітику, штучний інтелект та автоматизацію для ефективнішого реагування на кіберзагрози та мінімізації їхніх наслідків.

Основними видами загроз для кібербезпеки є malware (шкідливе програмне забезпечення), ransomware (програми-вимагачі), phishing (фішинг), insider threats (внутрішні загрози), distributed denial of service (ddos) attacks (атаки на відмову в обслуговуванні), а також атаки ботнетів, хмарні експлойти тощо [12].

Згідно зі звітом IBM (International Business Machines Corporation) “Вартість витоку даних у 2023 р.”, середня вартість витоку даних у 2023 р. становила 4,45 млн доларів США, що на 15 % перевищує показники останніх трьох років. Зокрема, середня вартість витоку даних, пов’язаного з

програмами-вимагачами, у 2023 р. була ще більшою – 5,13 млн доларів США. Це значення не враховує витрат на викуп, що в середньому становили додатково 1 542 333 доларів США, тобто на 89 % більше, ніж у попередньому році. За однією з оцінок, до 2025 р. кіберзлочинність може призвести до збитків для світової економіки на рівні 10,5 трильйонів доларів США за рік [12]. Ці цифри свідчать про зростання загроз кібербезпеці та необхідність реалізації ефективних заходів у цій сфері.

Україна перебуває під значним тиском кіберзлочинності, що відображає високу активність з боку хакерських груп. Сьогодні, в умовах російсько-української війни, відбувається зростання кількості кібератак на державні та комерційні об'єкти.

За даними Microsoft, у 2021 р., до розгортання широкомасштабного вторгнення Україна була однією із найзатребуваніших цілей для кібератак у світі, поступаючись лише США за цим показником. Протягом 2022 р. кількість кіберінцидентів істотно зросла, а урядова команда CERT-UA зафіксувала понад дві тисячі кібератак, що свідчить про надзвичайно високий рівень активності в цій сфері [3].

Підтвердженням цього є те, що українські владні органи зафіксували понад 85 хакерських груп, які негативно впливають на кібербезпеку країни. Більшість з них пов'язані з росією, з якою воює Україна. Незважаючи на це, Україна активно працює над зміцненням своїх кіберзахисних зусиль. Наприклад, за Національним індексом кібербезпеки Україна посідає 24-те місце серед 160 країн [3]. Це доволі високий показник, який свідчить про успішність заходів кіберзахисту. Однак у вітчизняній системі є слабкі місця, що спонукає до вдосконалення заходів для їх вирішення у наступні роки.

Варто зазначити, що кібератаки загрожують різним секторам, зокрема енергетичним компаніям, промисловим виробникам, логістичним підприємствам, телекомунікаційним компаніям та розробникам програмного забезпечення [3]. Однак останнім часом найсерйозніші атаки спрямовані на фінансовий сектор України, зокрема великі банки, які істотно впливають на фінансову систему країни.

Банки надають базові фінансові послуги населенню та зберігають чимало конфіденційної інформації, що робить їх привабливою мішенню для кіберзлочинців. Необхідно пам'ятати, що кіберзагрози не обмежуються великими компаніями, навіть невеликі підприємства можуть стати жертвами кібератак, зазнаючи серйозних фінансових та репутаційних втрат.

У звіті Держспецзв'язку України за 2023 р. відзначено зростання кількості кібератак порівняно з 2022 р. на 15,9 %, до 2543 інцидентів, у другій половині 2023 р. було зафіксовано та розслідувано 1,46 тис. кіберінцидентів [2].

