УДК 343.34
https://doi.org/10.32703/2663-6352/2024-2-16-258-264
https://orcid.org/0009-0009-4491-8677
Лугівська Луїза Русланівна
здобувач другого (магістерського) рівня вищої освіти

https://orcid.org/0009-0009-2061-6420
Яцишин Олександр Олександрович
здобувач другого (магістерського) рівня вищої освіти
Державного податкового університету

https://orcid.org/0000-0003-4715-1749
Любавіна Вікторія Петрівна
к.ю.н., доцент
кафедри кримінального права та процесу
Державного податкового університету

ТЕНДЕНЦІЇ РОЗВИТКУ КРИМІНАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ ЗА КІБЕРЗЛОЧИНИ В УМОВАХ ЦИФРОВІЗАЦІЇ СУСПІЛЬСТВА

Анотація. *Швидкий розвиток цифрових технологій суттєво трансформував соціально-економічний та правовий ландшафт у всьому світі. Зі зростаючою залежністю від інформаційно-комунікаційних технологій поширеність і складність кіберзлочинів значно збільшилися. У статті досліджуються еволюційні тенденції кримінальної відповідальності за кіберзлочини в умовах глобальної диджиталізації. Вона пропонує всебічний аналіз правових та інституційних механізмів, спрямованих на боротьбу з кіберзлочинністю, з особливим акцентом на кримінальному законодавстві України та його відповідності міжнародним стандартам.*

Дослідження охоплює типологію кіберзлочинів, зокрема несанкціонований доступ, крадіжку ідентифікаційних даних, фінансове шахрайство та розповсюдження шкідливого програмного забезпечення, а також їхній вплив на національну та глобальну безпеку. Особлива увага приділяється положенням Кримінального кодексу України, зокрема статтям 361–363-1, які визначають та регулюють відповідальність за кіберзлочини. У статті також аналізуються міжнародні практики, зокрема Будапештська конвенція про кіберзлочинність, і розглядається роль транснаціонального співробітництва у протидії транскордонним кіберзагрозам.

Ключові тенденції включають зростаючу гармонізацію національних правових систем з міжнародними стандартами, запровадження жорсткіших санкцій за кіберзлочини та активне використання цифрових інструментів,

таких як штучний інтелект, у правоохоронній діяльності. Результати підкреслюють важливість законодавчої адаптивності, посилення міжнародної співпраці та партнерства між державним і приватним секторами для ефективної боротьби з динамічною природою кіберзагроз.

Дослідження висвітлює виклики, з якими стикаються держави у забезпеченні ефективної правової реакції на кіберзлочини, особливо в умовах глобальної взаємопов'язаності. Рекомендації для України включають подальший розвиток правової бази, інтеграцію міжнародних норм та впровадження превентивних заходів для зміцнення інфраструктури кібербезпеки.

Ключові слова: *кіберзлочини, кримінальна відповідальність, цифровізація, міжнародне право, Україна, інформаційні технології, гармонізація законодавства, транснаціональні загрози, кібербезпека.*

Abstract. *The rapid advancement of digital technologies has significantly transformed the socio-economic and legal landscape worldwide. With the increasing reliance on information and communication technologies, the prevalence and sophistication of cybercrimes have grown exponentially. This article investigates the evolving trends in criminal liability for cybercrimes within the framework of global digitalization. It provides a comprehensive analysis of the legal and institutional mechanisms aimed at addressing cybercrimes, focusing on Ukraine's criminal legislation and its alignment with international standards.*

The study delves into the typologies of cybercrimes, including unauthorized access, identity theft, financial fraud, and the dissemination of malicious software, and their impact on national and global security. Particular attention is given to the legislative provisions of the Criminal Code of Ukraine, specifically Articles 361–363-1, which define and regulate responsibility for cyber offenses. The article also examines international practices, such as the Budapest Convention on Cybercrime, and explores the role of transnational cooperation in combating cross-border cyber threats.

Key trends identified include the increasing harmonization of national legal systems with international frameworks, the introduction of more stringent penalties for cyber offenses, and the active use of digital tools, such as artificial intelligence, in law enforcement. The findings emphasize the importance of legislative adaptability, enhanced international collaboration, and public-private partnerships to address the ever-changing nature of cyber threats.

