УДК 343.9:004.056(477)
DOI: https://doi.org/10.31359/2079-6242-2025-49-178

В. Л. Гончарук, адвокат, доктор філософії у галузі права, доцент кафедри національної безпеки, доцент кафедри управління фінансово-економічною безпекою Інститут безпеки Міжрегіональної академії управління персоналом (МАУП)
ORCID: 0000-0002-9627-9530

ПРАВОВІ МЕХАНІЗМИ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ: СВІТОВА ПРАКТИКА ТА ВІТЧИЗНЯНИЙ КОНТЕКСТ

Постановка проблеми. Загроза національній безпеці України є одним із серйозних викликів, що охоплює різні сфери – військову, економічну, інформаційну та кіберпростір. Особливу увагу привертає до себе кібербезпека, оскільки кібернапади на критичну інфраструктуру, державні установи та фінансові системи, як правило, мають масштабні та деструктивні форми. Такі дії спрямовуються на дестабілізацію державного управління, підрив довіри громадян до органів влади, а також порушення роботи ключових секторів економіки. Ефективне протистояння кіберзагрозам потребує розробки та впровадження сучасних технологій захисту, міжнародної співпраці, а також підвищення рівня обізнаності громадян про правила «цифрової гігієни». Забезпечення кібербезпеки є невід'ємною складовою національної безпеки, забезпечуючи консолідацію зусиль держави, бізнесу (приватного сектора) та суспільства.

В Україні питання кіберзахисту набуло особливої значущості через збройну агресію РФ, спрямовану в тому числі на знищення цифрової інфраструктури. Забезпечення захищеності інформаційних систем об'єктів критичної інфраструктури та державних інформаційних кластерів потребує систематичного розвитку й постійного вдосконалення. Міжнародна практика, зокрема впровадження Будапештської конвенції та створення кіберпідрозділів, є основою для вдосконалення вітчизняного законодавства. Забезпечення ефективних правових механізмів виступає важливим елементом, який сприяє зміцненню національної безпеки та інтеграції України до європейського правового простору.

Аналіз останніх досліджень і публікацій. Дослідженням питання боротьби з кіберзлочинністю у вітчизняному та міжнародному просторі займалося чимало науковців. Значний внесок у цьому напряму зробили В. В. Шемчук[1], М. Ю. Якимчук[2], Ю. В. Гурзель[3], В. В. Аніщук[4], І. І.. Коцман[5], Б. М. Головкін та ін. Однак, незважаючи на свою розробленість, зазначене питання залишається відкритим і потребує додаткового опрацювання.

Метою цієї **статті** є комплексне і всебічне висвітлення проблем боротьби з кіберзлочинністю в межах вітчизняної і міжнародної практики. Виходячи із поставленої мети, головними завданням є: дослідити поняття кіберзлочинності та його основних елементів; розкрити правові механізми боротьби з кіберзлочинністю; охарактеризува-

[1] Шемчук В. В. 'Кіберзлочинність як перешкода розвитку інформаційного суспільства в Україні' (2018) 29 (68) 6 Вчені записки ТНУ імені В. І. Вернадського. Серія: юридичні науки 119–124. <https://www.juris.vernadskyjournals.in.ua/journals/2018/6_2018/23.pdf> (дата звернення 21.12.2024)

[2] Якимчук М. Ю. 'Особливості правового регулювання протидії кіберзлочинності в Україні: порівняльно-правовий аспект' (2021) 4 Нове українське право. 182–186 <http://newukrainianlaw.in.ua/index.php/journal/article/view/98/89> (дата звернення 24.12.2024)

[3] Гурзель Ю. В. 'Кіберзлочинність: основні причини та методи боротьби' *Протидія кіберзагрозам та торгівля людьми* (Харків, 2019) 49–51 <https://univd.edu.ua/general/publishing/konf/26_11_2019/pdf/12.pdf> (дата звернення 26.12.2024)

[4] Аніщук В. В., Зицик С. Г. 'Проблема протидії кіберзлочинності: порівняльно-правовий аналіз' (2024) 83 (3) Науковий вісник Ужгородського Національного Університету 19–23 <https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/07/4–2.pdf> (дата звернення 26.12.2024)

[5] Коцман І. І. 'Державне регулювання протидії кіберзлочинності в Україні: поняття та основні напрямки' (2024) 40 Публічне управління і адміністрування в Україні 245–252 <https://pag-journal.iei.od.ua/archives/2024/40–2024/43.pdf> (дата звернення 31.12.2024)

ти правові основи боротьби на міжнародному рівні та у вітчизняному просторі; розробити дієві механізми захисту секторів, які є найбільш вразливими до кібератак; узагальнити отримані результати та навести перспективи подальших досліджень.

