ISSN (Print) 2708-339X ISSN (Online) 2786-7498
Legal Bulletin № 4 (14), 2024

УДК 343.9:004.056
DOI 10.31732/2708-339X-2024-14-A10

СУЧАСНІ ПРОБЛЕМИ ЗАПОБІГАННЯ І ПРОТИДІЇ ЗЛОЧИННОСТІ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Степаненко Н.В.,
доктор філософії в галузі права, доцент,
доцент кафедри теорії та історіїдержави і права
Університет економіки та права «КРОК»
м. Київ, вул. Табірна, 30-32, Україна, 03113
e-mail: nataliasv@krok.edu.ua
ORCID: https://orcid.org/0000-0001-6216-2206

Піддубний Д.Д.,
здобувач ступеня вищої освіти «Магістр»
Університет економіки та права «КРОК»
м. Київ, вул. Табірна, 30-32, Україна, 03113
e-mail: piddubnyidd@krok.edu.ua
ORCID: https://orcid.org/0009-0000-4874-228X

MODERN PROBLEMS OF PREVENTING AND COUNTERING CRIME IN THE FIELD OF INFORMATION TECHNOLOGIES

Stepanenko N.V.,
PhD in law,
associate Professor of the Department of Theory and History of the State and Law of «KROK» University
Kyiv, Tabirna St. 30-32, Ukraine, 03113
e-mail: nataliasv@krok.edu.ua
ORCID:https://orcid.org/0000-0001-6216-2206

Piddubnyi D.D.,
graduate of the Master's degree of
«KROK» University
Kyiv, Tabirna St., 30-32, Ukraine, 03113
e-mail: piddubnyidd@krok.edu.ua
ORCID: https://orcid.org/0009-0000-4874-228X

Анотація. *Сучасний розвиток інформаційних технологій створює нові можливості для розвитку суспільства, бізнесу та урядових організацій, але водночас ставить нові виклики для безпеки. Однією з найгостріших проблем є злочинність у сфері інформаційних технологій, яка включає в себе багато різних видів правопорушень, таких як кіберзлочинність, шахрайство з використанням електронних ресурсів, несанкціонований доступ до інформаційних систем, шкідливе програмне забезпечення та інші технологічні експлойти. Зростання кіберзагроз зумовлене швидким розвитком цифрових інфраструктур, глобалізацією даних та ускладненням технологій, що робить боротьбу з цими злочинами дедалі складнішою. Ця проблема є особливо актуальною через зростання кількості кіберзлочинів, які завдають значних економічних збитків як урядам, так і приватному сектору, а також загрожують інформаційній безпеці громадян. Такі злочини характеризуються транснаціональним характером та анонімністю зловмисників, що ускладнює їх розслідування та притягнення до відповідальності. Крім того, стрімкий розвиток таких технологій, як штучний інтелект, великі дані та Інтернет речей (IoT), призводить до появи нових векторів експлуатації та кіберзагроз. Запобігання та боротьба з кіберзлочинністю вимагає комплексного підходу, що поєднує правове регулювання, технологічні рішення, міжнародне співробітництво та кіберграмотність. У дослідженні наголошується на необхідності розвитку національного законодавства у сфері кібербезпеки та кіберзлочинності відповідно до міжнародних стандартів. Законодавча робота повинна охоплювати як кримінально-правові заходи, так і цивільно-правові регуляторні аспекти, такі як захист персо-*

нальних даних, електронна комерція та інформаційна безпека. Важливою передумовою ефективної боротьби з кіберзлочинністю є співпраця між державними органами та приватним сектором. IT-компанії повинні брати активну участь у процесі захисту від кіберзагроз. Це пов'язано з тим, що значна частина таких злочинів вчиняється через атаки на власну інфраструктуру та дані клієнтів. Крім того, важливу роль у запобіганні злочинам відіграє обізнаність та кіберграмотність населення. Адже часто саме необережна поведінка користувачів призводить до успішних кібератак.

