ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНО-ТЕХНІЧНОЇ ДІЯЛЬНОСТІ ПОЛІЦІЇ

УДК 004.056
DOI https://doi.org/10.32782/2709-9261-2026-1-17-21

Зеленський Сергій Миколайович,
кандидат юридичних наук, доцент,
доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки
Навчально-наукового інституту підготовки фахівців
для підрозділів кримінальної поліції імені Е. О. Дідоренка
(Донецький державний університет внутрішніх справ, м. Кропивницький)
ORCID: https://orcid.org/0000-0002-0945-4485

КІБЕРЗЛОЧИННІСТЬ ЯК ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ДЕРЖАВИ: СУЧАСНІ ТЕНДЕНЦІЇ ТА ВИКЛИКИ

Ця стаття присвячена аналізу кіберзлочинності, яка виступає серйозною загрозою для інформаційної безпеки держави в умовах активної цифровізації та зростаючої залежності від інформаційних комунікаційних технологій.

Автор доводить, що сучасна кіберзлочинність виходить за межі традиційного кримінально-правового феномена, перетворюючись на системну загрозу національній та інформаційній безпеці. Це явище значно впливає на функціонування державних установ, економічну стабільність, критично важливу інформаційну інфраструктуру, а також на реалізацію конституційних прав громадян.

У статті розглядаються сучасні тенденції розвитку кіберзлочинності, такі як зростання кількості й складності кібератак, застосування шкідливих програм, фішингових атак, програм-вимагачів, атак типу DDoS і методів соціальної інженерії. Окрема увага приділяється транснаціональному характеру кіберзлочинів, їх високій латентності, а також труднощам, які виникають під час їх виявлення, розкриття та розслідування.

Наголошується на збільшенні кіберзагроз у контексті гібридних конфліктів і воєнного стану, коли кіберпростір використовується для дестабілізації держави, впливу на інформаційний простір та підриву її інформаційного суверенітету. Визначено основні виклики у протидії кіберзлочинності, серед яких виділяються недосконала законодавча база, недостатня координація між державними органами та міжнародними партнерами, дефіцит кваліфікованих кадрів і швидкий розвиток цифрових технологій, який випереджає можливості правоохоронних структур. У висновках підкреслюється необхідність впровадження комплексного підходу до боротьби з кіберзлочинністю. Це розглядається як ключовий фактор для забезпечення належного рівня інформаційної безпеки країни і зміцнення загальної національної безпеки.

Ключові слова: *кіберзлочинність, інформаційна безпека, кібербезпека, національна безпека, кіберзагрози, цифровізація, інформаційні комунікаційні технології.*

Постановка проблеми. Стрімка цифровізація суспільних відносин, активне впровадження інформаційних комунікаційних технологій у діяльність державних органів влади, сектору безпеки, фінансових установ та критичної інфраструктури призвели до значної залежності держави від стабільного функціонування інформаційного простору. Водночас це створює нові вразливості, які використовуються кіберзлочинцями – складні та динамічні форми протиправної діяльності в цифровому середовищі, що становлять серйозну загрозу національній інформаційній безпеці.

Кіберзлочинність набуває глобального масштабу, трансформуючись із сегментованих епізодичних правопорушень у системний, транснаціональний виклик з високим рівнем техногенності.

Аналіз останніх досліджень та публікацій. Основні ознаки та напрями протидії кіберзлочинності, як загрози інформаційній безпеці, досліджували науковці

В.М. Бутузов, Д.О. Грицишен, О.Д. Довгань, О.Ю. Довженко, Б.А. Кормич, А.І. Марущак, В.Г. Хахановський, В.С. Цимбалюк та інші.

Метою наукового пошуку у даному напрямі поставлено виявлення сучасних тенденцій і викликів кіберзлочинності, як загрози інформаційній безпеці держави, а завданням – визначення шляхів протидії цьому явищу.

Виклад основного матеріалу. Ю.М. Якименко, В.А. Савченко, С.В. Легомінова представили системний аналіз інформаційної безпеки, а саме використання різних методологічних підходів для створення систем управління інформаційною безпекою, зокрема щодо захисту даних, управління інформаційною безпекою, реагування на інциденти та оцінки ризиків у цій сфері, показано практичний досвід проведення перевірки відповідності системи управління інформаційною безпекою вимогам міжнародних і національних стандартів. Також розкрито застосування методів системного аналізу для оцінки інформаційної безпеки, таких як аналіз інформаційних систем, дослідження організацій через аналіз і синтез, метод аналізу ієрархій та мережеве планування. Визначено порядок оцінки стану інформаційної безпеки в організації, включно з аналізом економічної безпеки підприємства, моніторингом та аудитом системи інформаційної безпеки [1].

