Кібербезпека та правозастосування

УДК 343.9:004.056(477)

DOI https://doi.org/10.5281/zenodo.15074665

ОЦІНКА ЕФЕКТИВНОСТІ ПРАВОВИХ МЕХАНІЗМІВ ЗАПОБІГАННЯ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ

Дрижакова Діна Юріївна,
аспірантка кафедра кримінально-правової політики та кримінального права, Інститут права, КНУ імені Тараса Шевченка, м. Київ, Україна,
https://orcid.org/0009-0004-7585-5860

Горішній Олег Олександрович,
кандидат юридичних наук, доцент кафедри правових дисциплін, Херсонський інститут ПрАТ «ВНЗ «МАУП», м. Херсон, Україна,
https://orcid.org/0000-0001-9867-7199

Тараненко Микола Миколайович,
кандидат юридичних наук, старший викладач кафедри інформаційного, господарського та адміністративного права, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ, Україна,
https://orcid.org/0000-0002-1594-5598

Прийнято: 09.03.2025 | Опубліковано: 24.03.2025

Анотація. Метою дослідження є всебічна оцінка ефективності правових механізмів запобігання кіберзлочинності в Україні, зокрема про необхідність удосконалення законодавчих ініціатив та підвищення ефективності боротьби з новими, складними формами кіберзлочинів. Серед нових загроз особливу

увагу приділено хакерським атакам, кібершахрайству, злочинам у сфері електронних платежів, а також проблемам, що виникають із використанням технологій блокчейн та криптовалют.

У дослідженні проводиться детальний аналіз сучасних правових норм та інструментів, що регулюють боротьбу із кіберзлочинністю. Також вивчаються основні проблеми, які виникають в умовах інтенсивного розвитку інформаційних технологій та перманентно нестійкого характеру цифрових загроз.

Важливим аспектом дослідження є аналіз ефективності взаємодії органів державного управління з приватним сектором у питаннях кібербезпеки, а також оцінка міжнародної співпраці в контексті протидії кіберзлочинності.

Результати дослідження свідчать, що в Україні досягнуто значного прогресу в удосконаленні правового забезпечення кібербезпеки, зокрема через прийняття низки законів і механізмів, орієнтованих на боротьбу із кіберзлочинністю.

Також дослідження охоплює проблеми, пов’язані з кваліфікацією кіберзлочинів, яка не завжди відповідає реальним викликам. У статті розглядається питання недостатньої підготовленості правоохоронних органів та органів влади для ефективної боротьби з кіберзлочинністю в умовах стрімкої цифрової трансформації. Нагальними постають проблеми з координацією між державними і приватними структурами, що ускладнює оперативну реакцію на загрози.

Висновки дослідження містять комплексні рекомендації щодо подальшого вдосконалення кримінального законодавства, орієнтуючись на чіткіше визначення та кваліфікацію нових форм кіберзлочинів, створення правових механізмів для ефективного реагування на цифрові загрози, покращення співпраці між державними органами і приватними компаніями, які відповідають за кібербезпеку.

ISSN: 3041-2110

Крім того, підвищення рівня кваліфікації правоохоронців, розвиток міжнародної співпраці та створення спеціалізованих органів для боротьби із кіберзлочинністю є важливими кроками для зміцнення національної безпеки в умовах глобальних цифрових змін.

Ключові слова: кібербезпека, кримінальне законодавство, міжнародна співпраця, цифрові загрози, кібершахрайство.

ASSESSMENT OF THE EFFECTIVENESS OF LEGAL MECHANISMS FOR PREVENTING CYBERCRIME IN UKRAINE

Dina Dryzhakova,
PhD student, Department of Criminal Legal Policy and Criminal Law, Institute of Law, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine,
https://orcid.org/0009-0004-7585-5860

Oleh Horishnyi,
PhD in Law, Associate Professor of the Department of Legal Disciplines, Kherson Institute of Interregional Academy of Personnel Management, Kherson, Ukraine,
https://orcid.org/0000-0001-9867-7199

Mykola Taranenko,
PhD in Law, Senior Lecturer, Department of Informational, Business and Administrative Law, National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», Kyiv, Ukraine,
https://orcid.org/0000-0002-1594-5598