Важливість міжнародного співробітництва у боротьбі з кіберзлочинністю: Транснаціональний характер IT-злочинності вимагає координації зусиль національних правоохоронних органів, обміну інформацією про нові загрози та вироблення спільних підходів до розслідування і запобігання злочинам. Існують також виклики, пов'язані з юрисдикційними конфліктами та різним рівнем розвитку кібербезпеки в різних країнах, які вимагають спільних дій на міжнародному рівні.

Ключові слова: *кіберзлочинність, кібербезпека, правове регулювання, інформаційні технології, міжнародне співробітництво.*

Формул*: 0, рис.: 0, табл.: 0, бібл.: 12.*

Abstract*. The modern development of information technologies creates new opportunities for the advancement of society, business, and government organizations, but at the same time introduces new security challenges. One of the most pressing issues is crime in the field of information technology, which encompasses various offenses, such as cybercrime, fraud using electronic resources, unauthorized access to information systems, malicious software, and other technological exploits. The growth of cyber threats is driven by the rapid development of digital infrastructures, the globalization of data, and the increasing complexity of technologies, which makes combating these crimes ever more challenging. This issue is particularly relevant due to the rising number of cybercrimes that cause significant economic losses to both governments and the private sector, while also posing a threat to the information security of citizens. These crimes are characterized by their transnational nature and the anonymity of perpetrators, which complicates investigations and holding offenders accountable. Additionally, the rapid development of technologies such as artificial intelligence, big data, and the Internet of Things (IoT) creates new vectors for exploitation and cyber threats. Preventing and combating cybercrime requires a comprehensive approach that combines legal regulation, technological solutions, international cooperation, and cyber literacy. The study emphasizes the need for the development of national legislation on cybersecurity and cybercrime in accordance with international standards. Legislative efforts should cover both criminal justice measures and civil regulatory aspects, including personal data protection, e-commerce, and information security. An essential prerequisite for effective cybercrime prevention is collaboration between government agencies and the private sector. IT companies must actively participate in protecting against cyber threats, as a significant portion of these crimes target their infrastructure and customers' data. Furthermore, public awareness and cyber literacy play a crucial role in crime prevention, as careless user behavior often leads to successful cyberattacks.*

The Importance of International Cooperation in Combating Cybercrime The transnational nature of IT-related crimes requires the coordination of efforts by national law enforcement agencies, the exchange of information about emerging threats, and the development of common approaches to investigation and prevention. Challenges also arise from jurisdictional conflicts and varying levels of cybersecurity development across countries, necessitating joint actions at the international level.

Keywords*: cybercrime, cybersecurity, legal regulation, information technology, international cooperation.*

Formulas*: 0, fig.: 0, tabl.: 0, bibl.: 12.*

Постановка проблеми. З розвитком інформаційних технологій кіберзлочинність стала однією з найбільш критичних загроз сучасного суспільства. Кіберзлочинці використовують дистанційні методи для завдання шкоди, що значно ускладнює процес їхнього виявлення та притягнення до відповідальності. Ця проблема посилюється тим, що національні правові системи часто не встигають адаптуватися до швидких технологічних змін. Як наслідок, виникає потреба в ефективних законодавчих та технічних заходах для протидії новим кіберзагрозам. Необхідність міжнародного співробітництва стає ще актуальнішою, оскільки атаки не мають територіальних меж і можуть завдати шкоди будь-якій країні незалежно від її розташування.

Аналіз досліджень і публікацій. У наукових колах активно вивчаються різні аспекти кібербезпеки. Одним із ключових міжнародних документів є Будапештська конвенція про кіберзлочинність (2001), яка стала основою для міжнародного співробітництва у цій сфері. Дослідження McAfee (2022) свідчать про масштабні економічні втрати, що сягають 600 мільярдів доларів щороку внаслідок кіберзлочинів. У роботі Goodman (2015) підкреслюється, що цифрове підпілля продовжує розвиватися, створюючи нові виклики для глобальної безпеки. Проте, незважаючи на наявність нормативних документів, таких як Регламент GDPR у Європейському Союзі та USA Patriot Act

у США, проблема кіберзлочинності залишається однією з найбільш актуальних.

