https://doi.org/10.26565/2075-1834-2026-41-25
УДК 343.9:004

ПУЗИРНА Н. С.
кандидат юридичних наук, доцент,
доцент кафедри публічного та приватного права
E-mail: 1981-natasha@ukr.net ORCID: https://orcid.org/0000-0002-7297-0829
Національний університет «Чернігівська Політехніка»
м. Чернігів, 14027, Шевченка, 95

ПАДАЛКА В. О.
здобувач вищої освіти першого бакалаврського рівня
4 курсу групи КЮ-222
E-mail: vladpadalka17@gmail.com ORCID: https://orcid.org/0009-0006-2623-8078
Національного університету «Чернігівська політехніка»
м. Чернігів, 14027, Шевченка, 95

КІБЕРЗЛОЧИННІСТЬ: КРИМІНАЛЬНО-ПРАВОВА ХАРАКТЕРИСТИКА ТА ПРОТИДІЯ

АНОТАЦІЯ. *Вступ.* У статті досліджено проблему кіберзлочинності як однієї з найбільш динамічних та транснаціональних загроз сучасного суспільства. Актуальність теми зумовлена стрімкою цифровізацією суспільних відносин, зростанням кількості кримінальних правопорушень у кіберпросторі та необхідністю вдосконалення кримінально-правових механізмів протидії таким посяганням, особливо в умовах воєнного стану. Метою статті є здійснення комплексного кримінально-правового аналізу кіберзлочинності, виявлення прогалин чинного законодавства та формування пропозицій щодо підвищення ефективності протидії. У дослідженні використано загальнонаукові та спеціально-юридичні методи пізнання, зокрема формально-логічний, системно-структурний, порівняльно-правовий та аналіз нормативних джерел.

Короткий зміст. У роботі проаналізовано положення Конвенції про кіберзлочинність 2001 року, норми Розділу XVI Кримінального кодексу України та Закону України «Про основні засади забезпечення кібербезпеки України». Розкрито елементи складів кримінальних правопорушень у сфері використання інформаційних технологій, окреслено проблеми їх практичного застосування та визначення поняття кіберзлочину. Обґрунтовано необхідність удосконалення законодавства з урахуванням сучасних технологічних викликів та міжнародного досвіду. Запропоновано інноваційну концепцію «кіберімунітету», що передбачає впровадження механізмів «кібервакцинації», «кіберлейкоцитів» і «кіберпам'яті» як засобів превентивної протидії кіберзагрозам.

Висновок. У висновках наголошено, що ефективна протидія кіберзлочинності можлива лише за умови комплексного підходу, який поєднує вдосконалення кримінального законодавства, розвиток технологічних засобів захисту, підвищення рівня кіберграмотності населення та активне міжнародне співробітництво. Запропоновані підходи можуть слугувати підґрунтям для подальших наукових досліджень і практичних реформ у сфері забезпечення кібербезпеки.

КЛЮЧОВІ СЛОВА: *кіберзлочинність, кримінально-правова характеристика, кібербезпека, кримінальний кодекс України, протидія кіберзлочинам.*

Як цитувати: Пузирна Н. С., Падалка В. О. Кіберзлочинність: кримінально-правова характеристика та протидія. *Вісник Харківського національного університету імені В. Н. Каразіна, серія «Право».* 2026. Вип. 41. С. 278-284. https://doi.org/10.26565/2075-1834-2026-41-25

In cites: N. S. Puzyrna, V. O. Padalka (2026) Cybercrime: criminal law characteristics and countermeasures. *The Journal of V.N. Karazin Kharkiv National University, Series "Law"*, (41), P. 278-284. https://doi.org/10.26565/2075-1834-2026-41-25 (in Ukrainian)

Постановка проблеми. У сучасному світі, де інформаційні технології проникають у всі сфери життя, кіберзлочинність стає серйозною загрозою для особистості, суспільства та держави. Зловживання цифровими технологіями з метою вчинення злочинів набуває транснаціонального характеру, завдаючи значної матеріальної та моральної шкоди.