Abstract. The purpose of this study is a comprehensive assessment of the effectiveness of legal mechanisms for preventing cybercrime in Ukraine, with an

emphasis on the need to improve legislative initiatives and increase the effectiveness of combating new, complex forms of cybercrime. Among such new threats, special attention is paid to hacker attacks, cyberfraud, crimes in the field of electronic payments, as well as problems arising from the use of blockchain and cryptocurrency technologies. The study provides a detailed analysis of existing legal norms and instruments regulating the fight against cybercrime, and also studies the main problems that arise in the conditions of rapid development of information technologies and the constantly changing nature of digital threats. An important aspect of the study is the analysis of the effectiveness of interaction between state bodies and the private sector in cybersecurity issues, as well as the assessment of international cooperation in the context of combating cybercrime.

The results of the study indicate that significant progress has been made in Ukraine in improving the legal support for cybersecurity, in particular, through the adoption of a number of laws and regulations focused on combating cybercrime. Along with this, the study points to problems related to the qualification of cybercrimes, which does not always meet real challenges, as well as the insufficient preparedness of law enforcement agencies and authorities to effectively combat cybercrime in the conditions of rapid digital transformation. Problems with coordination between public and private structures remain, which complicates the operational response to threats.

The study's conclusions include comprehensive recommendations for further improvement of criminal legislation, focusing on a clearer definition and qualification of new forms of cybercrime, the creation of legal mechanisms for an effective response to digital threats, and the improvement of cooperation mechanisms between public authorities and private companies responsible for cybersecurity. In addition, improving the skills of law enforcement officers, developing international cooperation, and creating specialized bodies to combat cybercrime are important steps to strengthen national security in the context of global digital changes.

ISSN: 3041-2110

Keywords: cybersecurity, criminal legislation, international cooperation, digital threats, cyber fraud.

Постановка проблеми. У сучасних умовах цифрової трансформації суспільства кіберзлочинність стала одним із найбільших викликів для національної безпеки України. Вплив інформаційних технологій на всі сфери життя, включно з економікою, державним управлінням і соціальними комунікаціями, спричинив зростання ризиків, пов'язаних із неправомірним використанням цифрових ресурсів. Кібератаки, фінансові шахрайства, несанкціонований доступ до інформаційних систем, поширення шкідливого програмного забезпечення та інші види кіберзлочинів завдають значних матеріальних збитків та підривають довіру до цифрового середовища.

Україна, що перебуває в умовах воєнного стану та активної цифровізації, стикається з особливими загрозами у сфері кібербезпеки. Зокрема, фіксується зростання кількості кібератак на державні інформаційні ресурси, фінансовий сектор та критичну інфраструктуру. У відповідь на ці виклики держава здійснює заходи для вдосконалення правового регулювання кібербезпеки, зокрема через оновлення законодавства, міжнародне співробітництво та розширення функціоналу правоохоронних органів.

Водночас ефективність сучасних правових механізмів недостатня, оскільки кіберзлочинці постійно вдосконалюють свої методи, а правоохоронні органи та судова система стикаються з низкою правових і технічних перешкод у процесі розслідування та запобігання злочинам. Брак кваліфікованих кадрів, розмитість правового регулювання щодо цифрових доказів та юрисдикційні колізії є додатковими факторами, що ускладнюють боротьбу із кіберзлочинністю.

Аналіз останніх досліджень і публікацій у сфері правових механізмів запобігання кіберзлочинності в Україні показує високий рівень наукової зацікавленості щодо цієї теми. Зокрема, численні наукові праці висвітлюють

різні аспекти правового регулювання, практики боротьби із кіберзлочинністю, а також різні підходи до цієї проблеми у закордонних публікаціях.

Зокрема, дослідження М. І. Саєнка, Є. А. Савели, Ю. Ю. Тополянського [1] акцентують увагу на аналізі міжнародного досвіду та порівняльному правознавстві в цій сфері, що дозволяє визначити ефективні стратегії протидії кіберзлочинам, які можуть бути застосовані в Україні. У дослідженнях В. В. Аніщука і С. Г. Зицика [2] проводиться порівняльно-правовий аналіз законодавства різних країн щодо боротьби із кіберзлочинністю, що дозволяє визначити реальні прогалини в національному правовому регулюванні.