За оцінками провідних дослідників у галузі інформаційної безпеки, зокрема О.Д. Довгань, Т.Ю. Ткачук, інформаційну безпеку України визначено як стан, у контексті наявних і потенційних загроз, при якому забезпечується збереження, стабільний та поступовий розвиток інформаційної сфери, включаючи захист інформаційної інфраструктури, інформаційного простору, ресурсів, процесів та їх учасників. Це також охоплює досягнення відповідних національних цілей та реалізацію національних інтересів у цій сфері. Зокрема, забезпечення інформаційної безпеки держави варто розглядати як постійний процес діяльності правоохоронних органів, спрямований на запобігання та протидію загрозам в інформаційній сфері, використання активних заходів впливу. Сучасні кібератаки спрямовані на критично важливі інформаційні ресурси держав, що призводить до потенційного порушення функціонування державних інституцій, економічних систем та інфраструктури [2].

Вчені вказують на міждисциплінарний характер взаємодії криміналістичних, кримінально правових, кримінальних процесуальних, кримінологічних методів вивчення загроз інформаційній безпеці, що в поєднанні з узагальненим досвідом правоохоронної практики постають критично важливими для глибокого розуміння та ефективної протидії кіберзлочинності. Вітчизняні експерти, розкривають правові аспекти протидії кіберзлочинності та наголошують на необхідності вдосконалення правової бази для ефективного реагування на загрози цифровому комунікативному середовищу. Кібератаки включають умисний несанкціонований доступ, використання, маніпулювання, переривання або знищення (за допомогою електронних засобів) електронної інформації та/або електронної інфраструктури і технічних пристроїв, що використовуються для обробки, зв'язку та/або в якості баз даних [2]. Водночас рівень кібербезпеки визначається рівнем шкоди, яку може завдати кібератака.

Сучасні тенденції розвитку кіберзлочинності також відображені в роботах міжнародних дослідників, які аналізують глобальні тенденції кіберзлочинності, поширення кібератак та формування національних стратегій кібербезпеки. Крім того, у сфері кібербезпеки та протидії кіберзлочинності особлива увага приділяється питанням цифрової криміналістики та розслідування злочинів, які висвітлюють сучасні підходи до вивчення кіберзлочинності.

Проблема стає особливо актуальною в контексті гібридних загроз та інформаційних війн, де кіберзлочинність перетинається з елементами кібертероризму та кібердиверсій. Дослідження С.О. Гнатюка висвітлюють розвиток кібертерористичних загроз та можливості протидії їм у сучасному інформаційному суспільстві [3, с. 122]. Незважаючи на наявність нормативно-правових актів і стратегічних документів у сфері кібербезпеки, практика демонструє низку проблем: фрагментарність правового регулювання, недостатню координацію між відповідальними суб'єктами, дефіцит кваліфікованих фахівців, технологічну відсталість частини правоохоронних органів від актуальних загроз. Це зумовлює нагальну потребу в комплексному науковому аналізі сучасних тенденцій кіберзлочинності та викликів, які вона становить для забезпечення інформаційної безпеки держави з метою формування дієвих механізмів запобігання, виявлення й протидії цим загрозам.

Кібербезпека, відповідно п. 5 ч. 1 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України», – це захист життєво важливих інтересів людини та громадянина, суспільства та держави під час використання кіберпростору, що забезпечує сталий розвиток інформаційного суспільства та цифрового комунікаційного середовища, своєчасне виявлення, запобігання та нейтралізацію реальних і потенційних загроз національній безпеці України в кіберпросторі. Однак, слід зазначити, що цей Закон не містить правових інструментів для його практичного застосування під час кібератак [3].

Термін «кіберзлочинність» є відносно новим для науки кримінального права, утворений шляхом поєднання двох слів: «кібер» (розуміється як «кіберпростір», «віртуальний світ», «інформаційний простір») та «злочинність». Поняття «кіберзлочинність» слід розуміти як соціальне явище, що являє собою навмисне мотивоване суспільно небезпечне посягання з використанням мережі Інтернет на інформацію в комп'ютерній системі, програми чи дані, скоєне окремою особою або групою, що становить загрозу для суспільного ладу України, політичної та економічної системи держави, майнових, особистих, політичних, трудових, майнових та інших прав і свобод громадян [4, с. 106].