This research highlights the challenges faced by states in ensuring effective legal responses to cybercrimes, particularly in the context of global interconnectedness. Recommendations for Ukraine include further development of its legal framework, integration of international norms, and implementation of preventive measures to strengthen cybersecurity infrastructure.

Key words*: cybercrimes, criminal liability, digitalization, international law, Ukraine, information technology, harmonization of legislation, transnational threats, cybersecurity.*

Постановка проблеми. Сучасне суспільство характеризується стрімким розвитком інформаційних технологій та глибокою цифровізацією всіх сфер життя. Цей процес сприяє зростанню нових можливостей для комунікації,

бізнесу та навчання, але водночас породжує серйозні загрози, зокрема збільшення кіберзлочинності.

Кіберзлочини стали глобальною проблемою, що вимагає ефективних правових механізмів протидії. Оскільки технології швидко розвиваються, кримінальне право повинно адаптуватися до нових викликів і передбачати відповідальність за кіберзлочини.

Кіберзлочинність набула масового характеру, що зумовлює загрозу як окремим особам, так і державним інститутам. До найпоширеніших кіберзлочинів відносять хакерські атаки, фішинг, крадіжку даних, поширення шкідливого програмного забезпечення, фінансові шахрайства та кібершпигунство. В умовах глобалізації такі злочини часто виходять за межі однієї країни, що ускладнює їх розслідування.

Розвиток цифрових технологій в Україні супроводжується зростанням кіберзагроз. За даними CERT-UA (Кіберкоманда України), кількість інцидентів, пов'язаних із кібератаками, у 2022 році збільшилася на 40% порівняно з попереднім роком. У таких умовах необхідне вдосконалення кримінального законодавства для ефективної протидії злочинам у кіберпросторі.

Метою цієї роботи є аналіз тенденцій розвитку кримінальної відповідальності за кіберзлочини, зокрема в умовах цифровізації суспільства, на основі досліджень українських і зарубіжних науковців, а також аналіз існуючих правових механізмів.

Виклад основного матеріалу. Кіберзлочин — злочин, що вчиняється у цифровому середовищі із використанням інформаційно-комунікаційних технологій.

Кримінальна відповідальність — юридична відповідальність, яка передбачає покарання за вчинення злочину, встановленого Кримінальним кодексом

Цифровізація — процес інтеграції цифрових технологій у всі сфери суспільного життя.

Українські науковці, зокрема Т. Філіпова та О. Шевченко [8, ст. 210, 9,ст. 280], підкреслюють, що чинне кримінальне законодавство України лише частково враховує специфіку кіберзлочинів. Вони наголошують на необхідності внесення змін до Кримінального кодексу України з урахуванням міжнародних стандартів, таких як Будапештська конвенція про кіберзлочинність.

Серед зарубіжних дослідників Д. Гудман [2. ст. 320] акцентує увагу на ролі співпраці між країнами у боротьбі з кіберзлочинністю. Він зазначає, що ефективна протидія кіберзлочинам можлива лише за умови створення глобальної системи обміну інформацією між правоохоронними органами.

Згідно з дослідженням В. Клімова [7, ст. 200], більшість країн ЄС посилили відповідальність за кіберзлочини, впровадивши штрафи, тюремні строки, а також запровадження додаткових заходів, таких як блокування незаконного контенту.

Українські вчені, зокрема О. Кулик та Т. Філіпова [9, ст. 280], зазначають, що чинне кримінальне законодавство України лише частково

враховує специфіку кіберзлочинів. Вони наголошують на важливості гармонізації законодавства з міжнародними стандартами, такими як Будапештська конвенція про кіберзлочинність.

Зарубіжні дослідники, наприклад, Б. Брюс, підкреслюють, що ефективна боротьба з кіберзлочинністю можлива лише за умови тісної співпраці між країнами. Вони акцентують на важливості створення спільних баз даних і швидкого обміну інформацією.