У публікаціях А. Козія, Т. Марченка, В. Шевченка [3] та І. Коцмана [4] досліджуються основні напрямки державного регулювання кіберзлочинності в Україні, пропонуються конкретні механізми для підвищення ефективності національної політики щодо кіберзахисту, включаючи важливість взаємодії з міжнародними організаціями.

У дослідженні Н. А. Лугіної і А. М. Лучука [5] проведено порівняльний аналіз національних та європейських правових норм, що стосуються запобігання кіберзлочинності, виявлено ключові відмінності, які потребують урахування при реформуванні українського законодавства.

Публікація Є. Ю. Морданя, В. В. Бардакової, Л. В. Сокола [6] присвячена удосконаленню національної системи протидії кіберзлочинності на основі впровадження міжнародного досвіду. Водночас М. Сащенко [7] формулює проблеми запобігання кіберзлочинності в Україні, зокрема у сфері правозастосування та судової практики.

У дослідженні І. Флиса [7] акцентується на правовому реформуванні кіберзахисту в Україні, зокрема на необхідності адаптації сучасного законодавства до новітніх викликів у сфері кібербезпеки. Так, автор пропонує підвищити ефективність правових механізмів через інтеграцію міжнародного досвіду та впровадження нових підходів до захисту інформаційної інфраструктури країни.

Вітчизняні дослідники В. Г. Хахановський та В. Д. Гавловський [8] зосереджуються на кримінально-правовому забезпеченні протидії кіберзлочинності, досліджуючи особливості кваліфікації кіберзлочинів в Україні. Підкреслюється важливість удосконалення кримінального законодавства для чіткішого визначення та боротьби з новими формами кіберзлочинів, а саме: хакерські атаки та кібершахрайство. У роботі також зазначено, що для підвищення ефективності правозастосування необхідно створити спеціалізовані суди та прокуратури для розслідування кіберзлочинів.

Дослідник М. Ю. Якимчук [9] у своїй роботі аналізує особливості правового регулювання протидії кіберзлочинності в Україні у порівняльно-правовому аспекті. У публікації розглянуто розбіжності між українським та міжнародним законодавством і запропоновано рекомендації щодо гармонізації національних нормативно-правових актів із міжнародними стандартами, зокрема Європейським Союзом.

Публікація O. Kostenko et al. піднімає питання правового регулювання віртуальних простору та метавсесвіту, що є важливою складовою для розуміння нового напрямку кібербезпеки у майбутньому [11; 13].

Дослідження I. Kharytonenko [12] зосереджене на правових засадах гарантування кібербезпеки України в умовах цифрового комунікативного середовища. Автор розглядає розвиток цифрової інфраструктури та її безпеку як важливий елемент державної політики в умовах глобалізації та діджиталізації.

Виділення невирішених раніше частин загальної проблеми. Оцінка ефективності правових механізмів запобігання кіберзлочинності в Україні виявляє низку невирішених або частково вирішених аспектів, які потребують подальших досліджень та вдосконалення.

Основними нерозв'язаними проблемами залишаються питання адаптації правового регулювання до швидкого розвитку технологій, створення

ефективної системи міжнародної співпраці та підвищення рівня кваліфікації правоохоронців у боротьбі з кіберзлочинністю.

Потенційний внесок цієї публікації полягає в дослідженні цих проблем, аналізі міжнародного досвіду та розробці конкретних пропозицій щодо вдосконалення правових механізмів запобігання кіберзлочинності в Україні.

Формулювання цілей статті (постановка завдання). Метою цього дослідження є аналіз ефективності правових механізмів запобігання кіберзлочинності в Україні, виявлення основних проблем правозастосування та розробка рекомендацій щодо їх удосконалення.

Завдання дослідження полягає у:

1. аналізові чинної нормативно-правової бази України у сфері кібербезпеки;
2. визначенні основних проблеми правозастосування у цій сфері;
3. запропонуванні шляхів удосконалення правових механізмів запобігання кіберзлочинності.