У зв'язку з цим, питання кримінально-правової характеристики кіберзлочинності та ефективної протидії їй є надзвичайно актуальним. Кіберзлочинність є однією з найбільш актуальних та швидкозростаючих загроз сучасності. Вона характеризується транснаціональним характером, високою латентністю та постійним розвитком нових форм і методів. У зв'язку з цим, проблема кіберзлочинності потребує комплексного кримінально-правового аналізу та розробки ефективних механізмів протидії.

Стан наукового дослідження теми. Стан наукового дослідження теми кримінально-правової характеристики кіберзлочинності характеризується значним масивом напрацювань, над якими працювали такі вчені, як Вергун Л. О., Галушко П. П., Гарига М. М., Думчиков М. О., Захарченко А. Є., Каменський Д. В., Ковальчук Д. В., Корзун С. В., Кришевич О. В., Кузнєцов О. О., Нагірний І. П., Попко В. В., Попко Є. В., Рощина І. О., Ткаченко А. О. та Ткаченко П. І. Їхні роботи заклали фундаментальну базу для розуміння природи цифрових правопорушень у сучасних умовах.

Окремої уваги заслуговують наукові розвідки, у яких ґрунтовно розкрито елементи кримінально-правової характеристики кіберзлочинів та запропоновано вектори вдосконалення системи протидії їм. Важливий внесок у дослідження зробив Думчиков М. О., який детально проаналізував відмінності між злочинами у сфері комп'ютерної інформації та злочинами, що скоєні з використанням комп'ютерних технологій, наголошуючи на їхній нетотожності. Автор підкреслив, що чинне законодавство України не охоплює повний спектр викликів у кіберпросторі, та представив класифікацію кіберзлочинів відповідно до Конвенції про кіберзлочинність 2001 року, виокремивши вектори вдосконалення нормативно-правового регулювання [1, с. 66].

У праці Ткаченка П. І., Ткаченка А. О. та Ковальчука Д. В. основну увагу приділено питанням визначення поняття кіберзлочинності та необхідності гармонізації вітчизняного законодавства з міжнародними стандартами. Водночас науковці зазначають, що проблемам практичного застосування кримінально-правових норм у реальних судових та слідчих процесах наразі приділено недостатньо уваги, що створює певний вакуум між теорією та практикою [2, с. 280].

Кримінально-правові аспекти цієї сфери стали об'єктом детального вивчення Гариги М. М., Вергун Л. О. та Кузнєцова О. О., які зосередилися на специфіці кваліфікації відповідних діянь [3, с. 90]. Паралельно з цим Захарченко А. Є. та Каменський Д. В. акцентують увагу на недоліках сучасного законодавства у частині визначення складів правопорушень, пов'язаних із незаконним використанням ІТ, пропонуючи розширити положення Кримінального кодексу України для охоплення нових видів кіберзлочинів, що поки не мають чіткої правової оцінки [4, с. 109].

Незважаючи на ґрунтовність теоретичних розробок, практичні методи безпосередньої боротьби із кіберзлочинністю залишаються недосконалими. Більшість наявних робіт фокусується на термінологічному апараті та аналізі чинних норм, проте спостерігається гострий брак досліджень щодо вдосконалення юридичних інструментів запобігання злочинам та розробки ефективних механізмів їхнього застосування в умовах воєнного стану та тотальної цифровізації суспільства.

Мета дослідження. Провести комплексний кримінально-правовий аналіз кіберзлочинності, виявити проблемні аспекти чинного законодавства та практики його застосування, а також розробити пропозиції щодо удосконалення механізмів протидії кіберзлочинності.

Основні результати дослідження. Кіберзлочинність завдає значної шкоди особистим, суспільним та державним інтересам. Вона може призвести до втрати конфіденційної інформації, фінансових втрат, порушення роботи критичної інфраструктури та навіть загрози національній безпеці. Тому розробка ефективних кримінально-правових механізмів протидії кіберзлочинності є надзвичайно важливою для забезпечення сталого розвитку суспільства та захисту прав громадян.