Е. Еріксон [5, ст. 320] у своїх дослідженнях зазначає, що глобалізація кіберпростору ускладнює питання юрисдикції та покарання, оскільки злочинці можуть діяти з-за кордону.

Аналіз кримінального законодавства України показав, що статті 361–363-1 Кримінального кодексу України [1] передбачають відповідальність за несанкціоноване втручання в роботу комп'ютерів, поширення шкідливого програмного забезпечення та порушення правил експлуатації інформаційних систем. Однак, порівняно з країнами ЄС, ці положення є менш деталізованими.

У таблиці наведено порівняння підходів до кримінальної відповідальності за кіберзлочини в Україні та країнах ЄС.

Таблиця 1.1.

Критерій	**Україна**	**Країна ЄС**
Основні статті законодавства	Ст. 361–363-1 КК України	Загальний регламент із захисту даних (GDPR)
Типи покарань	Штраф, позбавлення волі	Штраф, позбавлення волі, блокування контенту
Врахування міжнародних стандартів	Частково (Будапештська конвенція)	Повністю (відповідність Будапештській конвенції)
Рівень захищеності особистих даних	Помірний	Високий

Також проведений аналіз показав, що в умовах цифровізації суспільства кількість кіберзлочинів щороку зростає. Це вимагає від України не лише вдосконалення законодавства, а й підвищення цифрової грамотності населення та посилення технічного забезпечення правоохоронних органів.

Основні тенденції [3, ст. 250].

- посилення відповідальності. У більшості країн ЄС запроваджено жорсткіші покарання за кіберзлочини, включаючи великі штрафи та блокування доступу до ресурсів.

- глобалізація правових механізмів. Уряди країн активніше співпрацюють у межах Інтерполу, Європолу та ООН для протидії кіберзлочинності.

– **технологізація правоохоронних органів.** Використання штучного інтелекту, аналізу великих даних та інших цифрових інструментів стає основою у розслідуванні злочинів.

Таблиця 1.2

Зростання кількості кіберзлочинів у світі (2019-2023)

Рік	Кількість кіберзлоичнів (у млн)	Рівень зростання
2019	1,2	-
2020	1,5	25,00%
2021	1,9	27,00%
2022	2,5	32,00%
2023	3,1	24,00%

Джерело [10]

Розвиток кримінальної відповідальності за кіберзлочини в умовах цифровізації суспільства є результатом адаптації правових систем до нових викликів, які виникають у зв’язку з поширенням інформаційно-комунікаційних технологій. Сучасне законодавство проходить трансформацію, спрямовану на врахування специфіки кіберпростору, глобалізації злочинів і необхідності міжнародної співпраці.

Етапи розвитку кримінальної відповідальності за кіберзлочини [7, ст. 200]:

Перший етап: поява перших правових норм

На початку розвитку цифрових технологій (1980–1990-ті роки) законодавчі органи різних країн почали формулювати базові положення для захисту інформаційних систем. Одними з перших з'явилися статті, які стосувалися несанкціонованого доступу до інформації, знищення або зміни даних

У цей період кримінальна відповідальність обмежувалася окремими положеннями, які не враховували стрімкий розвиток технологій. У більшості країн закони про кіберзлочини були лише доповненнями до існуючого кримінального законодавства.

Другий етап: стандартизація та міжнародне регулювання

У 2001 році було ухвалено **Будапештську конвенцію про кіберзлочинність**, яка стала першим міжнародним документом, що закріпив єдині стандарти для протидії злочинам у кіберпросторі. Конвенція встановила основні категорії кіберзлочинів, серед яких:

- несанкціонований доступ до інформаційних систем;

- втручання в роботу комп'ютерних систем;
- поширення шкідливих програм;
- крадіжка персональних даних.

Цей етап характеризувався активним розвитком національного законодавства країн-учасниць, які адаптували свої правові системи до стандартів Конвенції.

Третій етап: цифровізація та посилення покарань.

Зі стрімким розвитком цифрових технологій (2010–2020-ті роки) кіберзлочини стали більш складними, а їх масштаби — глобальними.