Не вирішені раніше проблеми у даній тематиці. Однією з основних проблем є недостатня адаптація національних законодавств до сучасних технологічних викликів. Багато країн стикаються з труднощами у зборі цифрових доказів та ідентифікації злочинців через використання анонімних мереж та VPN. Крім того, існують значні прогалини в міжнародному співробітництві, що ускладнює оперативне реагування на глобальні загрози. Хоча Будапештська конвенція створила основу для координації дій між країнами, кіберзлочинність продовжує еволюціонувати швидше, ніж адаптуються правові механізми.

Метою статті є виявлення основних викликів, пов'язаних із боротьбою з кіберзлочинністю, та аналіз заходів протидії з акцентом на вдосконалення правового регулювання і міжнародної співпраці. Дослідження зосереджується на вивченні ключових аспектів національних та міжнародних ініціатив у сфері кібербезпеки, а також визначенні напрямків для покращення технічних і правових заходів, необхідних для ефективної боротьби з кіберзлочинністю.

Виклад основного матеріалу. Інформаційні технології сьогодні є не тільки основним драйвером розвитку економіки, соціальних та державних систем, але й відкривають нові можливості для кіберзлочинності. З кожним роком кількість правопорушень у цифровому просторі збільшується, а новітні технології використовуються не лише для захисту, але й для скоєння злочинів. Кіберзлочинці отримують можливість завдавати шкоди, не виходячи з дому, і через це національні та міжнародні правові системи виявляються непідготовленими до реагування на ці загрози [9].

Кіберзлочини охоплюють широкий спектр незаконної діяльності – від крадіжки особистих даних до масованих атак на критичні інфраструктури. Прикладом таких атак є події 2015 року, коли хакери змогли проникнути в українські енергосистеми, викликавши масштабні відключення електроенергії. Це лише один із багатьох прикладів, що демонструє потенціал кіберзлочинності дестабілізувати ключові аспекти життєдіяльності суспільства. Сьогодні кібербезпека є однією з ключових складових національної безпеки кожної країни. Згідно з даними McAfee у 2022 році, глобальні втрати від кіберзлочинності досягли 600 мільярдів доларів на рік [8], що свідчить про масштабність цієї загрози. Проте законодавчі механізми боротьби з кіберзлочинністю часто відстають від технологічних інновацій, що дає злочинцям можливість використовувати сучасні технології без належної відповідальності.

Важливим аспектом є те, що кіберзлочинність не знає кордонів. Хакери можуть діяти з будь-якої точки світу, в той час як правові норми залишаються прив'язаними до національних юрисдикцій. Це вимагає розвитку міжнародного співробітництва для ефективної боротьби з цим явищем.

З розвитком інформаційних технологій та інтернету кіберзлочинність стала однією з найгостріших проблем сучасного суспільства. Визначення кіберзлочинності охоплює всі види правопорушень, що вчиняються з використанням комп'ютерних систем або проти них. Кіберзлочини можуть бути спрямовані на самі системи, їх користувачів або інфраструктуру, залежно від мети нападників. Одними з найпоширеніших видів кіберзлочинів є хакерські атаки, крадіжка особистих даних, фінансові махінації та кібертероризм.