Правове регулювання даного питання здійснюється такими нормативно-правовими актами: 1) Конвенція про кіберзлочинність [5] (Ратифікована 07.09.2005р.). Конвенція про кіберзлочинність є першим міжнародним treaty, що стосується криміналізації кіберзлочинів. Вона була розроблена Радою Європи та відкрита для підписання у 2001 році. Метою Конвенції є гармонізація національного законодавства у сфері боротьби з кіберзлочинністю, спрощення міжнародного співробітництва у розслідуванні та переслідуванні кіберзлочинів, а також захист прав людини та основоположних свобод в умовах розвитку інформаційних технологій.

Конвенція містить перелік діянь, які держави-учасниці зобов'язані криміналізувати, зокрема, незаконний доступ до комп'ютерних систем, незаконне перехоплення даних, пошкодження або знищення даних, виготовлення та розповсюдження шкідливого програмного забезпечення, підробка документів, що зберігаються в комп'ютерній системі, шахрайство пов'язане з використанням комп'ютерів.

2) Кримінальний кодекс України (далі – КК України) [6]. Для більш детального розуміння кримінально-правової характеристики кіберзлочинів, розглянемо порівняльну таблицю складів кримінальних правопорушень, передбачених Розділом XVI КК України. Табл. 1

Табл. 1
Порівняльна таблиця складів кримінальних правопорушень передбачених Розділом XVI КК України

Елементи	**Стаття 361. Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж**	**Стаття 361^{-1}. Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут**	**Стаття 361^{-2}. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації**	**Стаття 362. Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї**	**Стаття 363. Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється**	**Стаття 363^{-1}. Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку**
Об'єкт	Інформаційна (автоматизована), електронна комунікаційна, інформаційно-комунікаційна система, електронна комунікаційна мережа	Шкідливі програми чи технічні засоби	Інформація з обмеженим доступом	Інформація, яка обробляється в ЕОМ, автоматизованих системах, комп'ютерних мережах	ЕОМ, автоматизовані системи, комп'ютерні мережі чи мережі електрозв'язку або порядок чи правила захисту інформації	ЕОМ, автоматизовані системи, комп'ютерні мережі чи мережі електрозв'язку
Об'єктивна сторона	Несанкціонована не втручання	Створення, розповсюдження або збут шкідливих програм чи технічних засобів	Несанкціоновані збут або розповсюдження інформації	Несанкціоновані дії з інформацією особою, яка має право доступу до неї	Порушення правил експлуатації або порядку чи правил захисту інформації	Перешкоджання роботі шляхом масового розповсюдження повідомлень
Суб'єкт	Загальний - 16 років	Загальний - 16 років	Загальний - 16 років	Особа, яка має право доступу до інформації	Особа, відповідальна за експлуатацію	Загальний - 16 років
Суб'єктивна сторона	Умисел	Умисел	Умисел	Умисел	Умисел або необережність	Умисел

3) Закон України «Про основні засади забезпечення кібербезпеки України» [7]. Даний закон в ст. 1 містить легальне визначення кіберзлочину (комп'ютерний злочин) - суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [7].

Щодо визначення кіберзлочину в науці кримінального права та серед науковців немає єдиної думки. До прикладу Думчиков М. О., визначає кіберзлочини, як умисні, суспільно

небезпечні та протиправні діяння, які порушують встановлений порядок обігу, використання та захисту інформації в кіберпросторі, завдаючи шкоди суспільним відносинам [4, с. 66].

Така багатоаспектність термінології зумовлює необхідність звернення до міжнародного досвіду, оскільки кіберзлочинність за своєю природою не має державних кордонів. Уніфікація підходів до кваліфікації цих діянь є критично важливою для налагодження транскордонного співробітництва правоохоронних органів.