Виклад основного матеріалу. Від початку повномасштабного вторгнення в Україні цифрова та інформаційна сфери зазнали значного впливу внаслідок зовнішніх втручань. У наукових колах кіберзлочини прийнято вважати правопорушеннями, які здійснюються в кіберпросторі з використанням спеціальних пристроїв (комп'ютерів, смартфонів, планшетів, терміналів тощо), автоматизованих систем, комп'ютерних мереж або мереж електрозв'язку, пов'язаних із незаконним створенням, зберіганням, обробкою, підробкою, блокуванням або знищенням елементів інформаційної інфраструктури. Загалом кіберзлочинність охоплює різні аспекти повсякденного життя, і будь-хто може стати її жертвою.

Боротьба з кіберзагрозами триває як на національному, так і на міжнаціональному рівні. Першими кроками боротьби із кіберзагрозами стало підписання у 2001 р. у Будапешті Конвенції про кіберзлочинність[1]. У підписанні взяло участь 35 країн (країни Ради Європи, а також Австралія, Домініканська Республіка, Японія, Панама, США). До теперішнього часу Конвенція залишається актуальним міжнародним договором, покликаним захищати людей та їх права від злочинів у цифровій мережі. Україна приєдналася до цієї Конвенції у 2005 р.

Підписання документа було зумовлене необхідністю співпраці між державами для розслідування або переслідування кримінальних правопорушень, пов'язаних з комп'ютерними системами та даними, а також для збору доказів в електронному форматі, оскільки кіберзлочини, як правило, мають транснаціональний характер.

Згідно з Конвенцією кіберзлочини класифікуються за такими категоріями як:

– правопорушення, що стосуються конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ до систем, нелегальне перехоплення інформації, втручання в дані та системи, створення, поширення та збут шкідливого програмного забезпечення та спеціальних пристроїв);

– правопорушення, пов'язані з комп'ютерами (комп'ютерне підроблення та комп'ютерне шахрайство);

– правопорушення, що стосуються змісту (створення, володіння, розповсюдження або передача дитячої порнографії через комп'ютерні системи);

– правопорушення, пов'язані з порушенням авторських прав і суміжних прав[2].

Як слушно зауважує В. В. Шемчук, кіберзлочинність є неминучим наслідком глобалізації інформаційних процесів. Вона становить значну загрозу суспільству, впливаючи на зміни, які в ньому відбуваються. Відповідно до Кримінального кодексу України[3] кіберзлочинність охоплює кримінальні правопорушення, пов'язані з:

– використанням електронно-обчислювальних машин (комп'ютерів), систем, комп'ютерних мереж і мереж електрозв'язку, які стосуються підготовки, здійснення або приховування злочинів, зокрема у сфері платіжних систем;

– обігом інформації протиправного характеру із залученням комп'ютерних систем, мереж або мереж електрозв'язку;

– господарськими відносинами та приватною власністю, зокрема незаконними фінансовими операціями та забороненими видами господарської діяльності, які здійснюються через комп'ютерні мережі або мережі електрозв'язку[4].

Ефективна боротьба з кіберзлочинністю має спрямовуватися на зміцнення економічних основ безпеки підприємств, установ та організацій, а також на активізацію низки заходів, пов'язаних із цією боротьбою. В умовах сучасного інформаційного суспільства, де кіберзагрози з кожним днем набувають загрозливого характеру через свою масштабність на негативний вплив на суспільство і національну безпеку, необхідно впроваджувати комплексні заходи з протидії кіберзлочинності.