Важливим аспектом правопорушень у кіберпросторі є їх глобальний характер, що створює серйозні проблеми для правоохоронних органів, оскільки національні злочини, які раніше мали локальне значення, тепер вимагають міжнародної співпраці. Тому більшість держав зацікавлені у припиненні дій, пов'язаних з витоком персональних даних своїх громадян в Інтернет, та зменшенні кібератак, що перешкоджають роботі державних органів, підприємств, установ, організацій, банків тощо. Нормативно-правовою основою боротьби з кіберзлочинністю в Україні є: Конституція України, Кримінальний кодекс України, Закони України «Про основні засади забезпечення кібербезпеки України», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах» тощо, Доктрина інформаційної безпеки України 2017 року, Конвенція Ради Європи про кіберзлочинність, Додатковий протокол до неї та інші міжнародні договори, згода на які надана Верховною Радою України. 7 вересня 2005 року Україна ратифікувала Конвенцію Ради Європи про кіберзлочинність, яка була прийнята з метою співпраці та координації

правоохоронних органів різних держав у сфері боротьби з комп'ютерними злочинами.

Конвенція визначає чотири групи злочинів, пов'язаних з використанням комп'ютерних технологій. До першої групи належать правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, зокрема: – незаконний доступ – навмисний доступ до всієї комп'ютерної системи або її частини без права на це з метою отримання комп'ютерних даних або з іншою протиправною метою (стаття 2 Конвенції); – нелегальне перехоплення – незаконне перехоплення комп'ютерних даних технічними засобами (стаття 3 Конвенції); – втручання в дані – навмисне пошкодження, знищення, псування, зміна або приховування комп'ютерної інформації без права на це (стаття 4 Конвенції); – втручання в систему – навмисне серйозне втручання у функціонування комп'ютерної системи шляхом введення, передачі, пошкодження, знищення, псування, заміни або приховування комп'ютерних даних без права на це (стаття 5 Конвенції); – зловживання пристроями, а саме: їх виготовлення, продаж, придбання для використання, розповсюдження або надання для використання іншим способом (стаття 6 Конвенції) [5].

До другої групи належать правопорушення, пов'язані з використанням комп'ютерів, зокрема підробка та шахрайство: – підробка, пов'язана з комп'ютерами – введення, зміна, знищення або приховування комп'ютерних даних, що призводить до створення недійсних даних з метою надання їм вигляду справжніх, незалежно від того, чи можна їх прочитати або зрозуміти (стаття 7 Конвенції); – шахрайство, пов'язане з комп'ютерами – позбавлення іншої особи її майна шляхом введення, зміни, знищення або приховування комп'ютерних даних або втручання у функціонування комп'ютерної системи (стаття 8 Конвенції). До третьої групи належать правопорушення, пов'язані з контентом (інформацією), зокрема, дитяча порнографія (стаття 9 Конвенції), акти расизму та ксенофобії (стаття 3 Додаткового протоколу до Конвенції) [6, с. 813]. Четверта група, у свою чергу, включає правопорушення, пов'язані з порушенням авторського права та суміжних прав відповідно до чинного законодавства.

Кіберзлочинність як соціально-правове явище є складною формою протиправної діяльності, що реалізується з використанням інформаційних комунікаційних технологій і спрямована на порушення конфіденційності, цілісності та доступності інформації. У науковій літературі кіберзлочинність розглядається як один із ключових дестабілізуючих факторів інформаційної безпеки держави, оскільки її наслідки виходять за межі окремих правопорушень і можуть впливати на функціонування суспільства, економіки та державних інституцій загалом.

Сучасні тенденції розвитку кіберзлочинності характеризуються зростанням її організованості, професіоналізації та транснаціонального характеру. Злочинна діяльність у кіберпросторі дедалі частіше створюється організованими групами, які забезпечують складні технічні засоби, шифрування даних, анонімні мережі та криптовалюти для приховування своєї діяльності. Такі обставини суттєво вдосконалюють виявлення, документування та розслідування кіберзлочинів, а також притягнення винних осіб до кримінальної відповідальності.