Це зумовило посилення кримінальної відповідальності, включаючи підвищення розмірів штрафів, збільшення строків ув'язнення та введення додаткових санкцій, таких як блокування незаконного контенту або конфіскація цифрових активів

Наприклад, у країнах Європейського Союзу активно використовуються штрафи за порушення Регламенту про захист персональних даних (GDPR), які можуть досягати 20 млн євро або 4% від річного доходу компанії [4].

Глобалізація правового регулювання. Злочини у кіберпросторі часто мають транснаціональний характер, що вимагає тісної співпраці між країнами.

Інтерпол та Європол активно розробляють механізми обміну інформацією між правоохоронними органами різних держав. Для ефективної боротьби з кіберзлочинами Україна приєдналася до Будапештської конвенції, а також працює над гармонізацією свого законодавства з міжнародними стандартами.

Інклюзія нових типів злочинів.

Кримінальна відповідальність розширюється на нові види злочинів, такі як [5, ст. 320]:

- фінансові шахрайства у кіберпросторі (криптовалютні схеми);
- поширення дезінформації та маніпулювання громадською думкою;
- кібершпигунство та кібервійни.

Використання штучного інтелекту у злочинних схемах вимагає перегляду підходів до кримінальної відповідальності. Наприклад, у США та ЄС розглядаються проєкти законів, які передбачають відповідальність за розробку та розповсюдження шкідливих алгоритмів

Посилення захисту особистих даних.

У зв'язку зі зростанням кількості витоків інформації на законодавчому рівні впроваджуються суворіші норми щодо відповідальності за недотримання правил обробки даних. GDPR став зразком для багатьох країн, які розробляють власні аналоги цього регламенту.

Висновок. Таким чином підсумуємо те, що цифровізація суспільства змінює характер злочинності, акцентуючи увагу на кіберзлочинах. Досвід європейських країн показує, що для ефективної протидії необхідно розробляти детальні нормативно-правові акти, посилювати співпрацю між державами та впроваджувати нові технології у розслідування злочинів.

Україна потребує перегляду чинного кримінального законодавства з урахуванням міжнародних стандартів і рекомендацій, а також активізації

просвітницької роботи щодо цифрової безпеки. Це дозволить забезпечити ефективну протидію кіберзлочинам та підвищити рівень захищеності суспільства.

Розвиток кримінальної відповідальності за кіберзлочини відображає прагнення держав адаптувати свої правові системи до цифрової епохи. Україна робить важливі кроки у вдосконаленні законодавства, але потребує подальшої гармонізації з міжнародними стандартами, посилення захисту персональних даних і технічного забезпечення правоохоронних органів. Міжнародна співпраця та інтеграція інноваційних технологій у правову сферу є ключем до ефективної протидії кіберзлочинності в умовах цифровізації суспільства.

ЛІТЕРАТУРА

1. Кримінальний кодекс України від 05.04.2001 р. № 2341-III.
2. Гудман, Д. Міжнародна співпраця у протидії кіберзлочинності / Д. Гудман. – Лондон: Academic Press, 2018. – 320 с.
3. Зайченко, Н. Цифровізація та правопорядок у сфері кібербезпеки / Н. Зайченко. – Одеса: Фенікс, 2021. – 250 с.
4. Загальний регламент із захисту даних (GDPR). Європейський Союз, 2016
5. Еріксон, Е. Захист даних у кіберпросторі: міжнародні стандарти / Е. Еріксон. – Нью-Йорк: Routledge, 2018. – 320 с.
6. Конвенція про кіберзлочинність (Будапештська конвенція). Рада Європи, 2001.
7. Клімов, В. Правові основи боротьби з кіберзлочинами у країнах ЄС / В. Клімов. – Прага: EU Law, 2019. – 200 с.
8. Шевченко, О. Вдосконалення кримінального законодавства України у сфері кіберзлочинності / О. Шевченко. – Харків: Основа, 2021. – 210 с
9. Філіпова, Т. Проблеми протидії кіберзлочинності в Україні / Т. Філіпова. – Київ: Генеза, 2020. – 280 с.
10. CERT-UA. Звіт про стан кібербезпеки в Україні у 2022 році. – Київ: CERT-UA, 2022