Вітчизняна дослідниця М. Ю. Якимчук відзначає, що «у сучасному світі існує значна кількість

[1] Конвенція про кіберзлочинність від 23.11.2001 р. URL: http://zakon.rada.gov.ua/laws/ show/994_575 (дата звернення 24.12.2024)

[2] –

[3] Кримінальний кодекс України. Закон України від 05.04.2001. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341–14#Text

[4] Шемчук В. В. 'Кіберзлочинність як перешкода розвитку інформаційного суспільства в Україні' (2018) 29 (68) 6 Вчені записки ТНУ імені В. І. Вернадського. Серія: юридичні науки 121 <https://www.juris.vernadskyjournals.in.ua/journals/2018/6_2018/23.pdf> (дата звернення 26.12.2024)

видів кіберзлочинів, які можуть завдати значної шкоди. Серед них виокремлюють комп'ютерне шпигунство, поширення шкідливого програмного забезпечення, інтернет-шахрайство, дефейс, кібертероризм тощо. Особливе занепокоєння викликає те, що такі злочини здатні набувати масштабного характеру, загрожуючи міждержавній безпеці. Саме цей аспект є головним чинником активізації міжнародної співпраці у сфері протидії кіберзлочинності. Міжнародні організації, такі як Організація Об'єднаних Націй (ООН), Група восьми (G8), Рада Європи, Інтерпол, Організація економічного співробітництва і розвитку (ОЕСР), здійснюють заходи зі створення нормативно-правової бази для забезпечення ефективної взаємодії в галузі кібербезпеки»[1].

Інша дослідниця Ю. В. Гурзель говорить, що боротьба з кіберзлочинністю має здійснюватися на підставі правового розуміння інформаційних мереж. На думку авторки, головна причина кіберзлочинності полягає у значній прибутковості, оскільки ця сфера є надприбутковою і посідає третє місце за рівнем збагачення після торгівлі наркотиками та зброєю. Серед соціальних чинників впливу на суспільство варто виокремити зміни в суспільному житті, пов'язаними з комп'ютеризацією та формуванням інформаційного простору. Серед технологічних причин необхідно виокремити ті, які виникають в технічному просторі вчинення кіберзлочинів. Їх зміст полягає в тому, що хакери можуть в обхід захисту здійснити вторгнення в будь-яку мережу з метою заволодіння цінними даними. Політичні причини вчинення кіберзлочинів зазвичай пов'язані з прагненням вплинути на державну політику, дестабілізувати її, поширюючи ідеологічні погляди або дискредитуючи політичних опонентів. Кіберзлочини такого типу можуть включати хакерські атаки на урядові сайти, викрадення конфіденційної інформації, заволодіння конфіденційними даними з метою втручання у вибори або навіть з метою здійснення актів кібертероризму для залякування населення чи завдання шкоди критично важливій інфраструктурі. В умовах глобалізації та розвитку інформаційних технологій кіберзлочини з політичних мотивів є особливо небезпечними, оскільки вони можуть мати транскордонний характер і впливати на міжнародну безпеку[2].

Державне регулювання протидії кіберзлочинності спрямоване на формування безпечного кіберпростору шляхом реалізації правових, технічних та організаційних заходів, що забезпечують захист держави, бізнесу та громадян від кіберзагроз. Цей процес є багаторівневим і включає правові, адміністративні, технологічні аспекти, а також міжнародну співпрацю. Регулювання охоплює не лише створення та впровадження правових норм, а й постійне вдосконалення технологій кіберзахисту, розвиток превентивних заходів і розширення взаємодії з іншими країнами. Держава має відігравати провідну роль у побудові ефективної системи захисту інформаційних систем та протидії новітнім загрозам у цифровому просторі. З огляду на це у жовтні 2017 р. було прийнято Закон України «Про основні засади забезпечення кібербезпеки України»[3], який визначає правові й організаційні основи захисту ключових інтересів людини, суспільства та держави у кіберпросторі. Цей Закон регламентує основні напрями, цілі та принципи державної політики у сфері кібербезпеки, а також встановлює повноваження органів державної влади, підприємств, установ, організацій і громадян у цій галузі, закладає основи координації дій із забезпечення кібербезпеки. Згідно зі ст. 1 цього Закону кіберзлочинність охоплює всі кіберзлочини[4]. Кіберзлочином вважається суспільно небезпечне, винне діяння, вчинене у кіберпросторі або за його використанням, за яке передбачена кримінальна відповідальність відповідно до законодавства України чи яке визнане злочином міжнародними угодами України.