Виклад основного матеріалу дослідження. Кіберзлочинність є одним із найсерйозніших викликів сучасного цифрового суспільства. Під цим поняттям зазвичай розуміють протиправні дії, що вчиняються у кіберпросторі та за допомогою інформаційно-комунікаційних технологій.

Відповідно до міжнародних підходів кіберзлочини поділяються на кілька основних категорій:

- злочини проти комп'ютерних систем (наприклад, несанкціонований доступ до інформації, її знищення чи модифікація);
- злочини з використанням інформаційних технологій (шахрайство, розповсюдження шкідливого програмного забезпечення, викрадення персональної інформації);
- злочини, пов'язані з контентом (кібертероризм, розповсюдження незаконної інформації, зокрема пропаганди насильства або дитячої порнографії).

ISSN: 3041-2110

Ефективне запобігання та боротьба з кіберзлочинністю неможливі без активної участі спеціалізованих правоохоронних органів. В Україні ключовими суб'єктами, що відповідають за кібербезпеку, є кіберполіція, Служба безпеки України, Державна служба спеціального зв'язку та захисту інформації України, а також підрозділи Міністерства оборони, які здійснюють контррозвідувальні заходи у кіберпросторі. Кіберполіція виконує функції з виявлення, розслідування та запобігання кіберзлочинам, тоді як СБУ зосереджується на питаннях кібертероризму, захисту критичної інфраструктури та інформаційної безпеки держави. Важливим аспектом є співпраця цих органів із міжнародними структурами, такими як Європол, Інтерпол, НАТО та Європейське агентство з кібербезпеки (ENISA), що дозволяє обмінюватися досвідом і координаційно реагувати на кіберзагрози.

Протидія кіберзлочинності потребує не лише посилення законодавчих норм і роботи правоохоронних органів, а й активного залучення приватного сектору та громадянського суспільства.

Банки, технологічні компанії, телекомунікаційні оператори відіграють важливу роль у гарантуванні інформаційної безпеки, впроваджуючи сучасні технології захисту інформації, системи кібермоніторингу та штучного інтелекту для виявлення загроз.

Водночас підвищення рівня цифрової грамотності населення є необхідною умовою для зменшення впливів, пов'язаних із людським фактором, адже більшість кіберзлочинів стає можливими через недостатню обізнаність користувачів щодо базових принципів інформаційної безпеки.

Запобігання кіберзлочинності в Україні здійснюється через систему правових механізмів, що охоплюють як національне законодавство, так і міжнародні угоди. Основним нормативним актом, що передбачає відповідальність за кіберзлочини, є Кримінальний кодекс України [14]. Зокрема, низка статей ККУ регулює питання несанкціонованого доступу до інформаційних систем (ст. 361), створення, розповсюдження та використання

 ISSN: 3041-2110

шкідливих програмних засобів (ст. 361-1), несанкціонованого втручання в роботу електронно-обчислювальних машин (ст. 362), порушення правил експлуатації комп'ютерних систем (ст. 363) та інші правопорушення, пов'язані з інформаційними технологіями [14].

Окрім кримінального законодавства, ключову роль у забезпеченні кібербезпеки відіграє Закон України «Про основи забезпечення кібербезпеки України» [15], який визначає правові та організаційні засади захисту кіберпростору держави. У законі закріплено основні принципи кіберзахисту, серед яких визнано пріоритетність державних інтересів у сфері кібербезпеки, взаємодія між державними органами та приватним сектором, відповідальність власників критичної інфраструктури за її кіберзахист. Також у ньому визначено повноваження державних органів, зокрема Державної служби спеціального зв'язку та захисту інформації України, Національної поліції, Служби безпеки України та інших суб'єктів, відповідальних за протидію кіберзагрозам.

Додатково питання кібербезпеки регулюються рядом підзаконних актів, зокрема постановами Кабінету Міністрів України щодо захисту критичної інфраструктури, нормативними документами щодо реагування на кіберінциденти, а також стратегіями розвитку цифрової безпеки держави. Важливим документом є Стратегія кібербезпеки України [16], яка визначає пріоритетні напрями розвитку національної системи кіберзахисту, серед яких зміцнення державного контролю за безпекою інформаційних систем, посилення нормативно-правового забезпечення та вдосконалення механізмів міжнародної співпраці.