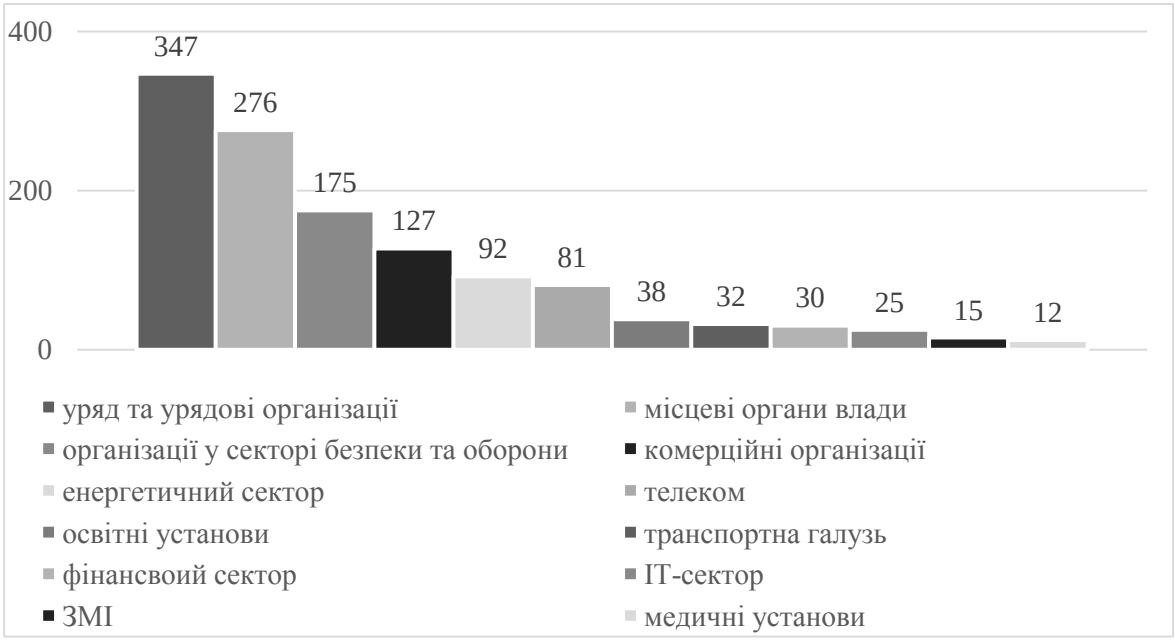

Рис. 1. Сектори, що найбільше постраждали від хакерських атак в Україні в 2023 р., од.

Відповідно до даних рис. 1, найбільше атак було спрямовано на урядові та місцеві органи влади, а також на організації у секторі безпеки та оборони. Енергетичний та телекомунікаційний сектори також були предметом численних атак.

Рис. 2. Рейтинг України за основними показниками Національного індексу безпеки у 2023 р., %

Також, згідно з даними національних та міжнародних рейтингів, у 2023 р. Україна посідала четверте місце в категорії Національний індекс кібербезпеки, досягши показника 81 %. За Глобальним індексом кібербезпеки Україна займає 78-ме місце із рівнем 66 %. Щодо Індексу розвитку електронного урядування та Індексу мережевої готовності Україна посідає відповідно 46-те та 43-тє місця з показниками 80 % та 55 % [11].

Ці дані свідчать про певний рівень захищеності кіберпростору в країні, але одночасно вказують на наявність прогалин та вразливостей, які потребують уваги та вдосконалення. Хоча показник не є найнижчим, він вказує на необхідність активніших заходів із підвищення захищеності кіберпростору та вдосконалення стратегій у цій галузі. Тому необхідним кроком для поліпшення статистики буде впровадження електронного урядування та розвитку інформаційних технологій, адже ці цифри вказують на можливості для підвищення ефективності управління й інфраструктури для забезпечення стабільності та безпеки в цих сферах [11].

Отже, у контексті вдосконалення системи кібербезпеки, необхідно, передусім, розглянути особливості правового забезпечення у сфері кіберзахисту. Відповідно до Закону України “Про основні засади забезпечення кібербезпеки України”, суб’єктами забезпечення кібербезпеки є міністерства та інші центральні органи виконавчої влади, місцеві державні адміністрації, органи місцевого самоврядування, правоохоронні, розвідувальні та контррозвідувальні органи, суб’єкти оперативно-розшукової діяльності, Збройні сили України, інші військові формування, утворені відповідно до закону, Національний банк України, підприємства, установи та організації, зараховані до об’єктів критичної інфраструктури, Служба безпеки України, Міністерство оборони України, Національна поліція України, Державна служба спеціального зв’язку та захисту України [4].

Ці установи забезпечують кібербезпеку, здійснюючи виявлення, запобігання та розслідування кіберзлочинності, захист критично важливих об’єктів та інформаційних ресурсів держави, розроблення та впровадження стратегій та заходів з кіберзахисту, співпрацю із міжнародними партнерами у сфері кібербезпеки, а також підвищення кіберсвідомості населення та бізнесу.