Відповідно до міжнародних норм, національного законодавства України та Європейського Союзу, кіберзлочини, вчинені за попередньою змовою групою осіб, є серйозними правопорушеннями. Це підтверджує важливість неперервної боротьби з такими злочинами шляхом розробки та впровадження ефективних міжнародних стратегій та механізмів [5, с. 281]. На нашу думку, важливим елементом таких стратегій є розуміння специфіки об'єктів нападу та кола осіб, які зазнають найбільших збитків унаслідок протиправних дій у цифровій сфері. Статистика свідчить, що концентрація капіталу та критичних даних у корпоративному секторі робить його пріоритетною ціллю для кіберзлочинців.

Окрім цього слід зазначити що потерпілими від кіберзлочинів найчастіше є юридичні особи. Це зумовлено тим, що процес комп'ютеризації широко охоплює, насамперед, юридичних осіб (організації, установи), а значно меншою мірою – фізичних осіб [6, с. 97].

Разом із тим, сучасні виклики, перед якими постала Україна, змушують розглядати проблему не лише через призму економічних інтересів, а й з позиції національної безпеки. Особливої гостроти це питання набуває в умовах збройної агресії, коли кібератаки стають частиною гібридної війни. Повертаючись до питання кримінально-правових засобів протидії кіберзлочинності, то в період воєнного стану підлягають застосуванню положення КК України, які встановлюють відповідальність за кіберзлочини, зокрема, статті Розділ XVI КК України [7, с. 110].

Проте, незважаючи на наявність спеціального розділу в КК України, динаміка розвитку ІТ-технологій значно випереджає швидкість законотворчого процесу. Це створює ситуації, коли новітні способи втручання в інформаційні системи залишаються поза межами належної юридичної оцінки. Незважаючи на значний прогрес у боротьбі з кіберзлочинністю, чимало її видів досі не мають належного правового регулювання на національному рівні. Для ефективної протидії цьому явищу необхідна розробка та впровадження комплексних кримінально-правових механізмів.

По-перше, ефективна боротьба з кіберзлочинністю починається з міцного законодавчого фундаменту. Удосконалення законодавства у сфері кібербезпеки є критично важливим для того, щоб йти в ногу зі швидко розвиваючими технологіями та методами кіберзлочинців. Закони повинні чітко визначати кіберзлочини, встановлювати відповідні покарання за них та забезпечувати правоохоронним органам необхідні інструменти для розслідування та переслідування кіберзлочинців. Міжнародне співробітництво у цій сфері також є життєво важливим, оскільки кіберзлочини часто мають транскордонний характер. Угоди про взаємну правову допомогу та екстрадицію злочинців можуть допомогти у боротьбі з кіберзлочинністю на глобальному рівні.

По-друге технології відіграють ключову роль у захисті від кіберзлочинів. Розробка та впровадження сучасних технологій захисту інформації, таких як firewalls, антивірусне програмне забезпечення, системи виявлення вторгнень та інші засоби кібербезпеки, є необхідними для запобігання кібератакам та захисту даних. Важливо зазначити, що технології захисту повинні постійно оновлюватися та вдосконалюватися, щоб відповідати новим викликам та загрозам. Крім того, важливо забезпечити належне використання цих технологій та навчання персоналу правилам кібербезпеки.

По-третє підвищення рівня обізнаності населення про кібербезпеку є критично важливим для запобігання кіберзлочинам. Люди повинні бути навчені правилам безпечної поведінки в інтернеті, таким як використання складних паролів, обережність у відкритті електронних листів та переході за посиланнями, захист особистих даних тощо. Проведення інформаційних кампаній, семінарів та тренінгів з кібербезпеки може допомогти підвищити рівень обізнаності населення та зменшити кількість жертв кіберзлочинів.