Хакерські атаки зазвичай полягають у несанкціонованому втручанні в роботу комп'ютерних систем з метою викрадення інформації, порушення функціонування мереж або нанесення шкоди. Один із відомих прикладів такої атаки стався в Україні у грудні 2015 року, коли хакери проникли в енергетичну мережу і відключили електроенергію для сотень тисяч людей на заході країни. Цей інцидент привернув увагу до важливості кібербезпеки, особливо у контексті захисту критичної інфраструктури. Іншою загрозою є крадіжка особистих даних, яка передбачає несанкціонований доступ до конфіденційної інформації фізичних або юридичних осіб. Яскравим прикладом є атака на компанію Equifax у 2017 році, під час якої було викрадено персональні дані понад 145 мільйонів осіб [11]. Такі інциденти демонструють глобальний характер проблеми, оскільки жертви можуть перебувати

у різних країнах, а злочинці можуть діяти з будь-якої точки світу.

Фінансові махінації у кіберпросторі стали особливо актуальними через поширення електронної комерції та банківських операцій в інтернеті. Кіберзлочинці використовують фішингові схеми для викрадення реквізитів банківських карток і подальшого зняття коштів з рахунків жертв. Такі схеми стають дедалі витонченішими, що ускладнює їх своєчасне виявлення і запобігання. Кібертероризм, у свою чергу, є однією з найбільш небезпечних форм кіберзлочинності, оскільки передбачає атаки на державні або приватні інфраструктурні об'єкти з метою дестабілізації політичної або економічної ситуації в країні. Наприклад, у 2007 році Естонія зіткнулася з масштабними DDoS-атаками, що паралізували роботу урядових сайтів та фінансових установ. Ця атака стала каталізатором для розвитку системи кібероборони на державному рівні.

Ключові етапи еволюції правового регулювання. Еволюція правового регулювання кіберзлочинності почалася з появою перших міжнародних угод, які окреслили основні правові механізми боротьби із кіберзагрозами. Найважливішим документом у цій сфері стала Будапештська конвенція про кіберзлочинність, ухвалена у 2001 році [1]. Це перша міжнародна угода, спрямована на гармонізацію кримінальних законів різних країн щодо злочинів у кіберпросторі, таких як несанкціонований доступ до комп'ютерних систем, злом та поширення шкідливого програмного забезпечення. Конвенція передбачає криміналізацію цих діянь і визначає засади міжнародного співробітництва у сфері кібербезпеки, оскільки кіберзлочини часто мають транснаціональний характер. Більше 60 країн, зокрема Україна, ратифікували цю конвенцію, що стало важливим кроком до побудови глобальної системи кіберзахисту.

Крім міжнародних ініціатив, багато країн розробили власні національні закони про кібербезпеку, що сприяють боротьбі з кіберзлочинами на внутрішньому рівні. Наприклад, у США після терактів 11 вересня 2001 року був ухвалений закон USA Patriot Act, який розширив повноваження правоохоронних органів [2] у боротьбі з тероризмом та кіберзагрозами. Цей закон дозволяє здійснювати моніторинг комунікацій у мережі з метою виявлення потенційних загроз і злочинців. У Європейському Союзі важливим кроком став Регламент загального захисту даних (GDPR), який встановив нові стандарти щодо обробки та зберігання персональних даних [4]. GDPR забезпечує захист особистої інформації громадян ЄС і вводить жорсткі санкції для компаній, що порушують вимоги регламенту.

Міжнародне співробітництво є ключовим елементом у боротьбі з кіберзлочинністю. Окрім Будапештської конвенції, країни активно співпрацюють у рамках таких організацій, як НАТО та Європол. Одним з основних механізмів співпраці є Центр Багатоцільової Кібероборони НАТО (CCDCOE), який займається координацією зусиль країн-членів Альянсу [10] у сфері кібероборони. Центр проводить навчання, дослідження та надає рекомендації з удосконалення кіберзахисту на державному рівні.

Законодавче забезпечення в Україні. Україна, регулярно піддаючись кібератакам, активно вдосконалює національне законодавство у сфері кібербезпеки. Важливим нормативним актом у цій галузі є Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», який визначає правові засади захисту інформаційних систем від несанкціонованого доступу. Цей закон окреслює ключові принципи захисту даних, встановлює вимоги до суб'єктів, які здійснюють обробку інформації, та передбачає відповідальність за порушення норм інформаційної безпеки.