Ще одним важливим суб'єктом забезпечення кібербезпеки є Рада національної безпеки. Її роль визначає законодавство, зокрема стаття 4 Закону України "Про Раду національної безпеки і оборони України" [6].

Згідно з цим положенням, Рада національної безпеки і оборони України відповідає за розроблення та розгляд питань, пов'язаних із безпекою стратегічних національних інтересів, ураховуючи напрями забезпечення кібербезпеки, оскільки вона є частиною національної безпеки України. Рада виконує також низку заходів щодо інформаційної безпеки, яка полягає у захисті інформаційної інфраструктури, а кібербезпека в цій стратегії передбачає заходи захисту від цифрових атак у кіберпросторі. Рада здійснює стратегічну оцінку стану та перспектив забезпечення кібербезпеки на основі аналізу інформації від суб'єктів забезпечення кібербезпеки про загальний стан кібербезпеки в країні. Це свідчить про важливість координаційної функції Ради в контексті забезпечення кібербезпеки України.

Важливою у цьому напрямі є міжнародна співпраця України та світу. Зокрема, у 2023 р. міністерства закордонних справ України, Канади, Данії, Естонії, Франції, Німеччини, Нідерландів, Польщі, Швеції, Великої Британії та Сполучених Штатів Америки оголосили про створення нового механізму співробітництва в сфері кібербезпеки, який отримав назву "Талліннський механізм" [9].

Оцінюючи роль цього проєкту для зміцнення кібербезпеки, зазначимо, що цей інструмент призначений передусім для поліпшення координації та підтримки України в захисті критичної інфраструктури від потенційних кіберзагроз. Тут уже враховано вплив російських кібероперацій на критичну інфраструктуру України, доволі частих у 2023 р., через що й виникла необхідність тривалої допомоги у зміцненні кібербезпеки країни. Ця співпраця має усі шанси стати центральним пунктом підтримки для держав-членів, сприяючи розбудові цивільного кіберпотенціалу та координації з іншими групами, які надають допомогу Україні. Для збільшення ефективності кіберзахисту України союз країн-учасниць договору пропонує координацію за короткостроковим, середньостроковим та довгостроковим напрямами, забезпечуючи комплексний та стійкий підхід до цієї проблеми.

Ще одним серйозним викликом для правового аспекту забезпечення кіберзахисту України, зокрема, у контексті розгляду національного та міжнародного законодавства, є використання штучного інтелекту в сфері кібербезпеки.

Лише 28 % організацій широко використовують у сфері безпеки штучний інтелект, який знижує витрати і пришвидшує стримування атак. Середня економія для організацій, які широко використовують штучний інтелект і автоматизацію у сфері безпеки, становить 1,76 млн доларів США порівняно з організаціями, які цього не роблять [10].

За прогнозами експертів, до 2027 р. ринкова вартість застосування штучного інтелекту в кібербезпеці сягне 46,3 мільярда доларів США. Компанії, які спеціалізуються на кібербезпеці з використанням штучного інтелекту, пропонують вагомі переваги, надаючи організаціям безцінні інструменти для ефективної навігації в кіберпросторі та забезпечуючи більшу гнучкість у подоланні викликів, пов'язаних із кіберзагрозами [8].

Сьогодні у світі відсутнє законодавство, що встановлювало б правила щодо застосування штучного інтелекту для захисту країн від кібератак, ураховуючи зберігання та захист конфіденційної інформації й персональних даних. Проте такий закон може визначати права й обов'язки суб'єктів, які використовують штучний інтелект у кібербезпеці, й механізми відповідальності за порушення цих правил. Також новостворені закони можуть регулювати використання штучного інтелекту для розроблення й упровадження кібербезпеки, встановивши стандарти та вимоги до їх функціонування й безпеки. Законодавство визначає межі й умови для ефективного використання штучного інтелекту в кібербезпеці й забезпечує дотримання правових норм й стандартів.