Окрім Закону «Про основні засади забезпечення кібербезпеки України»[5], до національного законодавства у цій сфері входять такі нормативно-правові акти, як Конституція України, Кримінальний кодекс України, а також закони «Про інформацію», «Про національну безпеку України», «Про захист

[1] Якимчук М. Ю. 'Особливості правового регулювання протидії кіберзлочинності в Україні: порівняльно-правовий аспект' (2021) 4 Нове українське право. 183 <http://newukrainianlaw.in.ua/index.php/journal/article/view/98/89> (дата звернення 29.12.2024)

[2] Гурзель Ю. В. 'Кіберзлочинність: основні причини та методи боротьби' *Протидія кіберзагрозам та торгівля людьми* (Харків. 2019) 49. <https://univd.edu.ua/general/publishing/konf/26_11_2019/pdf/12.pdf> (дата звернення 29.12.2024)

[3] Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII URL: https://zakon.rada.gov.ua/laws/show/2163–19 (дата звернення 30.12.2024)

[4] –

[5] –

інформації в інформаційно-телекомунікаційних системах» та ін. Питаннями кібербезпеки та протидії кіберзлочинності, крім кіберполіції, займаються різні державні органи, зокрема Державна служба спеціального зв'язку та захисту інформації, Служба безпеки України, Міністерство внутрішніх справ України тощо. Суб'єкти, що здійснюють боротьбу з кіберзлочинністю, повинні формувати інтегровану систему як з організаційної, так і з функціональної точок зору. Проте статистика щодо рівня кіберзлочинів в Україні свідчить, що існуючі заходи з їх попередження не є достатньо ефективними[1].

Дослідник І. І. Коцман зазначає, що «ефективна боротьба з кіберзлочинністю потребує не лише правового регулювання, а й створення та забезпечення діяльності спеціалізованих державних органів, які займалися б протидією таким злочинам. У багатьох країнах функціонують спеціалізовані підрозділи у складі правоохоронних органів, що займаються розслідуванням кіберзлочинів. Ці підрозділи оснащені сучасними технічними та аналітичними засобами, які дозволяють виявляти, відслідковувати й нейтралізовувати загрози в кіберпросторі. В Україні, зокрема, діє Департамент кіберполіції Національної поліції України, який є міжрегіональним територіальним підрозділом у складі кримінальної поліції. Відповідно до чинного законодавства цей департамент здійснює оперативно-розшукову діяльність, спрямовану на боротьбу з кіберзлочинами.

На офіційному сайті Департаменту кіберполіції окреслено такі основні напрями діяльності цього підрозділу, зокрема:

– впровадження державної політики у сфері протидії кіберзлочинності;

– своєчасне інформування громадськості про появу нових кіберзагроз;

– розробка та використання програмних засобів для систематизації кіберінцидентів;

– реагування на запити міжнародних партнерів через національну цілодобову мережу контактних пунктів.

Разом із тим існуючі завдання кіберполіції потребують перегляду та вдосконалення, зважаючи на появу нових форм кіберзлочинів та методів їх реалізації»[2].

Важливо наголосити, що кіберзлочинність є значною проблемою, що має транснаціональний характер і виходить далеко за межі окремих країн. Зважаючи на це, важливим кроком є гармонізація міжнародного та національного законодавства у сфері протидії кіберзлочинності, що передбачає внесення відповідних змін до кримінального й кримінального процесуального законодавства України. Це зумовлено наявністю низки проблем, що виникають під час досудового розслідування кіберзлочинів і судового розгляду справ та пов'язані з оцінкою електронних доказів судами.

Наразі науковці працюють над вдосконаленням кіберпростору і над питаннями кіберзахисту, оскільки збереження конфіденційних даних є прерогативою національної безпеки будь-якої держави. Міжнародне співтовариство приділяє значну увагу питанням захисту від кіберзагроз. У сучасних умовах багато науковців, політиків і глав держав акцентують увагу на важливості протидії цьому виду злочинності. Активні зусилля спрямовані на подолання кіберзлочинів та розбудову ефективних міжнародних механізмів захисту від них. Однією із головних особливостей кіберзлочинності є транснаціональний характер, який означає, що злочини часто здійснюються в одній країні, тоді як їх жертви перебувають в іншій. Правоохоронні органи окремої держави не можуть ефективно проводити досудове розслідування кіберзлочинів, якщо злочинці та ключові докази знаходяться за межами їх юрисдикції. У такому випадку вирішальну роль відіграє міжнародна співпраця. Важливо, щоб у країні, до якої надходить запит на екстрадицію або правову допомогу у розслідуванні зазначеного кримінального правопорушення, відповідне діяння також визнавалося злочином. Лише за умови ефективної співпраці можна досягнути бажаного результату і вплинути на рівень боротьби з кіберзлочинністю як на національному, так і на міжнародному рівнях, забезпечуючи своєчасне реагування на загрози, обмін інформацією та координацію зусиль у протидії цій проблемі глобального масштабу.