Важливим кроком у розбудові національної системи кіберзахисту стало прийняття Закону України «Про основні засади забезпечення кібербезпеки України». Цей закон визначає роль державних органів у забезпеченні кібербезпеки, зокрема координацію дій між Міністерством внутрішніх справ, Службою безпеки України та іншими відомствами. Закон передбачає створення інфраструктури для моніторингу та попередження кібератак, а також встановлює основні завдання для кіберполіції та інших органів, що займаються боротьбою з кіберзлочинністю.

Ключовим елементом системи кібер-

захисту в Україні є кіберполіція, створена у 2015 році як спеціалізований підрозділ Національної поліції України. Основним завданням кіберполіції є протидія кіберзлочинам, розслідування кібератак та запобігання новим загрозам у кіберпросторі. Однією з найбільш відомих операцій кіберполіції стала ліквідація злочинного угруповання, яке стояло за поширенням вірусу NotPetya у 2017 році [12]. Цей вірус завдав значних збитків багатьом українським та міжнародним компаніям і став одним з найбільших викликів для кібербезпеки України.

Однією з найбільших проблем у боротьбі з кіберзлочинністю є складність ідентифікації злочинців. Кіберпростір забезпечує високий рівень анонімності, що дозволяє злочинцям діяти приховано та ускладнює їх виявлення. Зокрема, використання шифрованих мереж, таких як Tor, а також VPN-сервісів, які приховують справжні IP-адреси користувачів, створює додаткові труднощі для правоохоронних органів у процесі розслідування кіберзлочинів. Хакери, які здійснюють атаки, можуть знаходитися в різних країнах, змінювати місце розташування або використовувати технології, що заплутують слідство. Це значно ускладнює процес ідентифікації, оскільки злочинці мають можливість діяти без відчуття негайної відповідальності. Наприклад, під час масштабних атак на українські урядові вебресурси в 2014-2015 роках більшість нападників використовували проксі-сервери, що не дозволяло одразу визначити їх місцезнаходження або джерело атак.

Ще однією серйозною проблемою є збір доказів. Електронні докази, такі як файли логів, мережевий трафік або дані з серверів, можуть бути легко змінені, знищені або приховані. У багатьох випадках злочинці використовують складні методи шифрування, які роблять неможливим розшифрування інформації без спеціальних інструментів чи паролів, доступ до яких можна отримати тільки у злочинців. Крім того, оскільки електронні докази є нестабільними, їх збір потребує оперативної та ретельної роботи правоохоронців. Неправильне вилучення чи обробка таких доказів може призвести до їх втрати або неприпустимості в суді, що ускладнює процес доведення вини злочинця. Як приклад, можна навести справу, пов'язану з атаками вірусу WannaCry у 2017 році. Цей вірус атакував комп'ютерні системи в більш ніж 150 країнах [6], однак злочинців вдалося ідентифікувати лише через кілька місяців завдяки складним міжнародним розслідуванням, у ході яких доводилося обробляти величезний масив цифрових даних.

Ще одним важливим аспектом є правовий статус електронних доказів у суді. У багатьох юрисдикціях, зокрема в Україні, законодавство ще не в повній мірі адаптоване до реалій використання цифрових доказів. Це часто призводить до проблем із їх прийняттям та оцінкою в судовому процесі. Для того щоб електронні докази були дійсними, їх збір та обробка повинні відповідати встановленим правовим стандартам. Проте, навіть коли дотримані всі вимоги, судді інколи мають обмежені знання про технічні аспекти таких доказів, що може негативно впливати на справедливість рішень. Вирішення цієї проблеми вимагає не тільки вдосконалення законодавства, а й підвищення кваліфікації суддів та правоохоронців у галузі цифрових технологій.