По-четверте ефективна боротьба з кіберзлочинністю неможлива без сильних та професійних правоохоронних органів. Створення спеціалізованих підрозділів з боротьби з кіберзлочинністю, навчання співробітників правоохоронних органів методам розслідування кіберзлочинів та використання сучасних технологій для ідентифікації та переслідування кіберзлочинців є необхідними для забезпечення правопорядку у кіберпросторі.

По-п'яте кіберзлочинність часто має транскордонний характер, тому міжнародне співробітництво є критично важливим для боротьби з нею. Обмін інформацією та досвідом між країнами, проведення спільних операцій з метою боротьби з кіберзлочинністю, а також розробка та впровадження міжнародних стандартів кібербезпеки можуть допомогти у боротьбі з кіберзлочинністю на глобальному рівні.

На основі проведеного аналізу існуючих механізмів протидії кіберзлочинам, ми пропонуємо нову концепцію. Ідея, якої полягає у створенні системи, яка б не просто реагувала на кіберзагрози, а й активно запобігала їм, подібно до того, як імунна система людини бореться з хворобами.

Для ефективної протидії кіберзлочинності пропонуємо застосувати інноваційні підходи, такі як «Кібервакцинація», «Кіберлейкоцити» та «Кіберпам'ять». «Кібервакцинація» передбачає розробку програмних засобів, що «тренують» системи на розпізнавання та нейтралізацію відомих кіберзагроз шляхом симуляції атак, аналізу поведінки шкідливого програмного забезпечення та постійного оновлення баз даних загроз. «Кіберлейкоцити» - це автономні програмні агенти, які постійно моніторять мережі та системи на наявність підозрілої активності та автоматично ізолюють уражені ділянки для нейтралізації загрози. «Кіберпам'ять» - це система накопичення та аналізу інформації про кібератаки для виявлення нових тенденцій, прогнозування майбутніх загроз та вдосконалення механізмів захисту.

Серед переваг цієї концепції можна виділити те, що замість пасивного реагування на атаки система активно запобігає їм, забезпечуючи випереджувальний захист інформаційних ресурсів. Важливою характеристикою є також її здатність до самонавчання та адаптації до нових видів загроз, що дозволяє ефективно протидіяти динамічним кібервикликам у реальному часі. Крім того, впровадження такого підходу сприяє суттєвому зменшенню потреби у ручному втручанні та мінімізації впливу людського фактора, що значно підвищує надійність і швидкість функціонування механізмів кібербезпеки.

Успіх цього механізму залежатиме від тісної співпраці між державними органами (фінансування, законодавче середовище, обмін інформацією), приватним сектором (участь у розробці, інвестування, обмін інформацією) та науковою спільнотою (фундаментальні дослідження, розробка методів, підготовка фахівців). Тільки завдяки спільним зусиллям можливо створити ефективну систему протидії кіберзлочинності. «Кіберімунітет» може стати новим етапом у боротьбі з кіберзлочинністю, забезпечуючи більш надійний та ефективний захист від кіберзагроз.

Висновки. У ході дослідження було проведено комплексний кримінально-правовий аналіз кіберзлочинності, що дозволило виокремити ключові проблеми в чинному законодавстві та використовувати можливості напряму його вдосконалення.

По-перше, кіберзлочинність є однією з найбільших динамічних загроз сучасності. Вона має транснаціональний характер, високий рівень латентності та постійно розвивається, що ускладнює її ефективне правове регулювання. Враховуючи збільшення кількості кіберзлочинців, їхня профілактика та розслідування стають пріоритетними завданнями як для правоохоронних органів, так і для держави в цілому.

По-друге, аналіз норм кримінального законодавства України розроблений про те, що хоча воно містить положення щодо боротьби з кіберзлочинністю, вони не охоплюють весь спектр загроз. Особливої уваги потребує адаптація законодавства до сучасних технологічних викликів, зокрема щодо відповідальності за нові види злочинів у кіберпросторі.