Однією з найбільш небезпечних тенденцій є спрямування кіберзлочинних посягань на об'єкти критичної інформаційної інфраструктури держави. Кібератаки на енергетичні системи, фінансові установи, транспортні мережі, державні реєстри та інформаційні ресурси органів влади здатні призвести до масштабних порушень життєдіяльності суспільства, значних економічних збитків і підриву національної безпеки. У цьому контексті кіберзлочинність виходить за межі традиційного кримінального явища та набуває ознак загрози стратегічного рівня [7].

Особливу увагу слід приділити взаємозв'язку кіберзлочинності з гібридними загрозами та інформаційними війнами. У сучасних умовах кіберпростір використовується не тільки для вчинення злочинів, а й як інструмент політичного, військового та інформаційного впливу [8, с. 186]. Кібератаки можуть супроводжуватися кампаніями дезінформації, втручанням у роботу державних інформаційних систем і спробами дестабілізації суспільної свідомості. В умовах воєнного стану такі дії викликають особливу небезпеку, спрямовану на послаблення обороноздатності держави та зниження довіри громадян до органів публічної влади. Науковці справедливо наголошують, що ефективна протидія кіберзлочинності неможлива без належного нормативно-правового забезпечення. В Україні сформовано базові законодавчі та стратегічні засади у сфері кібер- та інформаційної безпеки, однак правозастосовна практика виявляє низку проблем [9, с. 86]. Серед них – фрагментарність кримінально-правових норм, складність кваліфікації окремих видів кіберзлочинів, а також обмежені процесуальні можливості правоохоронних органів щодо збору цифрових доказів та міжнародного співробітництва.

Не менш важливим викликом є кадрове та технічне забезпечення протидії кіберзлочинності. Стрімкий розвиток цифрових технологій створює постійну потребу у спеціалістах, які володіють не лише юридичними знаннями, а й спеціальними навичками в галузі інформаційних технологій та цифрової криміналістики. Відсутність достатньої кількості таких спеціалістів негативно впливає на ефективність діяльності правоохоронних органів та судової системи [10].

Висновки. Підсумовуючи вищесказане слід зазначити, що кіберзлочинність у сучасних умовах є багатовимірною загрозою інформаційній безпеці держави, яка поєднує кримінально-правові, організаційні, технічні та безпекові аспекти. Її протидія вимагає комплексного підходу, що включає вдосконалення законодавства, розвиток інституційної спроможності державних органів, посилення міжвідомчої та міжнародної співпраці, а також формування належного рівня кіберкультури в суспільстві.

В результаті дослідження було встановлено, що кіберзлочинність у сучасних умовах стала однією з ключових загроз інформаційній безпеці держави, яка має системний, транснаціональний та високотехнологічний характер. Її небезпека зумовлена не лише масштабом та динамічністю, але й здатністю впливати на функціонування державних інституцій, критичну інформаційну інфраструктуру, економічну стабільність та громадську безпеку загалом.

Встановлено, що сучасні тенденції розвитку кіберзлочинності пов'язані з активним використанням складних технічних засобів, анонімних мереж, шифрування даних та криптовалют, що значно ускладнює процеси виявлення, документування та розслідування кіберзлочинів. Особливу загрозу становлять кібератаки на державні інформаційні ресурси та об'єкти критичної інфраструктури, результатом яких може бути дестабілізація соціально-політичної ситуації та підрив національної безпеки.

Обґрунтовано, що в умовах гібридних загроз та воєнного стану кіберзлочинність тісно переплітається з елементами інформаційної війни, кібертероризму та кібердиверсій, що вимагає комплексної та скоординованої відповіді з боку держави. Водночас, аналіз правоохоронної практики свідчить про наявність низки проблем у сфері протидії кіберзлочинності, зокрема, фрагментарність нормативно-правового регулювання, недостатній рівень міжвідомчої взаємодії, кадрові та технічні обмеження суб'єктів забезпечення кібербезпеки. Зроблено висновок, що ефективна протидія кіберзлочинності як загрозі інформаційній безпеці держави, можлива лише за умови реалізації комплексного підходу, який поєднує вдосконалення законодавства, розвиток інституційної спроможності правоохоронних органів, посилення міжнародного співробітництва, впровадження сучасних технологічних рішень та підвищення рівня кіберграмотності суспільства. Подальші наукові дослідження у цій галузі мають бути спрямовані на розробку ефективних механізмів запобігання та мінімізації кіберзагроз з урахуванням сучасних викликів національній безпеці України.