Кіберзлочинність є транснаціональною загрозою, оскільки атаки можуть здійснюватися в одній країні, а наслідки відчуваються в іншій. Це вимагає ефективного міжнародного співробітництва, адже жодна країна не може самостійно вирішити проблему глобальної кіберзлочинності. Успішна боротьба з кіберзагрозами залежить від здатності країн взаємодіяти та обмінюватися інформацією, що стосується кіберзлочинів, технічних аспектів атак та методів їх розслідування. Одним з ключових прикладів міжнародної співпраці є діяльність Інтерполу, який займається координацією міжнародних операцій з боротьби з кіберзлочинністю та надає технічну допомогу країнам-членам організації. Інтерпол постійно здійснює моніторинг кіберпростору та підтримує комунікацію між національними правоохоронними органами [3], що дозволяє швидко реагувати на нові кіберзагрози.

Європол також відіграє важливу роль у боротьбі з кіберзлочинністю, особливо у межах Європейського Союзу. У 2013 році був створений Європейський центр з кіберзлочинності (EC3), який зосереджується на

розслідуванні найбільш серйозних злочинів у кіберпросторі [7], таких як кібертероризм, дитяча порнографія та великомасштабні шахрайства в інтернеті. Цей центр надає підтримку національним правоохоронним органам у розслідуванні злочинів, а також проводить навчання для фахівців у сфері кібербезпеки. Завдяки діяльності Європолу було проведено кілька успішних міжнародних операцій, серед яких варто згадати операцію «Аваланш», що тривала з 2012 по 2016 рік. Вона привела до ліквідації великого кіберзлочинного угруповання, яке використовувало ботнети для здійснення шахрайства в інтернеті та завдало збитків на мільйони доларів.

Іншим важливим аспектом міжнародного співробітництва є участь країн у міжнародних угодах та конвенціях. Окрім Будапештської конвенції, важливим документом у цій сфері є Талліннський маніфест щодо кібероборони, який був прийнятий у рамках НАТО. Цей документ визначає основні засади співпраці країн-членів Альянсу у сфері кібероборони та окреслює принципи взаємодії у разі виникнення кіберзагроз. Крім того, багато країн беруть участь у глобальних форумах та ініціативах, таких як Форум з управління інтернетом (IGF), де обговорюються питання безпеки в інтернеті, цифрових прав та захисту приватності в глобальному масштабі.

Ефективна боротьба з кіберзлочинністю вимагає поєднання як технічних, так і правових заходів. Сучасні технічні рішення, такі як системи моніторингу та аналізу мережевого трафіку, штучний інтелект для виявлення аномалій у роботі систем, а також розробка нових методів захисту даних відіграють важливу роль у запобіганні кіберзлочинам. Важливим інструментом є створення національних центрів реагування на кіберзагрози (CERT), які здійснюють моніторинг мереж, виявляють підозрілу активність та реагують на кібератаки у реальному часі. В Україні функціонує Національний центр оперативно-технічного управління мережами телекомунікацій (CERT-UA), який є одним із ключових елементів у національній системі кіберзахисту [5].

Проте, технічні заходи самі по собі не є достатніми. Необхідне також вдосконалення правових механізмів боротьби з кіберзлочинністю, що включає не тільки прийняття нових законів, але й адаптацію існуючих норм до сучасних викликів. Важливим аспектом є оновлення нормативної бази для збору, зберігання та використання електронних доказів у судових процесах. Крім того, важливо підвищити ефективність правозастосування шляхом навчання правоохоронних органів та суддів щодо сучасних методів розслідування кіберзлочинів. Необхідно створювати спеціалізовані підрозділи, які б займалися розслідуванням злочинів у кіберпросторі та забезпечували тісну співпрацю між різними відомствами.