По-третє, ефективна боротьба з кіберзлочинністю можлива лише за умови комплексного підходу. Це включає удосконалення законодавства, зміцнення міжнародного співробітництва, розвиток технологічних засобів кіберзахисту, підвищення рівня правосвідомості громадян та кіберграмотності, а також створення спеціалізованих правоохоронних органів з розширеними повноваженнями у сфері кібербезпеки. У межах дослідження було запропоновано концепцію «кіберімунітету», яка передбачає новітні підходи до протидії кіберзлочинності. До таких підходів належить «кібервакцинація» – розробка програми, що моделює атаки для їхньої ефективної нейтралізації, «кіберлейкоцитів» – автономні агенти для моніторингу та ізоляції загроз, а також «кіберпам’ять» – система аналізу даних для прогнозування нових кіберзагроз.

Перспективи подальших досліджень у цій сфері передбачають детальніше вивчення питань криміналізації нових форм кіберзлочинності, розширення механізмів співпраці між державними органами, бізнесом та міжнародними структурами, а також інтеграції сучасних технологій, зокрема штучного інтелекту, для боротьби з кіберзлочинністю.

Таким чином, проведене дослідження підтвердило необхідність посилення кримінально-правових механізмів протидії кіберзлочинності та впровадження комплексного підходу, що охоплює законодавчі, технологічні та організаційні аспекти.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Думчиков М. О. Кримінально-правова характеристика поняття та видів кіберзлочинів. Науковий вісник Міжнародного гуманітарного університету. Сер. : Юриспруденція. 2022. № 55. С. 65–68. DOI: https://doi.org/10.32841/2307-1745.2022.55.14 (дата звернення: 13.02.2025).

2. Ткаченко П. І., Ткаченко А. О., Ковальчук Д. В. Кримінально-правова характеристика кіберзлочинності, яка вчиняється за попередньою змовою групою осіб: аналіз проблем і перспектив. Право і суспільство. 2023. № 3. С. 278–283. DOI: https://doi.org/10.32842/2078-3736/2023.3.41 (дата звернення: 13.02.2025).

3. Гарига М. М., Вергун Л. О., Кузнєцов О. О. Деякі аспекти криміналістичної характеристики кіберзлочинів. Науковий вісник Сіверщини. серія: право. 2020. № 3. С. 89–99. DOI: https://doi.org/10.32755/sjlaw.2020.03.089 (дата звернення: 13.02.2025).

4. Захарченко А. Є., Каменський Д. В. Актуальні питання кримінально-правових засобів протидії кіберзлочинності. The latest development trends in philological science and education (February 7–8, 2024. Riga, the Republic of Latvia) : International scientific conference. Riga, Latvia : Baltija Publishing, 2024. P. 108-112. DOI: https://doi.org/10.30525/978-9934-26-409-2-25 (дата звернення: 13.02.2025).

5. Конвенція про кіберзлочинність : Конвенція Ради Європи від 23.11.2001 : станом на 7 верес. 2005 р. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 10.02.2025).

6. Кримінальний кодекс України : Кодекс України від 05.04.2001 № 2341-III : станом на 1 лют. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 10.02.2025).

7. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : станом на 28 черв. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 10.02.2025).

Внесок авторів: всі автори зробили рівний внесок у цю роботу
Конфлікт інтересів: автори повідомляють про відсутність конфлікту інтересів

Стаття надійшла до редакції 28.03.2026 Переглянуто 30.04.2026
Стаття рекомендована до друку 14.05.2026 Опубліковано 30.05.2026

N. S. PUZYRNA
Candidate of Legal Sciences, Associate Professor,
Associate Professor of the Department of Public and Private Law
E-mail: 1981-natasha@ukr.net ORCID: https://orcid.org/0000-0002-7297-0829
Chernihiv Polytechnic National University
Chernihiv, 14027, Shevchenko, 95

V. O. PADALKA
Higher education student
E-mail: vladpadalka17@gmail.com ORCID: https://orcid.org/0009-0006-2623-8078
National University ‘Chernihiv Polytechnic’
Chernihiv, 14027, Shevchenko, 95