Список використаних джерел

1. Якименко Ю. М., Савченко В. А., Легомінова С. В. Системний аналіз інформаційної безпеки: сучасні методи управління : підручник. Київ : Державний університет телекомунікацій, 2022. 308 с. URL: https://www.dut.edu.ua/uploads/l_2230_88161692.pdf

2. Довгань О. Д., Ткачук Т. Ю. Концептуальні засади законодавчого забезпечення інформаційної безпеки України. *Інформація і право*. 2019. № 1. С. 86–99. DOI: https://doi.org/10.37750/2616-6798.2019.1(28).221314.

3. Гнатюк С. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи. *Безпека інформації*. 2013. Т. 19, № 2. С. 118–129. URL: http://nbuv.gov.ua/UJRN/bezin_2013_19_2_8

4. Рафальський І., Соха С., Савчук С., Здібель Р. Сучасний стан наукових досліджень з проблем державної кримінально-правової політики протидії кіберзлочинності / І. Рафальський, С. Соха, С. Савчук, Р. Здібель. *Society and Security*. 2024. № 6. С. 103–115. DOI: 10.26642/sas-2024-6(6)-103-115.

5. Поліщук В. Кіберзлочини та кібербезпека: боротьба з комп'ютерними злочинами і кібератаками. *Наукові праці Міжрегіональної Академії управління персоналом. Юридичні науки*. 2023. № 3. С. 44–47. DOI: 10.32689/2522-4603.2023.3.7.

6. Галушко П. П. Кіберзлочинність: поняття та соціально-правова природа. *Вісник Кримінологічної асоціації України*. 2026. № 34. С. 808–817. DOI: https://doi.org/10.32631/vca.2025.1.66

7. Lukashevych S., Palkova K. Cybersecurity of the information space of a higher education institution. *Archives of Criminology and Forensic Sciences*. 2024. Vol. 10, № 2. С. 60–71. DOI: 10.32353/acfs.10.2024.02.

8. Якимчук М. Особливості правового регулювання протидії кіберзлочинності в Україні: порівняльно-правовий аспект. *Нове українське право*. 2021. № 4. С. 182–186. DOI: 10.51989/NUL.2021.4.27.

9. Гребенюк А. М. Кіберзлочинність в Україні. *Економічна та інформаційна безпека: актуальні питання та інновації* : матеріали Міжнар. наук.-практ. конф. (м. Дніпро, 4 листопада 2021 р.). Дніпро : ДДУВС, 2021. С. 85–88. URL: https://er.dduvs.edu.ua/handle/123456789/8596

10. Ільєнко А., Телющенко В., Дубчак О. Сучасні кіберзагрози критичної інфраструктури України та світу. *Кібербезпека: освіта, наука, техніка*. 2025. № 3. С. 150–164. DOI: 10.28925/2663-4023.2023.27.719.

References

1. Yakymenko, Yu. M., Savchenko, V. A., & Lehominova, S. V. (2022). *Systemnyi analiz informatsiinoi bezpeky: suchasni metody upravlinnia* [Systems analysis of information security: modern management methods] [Textbook]. State University of Telecommunications. https://www.dut.edu.ua/uploads/l_2230_88161692.pdf [in Ukrainian].

2. Dovhan, O. D., & Tkachuk, T. Yu. (2019). Kontseptualni zasady zakonodavchoho zabezpechennia informatsiinoi bezpeky Ukrainy [Conceptual foundations of legislative support for information security of Ukraine]. *Informatsiia i pravo*, (1), 86–99. https://doi.org/10.37750/2616-6798.2019.1(28).221314 [in Ukrainian].

3. Hnatiuk, S. (2013). Kiberterroryzm: istoriia rozvytku, suchasni tendentsii ta kontrzakhody [Cyberterrorism: history of development, current trends and countermeasures]. *Bezpeka informatsii*, *19*(2), 118–129. http://nbuv.gov.ua/UJRN/bezin_2013_19_2_8 [in Ukrainian].

4. Rafalskyi, I., Sokha, S., Savchuk, S., & Zdibel, R. (2024). Suchasnyi stan naukovykh doslidzhen z problem derzhavnoi kryminalno-pravovoi polityky protydii kiberzlochynnosti [Current state of scientific research on the problems of state criminal law policy to combat cybercrime]. *Society and Security*, (6), 103–115. https://doi.org/10.26642/sas-2024-6(6)-103-115 [in Ukrainian].