Серед пропозицій щодо вдосконалення правового регулювання в Україні можна зазначити посилення санкцій за кіберзлочини, особливо за рецидивні кібератаки, що завдають значної шкоди національній безпеці та економіці. Крім того, слід переглянути законодавчі норми щодо кримінальної відповідальності за використання шкідливого програмного забезпечення та здійснення атак на критичні об’єкти інфраструктури. Україна, як частина глобальної спільноти, повинна активно впроваджувати міжнародні стандарти кібербезпеки і зміцнювати свої позиції у боротьбі з кіберзлочинністю як на національному, так і міжнародному рівні.

Висновки. Кіберзлочинність у сучасному світі стає однією з найактуальніших загроз як для окремих країн, так і для глобальної безпеки. З кожним роком інформаційні технології все глибше інтегруються у повсякденне життя людей, що, у свою чергу, створює нові можливості для зловмисників використовувати ці технології з метою скоєння правопорушень. Цифрові злочини, такі як хакерські атаки, крадіжка персональних даних, фінансові махінації та кібертероризм, набули глобальних масштабів, завдаючи значних економічних, політичних та соціальних збитків. Високий рівень анонімності в інтернеті, технічні складнощі ідентифікації кіберзлочинців та правові проблеми збору та обробки електронних доказів роблять боротьбу з кіберзлочинністю надзвичайно складним завданням для правоохоронних органів.

Серед головних проблем сучасної боротьби з кіберзлочинністю варто виділити

складність ідентифікації злочинців у кіберпросторі через використання технологій, що приховують їхню особистість. Це значно ускладнює роботу правоохоронних органів у розслідуванні кіберзлочинів. Водночас законодавство в багатьох країнах, зокрема в Україні, ще не повністю адаптоване до реалій кіберзлочинності, що ускладнює їх прийняття в судовому процесі.

Міжнародне співробітництво залишається ключовим інструментом у боротьбі з кіберзлочинністю, оскільки злочини в кіберпросторі рідко обмежуються межами однієї країни. Важливу роль відіграє участь у глобальних ініціативах та програмах, які спрямовані на координацію зусиль різних країн у боротьбі з кіберзлочинністю та підвищення рівня захисту критичних інфраструктур.

Враховуючи швидкий розвиток технологій, держава повинна постійно оновлювати та вдосконалювати правову базу для ефективної боротьби з кіберзлочинністю. Одним із важливих напрямів є навчання суддів, слідчих та правоохоронців, щоб вони краще розуміли технічні аспекти цифрових доказів і могли правильно оцінювати їх у процесі розслідувань та судових розглядів. Водночас важливою є підтримка інновацій у сфері кібербезпеки, розробка нових технологій захисту даних та запобігання атакам. Це має стати спільним завданням держави, приватного сектору та міжнародної спільноти.

Таким чином, боротьба з кіберзлочинністю вимагає комплексного підходу, що включає як технічні рішення, так і вдосконалення правових механізмів. Міжнародна співпраця, підвищення рівня кваліфікації кадрів у сфері кібербезпеки та постійне оновлення законодавства є тими ключовими напрямками, які дозволять ефективно протистояти кіберзлочинам. Україна, як частина глобальної цифрової економіки, повинна активно впроваджувати нові технології кіберзахисту, брати участь у міжнародних ініціативах та вдосконалювати національну правову базу, щоб забезпечити ефективний захист від кіберзлочинності та гарантувати безпеку своїх громадян та інфраструктур.

Література:

1.Budapest Convention on Cybercrime: Рада Європи, 2001 р. URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 (дата звернення: 25.10.2024).

2.General Data Protection Regulation (GDPR): Регламент Європейської Комісії від 27.04.2016р. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (дата звернення: 25.10.2024).

3.Tallinn Manual on Cyber Defence 2.0: Рекомендаційний документ НАТО, 2017 р. URL: https://www.onlinelibrary.iihl.org/wp-content/uploads/2021/05/2017-Tallinn-Manual-2.0.pdf (дата звернення: 25.10.2024).