CYBERCRIME: CRIMINAL LAW CHARACTERISTICS AND COUNTERMEASURES

ANNOTTION. *Introduction.* The article examines cybercrime as one of the most dynamic and transnational threats of the modern digital society. The relevance of the topic is обусловлена the rapid digitalization of social relations, the growing number of criminal offenses committed in cyberspace, and the need to improve criminal law mechanisms for combating such acts, particularly under martial law conditions. The purpose of the study is to conduct a comprehensive criminal law analysis of cybercrime, identify gaps in current legislation, and develop proposals to enhance counteraction mechanisms. The research is based on general scientific and special legal methods, including formal-logical, systemic-structural, comparative-legal analysis, and the study of regulatory sources.

Summary of the main results of the study. The paper analyzes the provisions of the Convention on Cybercrime (2001), Chapter XVI of the Criminal Code of Ukraine, and the Law of Ukraine «On the Basic Principles of Ensuring Cybersecurity of Ukraine». The elements of criminal offenses in the field of information technology are characterized, and problematic aspects of their legal qualification and practical application are identified. The necessity of legislative improvement in accordance with contemporary technological challenges and international standards is substantiated. An innovative concept of «cyber immunity» is proposed, including the mechanisms of «cyber vaccination», «cyber leukocytes», and «cyber memory» as preventive tools against cyber threats.

Conclusion. The conclusions emphasize that effective counteraction to cybercrime requires a comprehensive approach combining legislative modernization, technological development, increased public cyber awareness, and active international cooperation. The proposed approaches may serve as a foundation for further academic research and practical reforms in the field of cybersecurity.

KEY WORDS: *cybercrime, criminal law characteristics, cybersecurity, Criminal Code of Ukraine, counteraction to cybercrime.*

REFERENCES

1. Convention on Cybercrime: Council of Europe Convention dated November 23, 2001. / Council of Europe. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (date of application: 10/02/2025).

2. Criminal Code of Ukraine: Law of Ukraine dated April 5, 2001 No. 2341-III. / Verkhovna Rada of Ukraine. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (date of application: 10/02/2025). (In Ukrainian).

3. On the Basic Principles of Ensuring Cybersecurity of Ukraine: Law of Ukraine dated October 5, 2017 No. 2163-VIII. / Verkhovna Rada of Ukraine. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (date of application: 10/02/2025). (In Ukrainian).

4. Dumchykov, M. O. (2022). Criminal law characteristics of the concept and types of cybercrimes. Scientific Bulletin of the International Humanitarian University. Series: Jurisprudence, 55, 65–68. https://doi.org/10.32841/2307-1745.2022.55.14 (in Ukrainian).

5. Tkachenko, P. I., Tkachenko, A. O., & Kovalchuk, D. V. (2023). Criminal law characteristics of cybercrime committed by prior conspiracy of a group of persons: Problems and prospects. Law and Society, 3, 278–283. https://doi.org/10.32842/2078-3736/2023.3.41 (in Ukrainian).

6. Haryha, M. M., Verhun, L. O., & Kuznetsov, O. O. (2020). Some aspects of the forensic characteristics of cybercrimes. Scientific Bulletin of Sivershchyna. Series: Law, 3, 89–99. https://doi.org/10.32755/sjlaw.2020.03.089 (in Ukrainian).

7. Zakharchenko, A. Ye., & Kamenskyi, D. V. (2024). Current issues of criminal law measures to combat cybercrime. In The latest development trends in philological science and education (International scientific conference, February 7–8, 2024, Riga, Republic of Latvia) (pp. 108–112). Baltija Publishing. https://doi.org/10.30525/978-9934-26-409-2-25 (in Ukrainian)

Authors Contribution: All authors have contributed equally to this work
Conflict of Interest: The authors declare no conflict of interest

The article was received by the editors 28.03.2026
The article was revised 30.04.2026
The article is recommended for printing 14.05.2026
This article published 30.05.2026