Проте перші кроки у напрямі легалізації на державному рівні штучного інтелекту були зроблені 21 квітня 2021 року. У цей день Європейська комісія оприлюднила пропозицію Регламенту про штучний інтелект (AI Act), що являє собою новаторську правову ініціативу, оскільки вперше в історії встановлює уніфіковані норми для розроблення, розміщення на ринку та використання

штучного інтелекту в країнах Європейського Союзу. Попри розбіжності в підходах до регулювання штучного інтелекту в окремих країнах ЄС, цей Регламент прагне забезпечити спільний стандарт та визначити основні принципи, які регулюють цю сферу. Пропонований закон розроблено з метою забезпечення високого рівня захисту прав та інтересів громадян, а також сприяння використанню штучного інтелекту для загального блага суспільства.

За певних умов використання штучного інтелекту в сфері ризикової діяльності може призвести до ситуації, коли користувач або виробник не матиме законних підстав для притягнення до кримінальної або іншого виду юридичної відповідальності. Зазначена ситуація являє собою незвичайний випадок для доктрини кримінального права, тому потребує подальшого вивчення та аналізу. Виникнення таких ситуацій може потребувати розширення поняття суб'єкта кримінально-правових відносин та суб'єкта кримінальної відповідальності, враховуючи специфіку застосування штучного інтелекту в правовій сфері [7].

Висновки. Законодавство України про кібербезпеку встановлює ефективні механізми реагування на кіберзагрози та кіберінциденти, які закріплюються у нормативно-правових документах та становлять основу правового забезпечення кібербезпеки відповідно до міжнародного права. 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, зокрема США, 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.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Баранов О. А. Про тлумачення та визначення поняття "кібербезпека". *Правова інформатика*. 2014. № 2 (42). С. 54–62
2. Жарикова А. (2024). *Кількість кібератак у 2023 році зросла на 16 % – Держспецзв'язку. Економічна правда*. URL: https://www.epravda.com.ua/news/2024/01/31/709355/
3. Кібербезпека бізнесу під час війни. *Мінфін*. URL: https://www.project.minfin.com.ua/kiberbezpeka-biznesu-pid-chas-vijny
4. Про основні засади забезпечення кібербезпеки України. Закон України. *Відомості Верховної Ради (ВВР), 2017, № 45, ст.403)*. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
5. Про основні засади забезпечення кібербезпеки України. *Проєкт Закону України від 14.04.2016 № 2126а*. URL: https://ips.ligazakon.net/document/JH1N268B?an=11
6. Про Раду національної безпеки і оборони України. Закон України. *Відомості Верховної Ради України (ВВР), 1998, № 35, ст. 237)*. URL: https://zakon.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80#Text
7. Радутний О. Е. (2018). Кримінальна відповідальність штучного інтелекту. *Інформація і право*: науковий журнал. Київ: Науково-дослідний інститут інформатики і права Національної академії правових наук України. № 2 (21). С. 124–133. https://ippi.org.ua/sites/default/files/14boavpk.pdf
8. Роль штучного інтелекту в кібербезпеці: передбачення та запобігання атакам (2024). *Європейська Бізнес-асоціація*. URL: https://eba.com.ua/rol-shtuchnogo-intelektu-v-kiberbezpetsi-peredbachennya-ta-zapobigannya-atakam/
9. Талліннський механізм: Україна та міжнародні партнери започаткували новий інструмент співпраці у кіберпросторі (2023). *Урядовий портал*. URL: https://www.kmu.gov.ua/news/tallinnskyi-mekhanizm-ukraina-ta-mizhnarodni-partnery-zapochatkuvaly-novyi-instrument-spivpratsi-u-kiberprostori
10. Cost of a Data Breach Report (2023). *IMB*. URL: https://www.ibm.com/reports/data-breach
11. Ukraine. *National Cyber Security Index*. URL: https://ncsi.ega.ee/country/ua/
12. What is cybersecurity? *IBM*. URL: https://www.ibm.com/topics/cybersecurity

REFERENCES

1. Baranov O. A. ***Pro tlumachennya ta vy`znachennya ponyattya "kiberbezpeka".*** Pravova informaty`ka, 2014. No. 2 (42). P. 54–62 [in Ukrainian].

2. Zhary`kova A. (2024). ***Kil`kist` kiberatak u 2023 roci zrosla na 16 % – Derzhspeczzv'yazku. Ekonomichna pravda.*** URL: https://www.epravda.com.ua/news/2024/01/31/709355/ [in Ukrainian].