[1] Аніщук В. В., Зицик С. Г. 'Проблема протидії кіберзлочинності: порівняльно-правовий аналіз' (2024) 83 (3) Науковий вісник Ужгородського Національного Університету 20 <https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/07/4–2.pdf> (дата звернення 28.12.2024)

[2] Коцман І. І. 'Державне регулювання протидії кіберзлочинності в Україні: поняття та основні напрямки' (2024) 40 Публічне управління і адміністрування в Україні 248 <https://pag-journal.iei.od.ua/archives/2024/40–2024/43.pdf> (дата звернення 30.12.2024)

Міжнародно-правове співробітництво у боротьбі з кіберзагрозами має здійснюватися у чіткій відповідності до норм вітчизняного законодавства. Лише посилена співпраця може дати свої плоди і забезпечити ефективну боротьбу в подоланні кіберзагроз. Оскільки кіберзагрози впливають на транснаціональну безпеку, важливо зосередити увагу на розвитку кібербезпекової інфраструктури, зокрема на захисті критичних інформаційних систем, розробці освітніх програм для підвищення рівня обізнаності громадян, проведенні відповідного навчання і підвищення кваліфікації фахівців кіберсектору. Окрім того, інвестування в дослідження та розробка у сфері кіберзахисту передбачає використання нових методів шифрування, створення систем виявлення потенційних загроз, а також низки інших заходів, що сприяють захисту кіберпростору від загроз. Досить важливо також розвивати й публічно-приватне партнерство, оскільки воно сприяє взаємодії та швидкому реагуванню на кібератаки і їх ефективну боротьбу.

Ще одним кроком у боротьбі з кіберзагрозами є попередження та профілактика кіберзлочинів. Боротьба в цьому напряму є ключовим елементом державної політики, оскільки охоплює комплекс заходів, спрямованих на зниження кількості кіберзлочинів і зменшення пов'язаних із ними ризиків. Насамперед важливо організовувати інформаційно-просвітницькі кампанії, які підвищуватимуть обізнаність населення та сприятимуть формуванню навичок кібергігієни. Серед базових правил – використання надійних паролів, регулярне оновлення програмного забезпечення та обережність у процесі роботи в Інтернеті.

Бізнес-сектор також має приділяти увагу навчальним тренінгам із питань запобігання фішинговим атакам і витоку даних та питань ефективного реагування на кіберзагрози. Освітні програми повинні бути доступними для всіх вікових категорій, сприяючи кращому розумінню небезпечного впливу кіберзагроз, методів захисту інформації та основних правил безпечного користування цифровими технологіями.

Захист критичної інфраструктури є одним із ключових елементів профілактики кіберзлочинності. Держава повинна гарантувати безпеку стратегічно важливих об'єктів, таких як енергетичні компанії, банки, транспортні системи та державні установи. Важливим завданням є впровадження національних стандартів кібербезпеки та використання сучасних технологій, що ускладнюють здійснення кібератак. Окрім фізичного захисту серверів, потрібно забезпечувати постійний моніторинг кіберпростору з метою своєчасного виявлення загроз і реагування на них.

Аудит та моніторинг інформаційних систем – важливі заходи протидії кіберзлочинності. Державні та приватні організації повинні регулярно аналізувати свої інформаційні системи для виявлення вразливостей, що досягається шляхом проведення аудитів із залученням експертів із кібербезпеки. Особливу увагу слід приділяти оновленню систем захисту, адже технології швидко змінюються, а тому нові кіберзагрози виникають постійно. Належний моніторинг мереж організацій дозволяє оперативно виявляти кіберзагрози та нейтралізувати їх ще до того, як вони зможуть завдати серйозних проблем.