4.USA Patriot Act: Закон Конгресу США від 2001 р. RL: https://www.justice.gov/archive/ll/archive.htm (дата звернення: 25.10.2024).

5.CERT-UA Reports: CERT-UA. URL: https://cert.gov.ua/ (дата звернення: 25.10.2024).

6.Equifax Data Breach Report: Звіт Комітету з нагляду і реформ Палати представників США, 2017 р. URL: https://oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf (дата звернення: 25.10.2024).

7.Interpol Operations Against Cybercrime: Інтерпол, URL: https://www.interpol.int/Crimes/Cybercrime/Cybercrime-operations (дата звернення: 25.10.2024).

8.McAfee Report on Economic Impact of Cybercrime: Звіт McAfee, 2022 р.

URL: https://www.mcafee.com/de-ch/consumer-corporate/newsroom/press-releases/press-release.html?news_id=6859bd8c-9304-4147-bdab-32b35457e629 (дата звернення: 25.10.2024).

9.WannaCry Ransomware Attack Report: Європол, 2017 р. URL: https://www.europol.europa.eu/wannacry-ransomware (дата звернення: 25.10.2024).

10.Goodman, M. (2015). Future Crimes: Inside the Digital Underground and the Battle for Our Connected World. URL: https://books.google.com.ua/books/about/Future_Crimes.html?id=tn22CwAAQBAJ&redir_esc=y (дата звернення: 25.10.2024).

11.Europol's European Cybercrime Centre (EC3): Європол, без дати.

URL: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (дата звернення: 25.10.2024).

12.NotPetya Cyberattack Analysis: BBC News, 2017 р. URL: https://www.bbc.com/news/technology-40428967 (дата звернення: 25.10.2024).

References:

1.Budapest Convention on Cybercrime: Council of Europe, 2001. URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 (Accessed: October 25,2024).

2.General Data Protection Regulation (GDPR): European Commission Regulation of 27.04.2016. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (Accessed: October 25,2024).

3.Tallinn Manual on Cyber Defence 2.0: NATO advisory document, 2017. URL: https://www.onlinelibrary.iihl.org/wp-content/uploads/2021/05/2017-Tallinn-Manual-2.0.pdf (Accessed: October 25,2024).

4.USA Patriot Act: U.S. Congress Law of 2001. URL: https://www.justice.gov/archive/ll/archive.htm (Accessed: October 25,2024).

5. CERT-UA Reports: CERT-UA, n.d. URL: https://cert.gov.ua/ (Accessed: October 25,2024).

6. Equifax Data Breach Report: U.S. House Committee on Oversight and Reform, 2017. URL: https://oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf (Accessed: October 25,2024).

7. URL: https://www.interpol.int/Crimes/Cybercrime/Cybercrime-operations (Accessed: October 25,2024).

8. McAfee Report on Economic Impact of Cybercrime: McAfee Report, 2022. URL: https://www.mcafee.com/de-ch/consumer-corporate/newsroom/press-releases/press-release.html?news_id=6859bd8c-9304-4147-bdab-32b35457e629 (Accessed: October 25,2024).

9. WannaCry Ransomware Attack Report: Europol, 2017. URL: https://www.europol.europa.eu/wannacry-ransomware (Accessed: October 25,2024).

10.Goodman, M. (2015). Future Crimes: Inside the Digital Underground and the Battle for Our Connected World. URL:https://books.google.com.ua/books/about/Future_Crimes.html?id=tn22CwAAQBAJ&redir_esc=y (Accessed: October 25,2024).

11. Europol's European Cybercrime Centre (EC3): Europol, URL: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (Accessed: October 25,2024).

12. NotPetya Cyberattack Analysis: BBC News, 2017. URL: https://www.bbc.com/news/technology-40428967 (Accessed: October 25,2024).

Стаття надійшла до друку 31 жовтня 2024 року