3. ***Kiberbezpeka biznesu pid chas vijny`***. *Minfin.* URL: https://www.project.minfin.com.ua/kiberbezpeka-biznesu-pid-chas-vijny [In Ukrainian].

4. ***Pro osnovni zasady` zabezpechennya kiberbezpeky` Ukrayiny`***. Zakon Ukrayiny`, Vidomosti Verxovnoyi Rady` (VVR), 2017, No. 45, st. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text [In Ukrainian].

5. ***Pro osnovni zasady` zabezpechennya kiberbezpeky` Ukrayiny`***. Proekt Zakonu Ukrayiny` vid 14.04.2016 No. 2126a. URL: https://ips.ligazakon.net/document/JH1N268B?an=11 [in Ukrainian].

6. ***Pro Radu nacional`noyi bezpeky` i oborony` Ukrayiny`***. Zakon Ukrayiny` (Vidomosti Verxovnoyi Rady` Ukrayiny` (VVR), 1998, No. 35, st. 237). URL: https://zakon.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80#Text [in Ukrainian].

7. Radutny`j O. E. (2018). ***Kry`minal`na vidpovidal`nist` shtuchnogo intelektu. Informaciya i pravo: naukovy`j zhurnal.*** Ky`yiv: Naukovo-doslidny`j insty`tut informaty`ky` i prava Nacional`noyi akademiyi pravovy`x nauk Ukrayiny`, 2017, No. 2 (21). S. 124–133. https://ippi.org.ua/sites/default/files/14boavpk.pdf [in Ukrainian].

8. ***Rol` shtuchnogo intelektu v kiberbezpeci: peredbachennya ta zapobigannya atakam*** (2024). Yevropejs`ka Biznes Asociaciya. URL: https://eba.com.ua/rol-shtuchnogo-intelektu-v-kiberbezpetsi-peredbachennya-ta-zapobigannya-atakam/ [in Ukrainian].

9. ***Tallinns`ky`j mexanizm: Ukrayina ta mizhnarodni partnery` zapochatkuvaly` novy`j instrument spivpraci u kiberprostori*** (2023). Uryadovy`j portal. URL: https://www.kmu.gov.ua/news/tallinnskyi-mekhanizm-ukraina-ta-mizhnarodni-partnery-zapochatkuvaly-novyi-instrument-spivpratsi-u-kiberprostori [in Ukrainian].

10. ***Cost of a Data Breach Report*** (2023). *IMB.* URL: https://www.ibm.com/reports/data-breach [in English].

11. Ukraine. ***National Cyber Security Index***. URL: https://ncsi.ega.ee/country/ua/ [in English].

12. ***What is cybersecurity? IBM.*** URL: https://www.ibm.com/topics/cybersecurity [in English].

Дата надходження: 03.02.2024 р.

Maksym SYROVATCHENKO
Kyiv national university of internal affairs,
assistant to the notary public, magister,
e-mail: m.syrovatchenko@gmail.com
ORCID ID: https://orcid.org/0009-0009-8859-4168

LEGAL ASPECTS OF CYBERSECURITY IN UKRAINE: CURRENT CHALLENGES AND THE ROLE OF NATIONAL LEGISLATION

The article identifies the peculiarities of the current state of cybersecurity in Ukraine and emphasizes the importance of applying effective legislation aimed at protecting the cyber structure, as well as choosing the best tools and mechanisms to combat cyber threats.

For the purpose of this study, the author has selected the national legislation aimed at regulating the cybersecurity sector. The key aspects of legislation affecting cybersecurity and protection of information resources of Ukraine, in particular in the context of current challenges and threats of modern cyberspace, are quite effective today, as evidenced by the results of statistics on solving problems related to hacker attacks on Ukraine during the military conflict in 2022–2024. However, despite the fact that the current legislative acts create a solid basis for the development of Ukraine's cybersecurity system, the article discusses issues that remain unresolved. In particular, the role of artificial intelligence in the field of data protection against cyberattacks in the current environment. The role of international cooperation in ensuring cybersecurity is also considered as one of the necessary conditions for ensuring the national security protection system of Ukraine.

Key words: cybersecurity; cyberattack; legislation; national security; international cooperation.