Важливим інструментом є впровадження систем управління інформаційною безпекою, що дозволяє підвищити ефективність реагування на кіберінциденти. Превентивні заходи на державному рівні також мають суттєве значення, включаючи не лише впровадження законодавчих норм, а й розробку стратегій для зниження ризику кіберзлочинів. Це передбачає створення систем раннього виявлення загроз, розвиток кіберрозвідки та налагодження міжнародної співпраці для обміну інформацією про кіберзагрози. Такий комплексний підхід дозволить посилити захист національної та міжнародної кібербезпеки.

Висновки. Боротьба з кіберзлочинністю зумовлена комплексним підходом, який містить вдосконалення законодавства, розвиток технічних засобів кіберзахисту та активізацію міжнародної співпраці. Світова практика кіберборотьби визначається доцільністю гармонізації національних норм у відповідності до міжнародних стандартів, втілених в нормативно-правових актах, зокрема таких, як Будапештська конвенція, що забезпечує єдині підходи до протидії кіберзагрозам. В Україні необхідно підсилити реалізацію існуючих правових механізмів, зокрема через впровадження систем раннього виявлення загроз і посилення відповідальності за кіберзлочини. Важливим аспектом є також підвищення цифрової грамотності населення та бізнесу, що здатне мінімізувати ризики майбутніх кіберзагроз.

Подальші дослідження повинні спрямовуватися на розробку ефективних моделей міжнародного співробітництва, аналіз впливу кіберзлочинності на економічну та соціальну стабільність, а також інтеграцію новітніх технологій у систему кіберзахисту. Особливу увагу необхідно приділяти вивченню практичної реалізації національних програм у сфері кібербезпеки та їх відповідності сучасним викликам.

REFERENCES

List of legal documents

Legislation

1. Kryminalnyi kodeks Ukrainy: Zakon vid 05.04.2001 №2341III. URL: http://surl.li/hwcs (in Ukrainian)
2. Convention on Cybercrime of November 23, 2001. URL: http://zakon.rada.gov.ua/laws/show/994_575.
3. On the Basic Principles of Cybersecurity in Ukraine: Law of Ukraine from 5 October 2017, No. 2163-VIII URL: https://zakon.rada.gov.ua/laws/show/2163–19 (in Ukrainian).

Bibliography

Journal articles

1. Shemchuk V. V., ’Kiberzlochynnist yak pereshkoda rozvytku informatsiinoho suspil′stva v Ukraini’ [Cybercrime as an Obstacle to the Development of the Information Society in Ukraine] (2018) 6 Vcheni zapysky TNU imeni V. I. Vernads′koho. Seriia: iurydychni nauky 119–124 <https://www.juris.vernadskyjournals.in.ua/journals/2018/6_2018/23.pdf> (in Ukrainian).
2. Yakymchuk M. Yu., ’Osoblyvosti pravovoho rehuliuvannia protydii kiberzlochynnosti v Ukraini: porivnial′no-pravovyi aspekt’ [Peculiarities of Legal Regulation of Counteracting Cybercrime in Ukraine: A Comparative Legal Aspect] (2021) 4 Nove ukrainske pravo 182–186 <http://newukrainianlaw.in.ua/index.php/journal/article/view/98/89> (in Ukrainian).
3. Hurzel Yu. V., ’Kiberzlochynnist: osnovni prychyny ta metody borot′by’ [Cybercrime: Main Causes and Methods of Combating*] in Protydiia kyberzahrozam ta torhivlia liudmy* (Kharkiv, 2019) 49–51 <https://univd.edu.ua/general/publishing/konf/26_11_2019/pdf/12.pdf> (in Ukrainian)
4. Anishchuk V. V., Zytsyk S. H., ’Problema protydii kiberzlochynnosti: porivnial′no-pravovyi analiz’ [The Problem of Counteracting Cybercrime: A Comparative Legal Analysis] (2024) 83:3 Naukovy visnyk Uzhhorods′koho Natsional′noho Universytetu 19–23<https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/07/4–2.pdf> (in Ukrainian).
5. Kotsman I. I., ’Derzhavne rehuliuvannia protydii kiberzlochynnosti v Ukraini: poniattia ta osnovni napriamky’ [State Regulation of Counteracting Cybercrime in Ukraine: Concept and Main Directions] (2024) 40 Publ′chne upravlinnia i administruvannia v Ukraini 245–252 <https://pag-journal.iei.od.ua/archives/2024/40–2024/43.pdf> (in Ukrainian).

Гончарук В. Л.