5. Polishchuk, V. (2023). Kiberzlochyny ta kiberbezpeka: borotba z kompiuternymy zlochynamy i kiberatakamy [Cybercrimes and cybersecurity: the fight against computer crimes and cyberattacks]. *Naukovi pratsi Mizhrehionalnoi Akademii upravlinnia personalom. Yurydychni nauky*, (3), 44–47. https://doi.org/10.32689/2522-4603.2023.3.7 [in Ukrainian].

6. Halushko, P. P. (2026). Kiberzlochynnist: poniattia ta sotsialno-pravova pryroda [Cybercrime: concept and socio-legal nature]. *Visnyk Kryminolohichnoi asotsiatsii Ukrainy*, (34), 808–817. https://doi.org/10.32631/vca.2025.1.66 [in Ukrainian].

7. Lukashevych, S., & Palkova, K. (2024). Cybersecurity of the information space of a higher education institution. *Archives of Criminology and Forensic Sciences*, *10*(2), 60–71. https://doi.org/10.32353/acfs.10.2024.02 [in English].

8. Yakymchuk, M. (2021). Osoblyvosti pravovoho rehuliuvannia protydii kiberzlochynnosti v Ukraini: porivnialno-pravovyi aspekt [Features of legal regulation of combating cybercrime in Ukraine: comparative legal aspect]. *Nove ukrainske pravo*, (4), 182–186. https://doi.org/10.51989/NUL.2021.4.27 [in Ukrainian].

9. Hrebeniuk, A. M. (2021, November 4). *Kiberzlochynnist v Ukraini* [Cybercrime in Ukraine] [Conference presentation]. Mizhnar. nauk.-prakt. konf. «Ekonomichna ta informatsiina bezpeka: aktualni pytannia ta innovatsii», Dnipro, Ukraine. https://er.dduvs.edu.ua/handle/123456789/8596 [in Ukrainian].

10. Ilienko, A., Teliushchenko, V., & Dubchak, O. (2025). Suchasni kiberzahrozy krytychnoi infrastruktury Ukrainy ta svitu [Modern cyber threats to critical infrastructure of Ukraine and the world]. *Kiberbezpeka: osvita, nauka, tekhnika*, (3), 150–164. https://doi.org/10.28925/2663-4023.2023.27.719 [in Ukrainian].

Zelenskyi Serhii,
Candidate of Law, Associate Professor,
Associate Professor at the Department of Operational and Investigative Activities
and Information Security of the Educational and Scientific Institute for Training Specialists for Criminal Police Units named after E. O. Didorenko
(Donetsk State University of Internal Affairs, Kropyvnytskyi)
ORCID: https://orcid.org/0000-0002-0945-4485

CYBERCRIME AS A THREAT TO THE INFORMATION SECURITY OF THE STATE: CURRENT TRENDS AND CHALLENGES

This article is devoted to the analysis of cybercrime, which poses a serious threat to the information security of the state in the context of active digitalization and growing dependence on information and communication technologies.

The author proves that modern cybercrime goes beyond the traditional criminal and legal phenomenon, turning into a systemic threat to national and information security. This phenomenon significantly affects the functioning of state institutions, economic stability, critical information infrastructure, as well as the implementation of the constitutional rights of citizens.

The article examines modern trends in the development of cybercrime, such as the growth in the number and complexity of cyberattacks, the use of malicious programs, phishing attacks, ransomware, DDoS attacks and social engineering methods. Special attention is paid to the transnational nature of cybercrimes, their high latency, as well as the difficulties that arise during their detection, disclosure and investigation.

The increase in cyber threats in the context of hybrid conflicts and martial law is emphasized, when cyberspace is used to destabilize the state, influence the information space and undermine its information sovereignty. The main challenges in combating cybercrime are identified, including an imperfect legislative framework, insufficient coordination between state bodies and international partners, a shortage of qualified personnel and the rapid development of digital technologies, which is ahead of the capabilities of law enforcement agencies. The conclusions emphasize the need to implement a comprehensive approach to combating cybercrime. This is considered a key factor in ensuring the proper level of information security of the country and strengthening overall national security.

Key words: *cybercrime, information security, cybersecurity, national security, cyber threats, digitalization, information communication technologies.*

Дата першого надходження статті до видання: 18.02.2026
Дата прийняття статті до друку після рецензування: 25.03.2026
Дата публікації (оприлюднення) статті: 11.05.2026