Правові механізми боротьби з кіберзлочинністю: світова практика та український контекст

У статті досліджуються питання боротьби з кіберзлочинністю, зокрема світова практика та український контекст. Багато років поспіль кіберзлочинність залишається однією з найактуальніших проблем у сфері безпеки,відтак, потребує комплексного підходу до її вирішення. Шкода, завдана кібератаками, впливає на безпеку держави і добробут громадян.

Головна увага звернена на те, що кібератаки паралізують роботу критичної інфраструктури, в тому числі енергетичної мережі, транспортних систем, банківських установ та державних сервісів. Це призводить до економічних втрат і дестабілізації суспільного життя. Витік персональних даних громадян може спричинити фінансові втрати, шахрайство та підрив довіри до цифрових сервісів. Підприємства зазнають значних збитків через порушення їх діяльності, втрату конфіденційної інформації та піддаються чималим витратам у процесі відновлення. Окрім економічного аспекту, кібератаки відзначаються значним психологічним впливом, провокуючи відчуття небезпеки, недовіри до державних і приватних структур, а також підривають стабільність всього суспільства.

Зазначено, що правові механізми захисту від кіберзагроз на національному та міжнародному рівнях – це головні елементи, які сприяють забезпеченню безпеки в сучасному цифровому середовищі. Національні механізми протидії кіберзлочинності ґрунтуються на впровадженні спеціалізованого законодавства, яке регулює відповідальність за вчинення кіберзлочинів, визначає основні принципи забезпечення кібербезпеки та координує діяльність відповідних структур, у тому числі й кіберполіції. На міжнародному рівні ключову роль відіграє співпраця держав

у рамках міжнародних угод, таких як Будапештська конвенція про кіберзлочинність, якою встановлюються універсальні стандарти протидії цьому виду правопорушень.

Зроблено висновок, що важливим аспектом наразі залишається гармонізація вітчизняного законодавства у відповідності до міжнародних норм, що сприяє посиленню взаємодії між країнами в процесі запобігання, розслідування та притягнення до відповідальності за кіберзлочини. Таким чином, багаторівневий підхід, що охоплює вітчизняні та міжнародні механізми, є визначальним для створення комплексної системи захисту від різних видів кіберзагроз.

Ключові слова: *кібератаки, кіберзагрози, протидія, правові механізми, міжнародне співробітництво, Будапештська конвенція, кіберполіція, критична інфраструктура, персональні дані.*

Honcharuk V. L.

Legal mechanisms for combating cybercrime: global practice and the Ukrainian context

The article examines the issue of combating cybercrime, in particular global practice and the Ukrainian context. For many years, cybercrime has remained one of the most pressing problems in the security sector, and therefore requires a comprehensive approach to its solution. The damage caused by cyberattacks affects the security of the state and the well-being of citizens.

The main attention is paid to the fact that cyberattacks paralyze the work of critical infrastructure, including the energy network, transport systems, banking institutions and government services. This leads to economic losses and destabilization of public life. The leakage of citizens' personal data can cause financial losses, fraud and undermining trust in digital services. Enterprises suffer significant losses due to disruption of their activities, loss of confidential information and are subject to considerable costs in the recovery process. In addition to the economic aspect, cyberattacks have a significant psychological impact, provoking a sense of danger, distrust of state and private structures, and undermining the stability of the entire society.

It is noted that legal mechanisms for protection against cyber threats at the national and international levels are the main elements that contribute to ensuring security in the modern digital environment. National mechanisms for combating cybercrime are based on the implementation of specialized legislation that regulates liability for committing cybercrimes, defines the basic principles of ensuring cybersecurity and coordinates the activities of relevant structures, including cyberpolice. At the international level, cooperation between states within the framework of international agreements, such as the Budapest Convention on Cybercrime, which establishes universal standards for combating this type of offense, plays a key role.

It is concluded that an important aspect at present remains the harmonization of domestic legislation in accordance with international norms, which contributes to strengthening cooperation between countries in the process of preventing, investigating and prosecuting cybercrimes. Thus, a multi-level approach, encompassing domestic and international mechanisms, is crucial for creating a comprehensive system of protection against various types of cyber threats.

Keywords: *cyberattacks, cyber threats, countermeasures, legal mechanisms, international cooperation, Budapest Convention, cyber police, critical infrastructure, personal data*

Стаття надійшла до редакції: 14.01.2025 р.
Прийнята до друку: 20.06.2025 р.