Оцінка ефективності правозастосовної практики у сфері запобігання кіберзлочинності вказує на значні виклики. Попри наявність нормативної бази, Україна стикається з проблемами у сфері реалізації законодавчих норм. Одним із основних недоліків є низький рівень виявлення та розслідування кіберзлочинів. Кіберполіція України та інші правоохоронні органи не завжди

мають достатні технічні та кадрові ресурси для ефективного протистояння цифровим загрозам. У багатьох випадках розслідування кіберзлочинів обтяжується складністю збору доказової бази, використанням анонімних мереж (наприклад, даркнету), а також міжнародною кіберзлочинністю, що потребує взаємодії з іноземними правоохоронними структурами.

Співпраця України з міжнародними організаціями є одним із важливих напрямів посилення правових механізмів запобігання кіберзлочинності. Важливим кроком у цьому напрямі стало приєднання до Будапештської конвенції про кіберзлочинність [17], яка є першим міжнародним договором, що визначає спільні стандарти криміналізації кіберзлочинів та механізми міжнародної співпраці у сфері розслідування цифрових правопорушень. Відповідно до положень цієї конвенції Україна здійснює обмін інформацією про кіберзлочини з іншими державами, отримує технічну допомогу у розслідуванні та сприяє екстрадиції осіб, підозрюваних у вчиненні кіберзлочинів.

Крім того, Україна активно співпрацює з Європейським агентством із кібербезпеки (ENISA), Європолом, Інтерполом, а також бере участь у програмах НАТО, спрямованих на підвищення рівня кіберзахисту. Одним із важливих кроків стало укладення Меморандуму про співпрацю між Україною та Європолом [18], що передбачає обмін інформацією, проведення спільних операцій та вдосконалення методів боротьби з кіберзлочинністю.

Важливу роль у міжнародному співробітництві відіграє також участь України в проєктах Європейського Союзу, таких як CyberEast, який спрямований на підвищення спроможності правоохоронних органів у сфері кібербезпеки, навчання спеціалістів та розвиток нормативної бази відповідно до європейських стандартів.

Кібербезпека України залишається однією з ключових сфер національної безпеки, особливо в умовах гібридної війни та зростання кількості кібератак. Незважаючи на активні кроки держави у вдосконаленні

правового регулювання та міжнародної співпраці, низка проблем та викликів продовжують ускладнювати ефективне забезпечення кіберзахисту.

У таблиці 1 наведено основні загрози, з якими стикається Україна у сфері кібербезпеки, а також можливі шляхи їх подолання.

Таблиця 1

Основні проблеми та виклики у сфері кібербезпеки України

Проблема	**Опис**
Недостатнє фінансування	брак фінансових ресурсів для модернізації кіберзахисту, закупівлі сучасного обладнання та програмного забезпечення
Низький рівень цифрової грамотності	недостатня обізнаність громадян та державних службовців щодо основ кібербезпеки
Кадровий дефіцит у сфері кібербезпеки	брак кваліфікованих фахівців у правоохоронних органах, державних установах та приватному секторі
Слабка координація між державними органами	відсутність ефективної взаємодії між різними структурами, що відповідають за кібербезпеку
Зростання кількості кібератак	атаки на державні установи, бізнес і критичну інфраструктуру, особливо у воєнний час
Використання анонімних мереж злочинцями	кіберзлочинці використовують даркнет, VPN, шифрування для уникнення покарання

Джерело: власна розробка авторів.

Аналіз проблем у сфері кібербезпеки України свідчить про необхідність комплексного підходу до їх вирішення. Важливими напрямами є удосконалення законодавчої бази, підвищення рівня цифрової грамотності населення, посилення міжнародної співпраці та залучення додаткових ресурсів для розвитку кіберзахисту.

Враховуючи динамічний розвиток технологій та зростання загроз, Україні необхідно впроваджувати сучасні методи боротьби з кіберзлочинністю та розвивати національну систему кібербезпеки відповідно до міжнародних стандартів.

Важливим кроком у підвищенні ефективності боротьби з кіберзлочинністю є гармонізація українського законодавства з міжнародними стандартами. Україна поступово адаптує своє правове поле до вимог Європейського Союзу, Ради Європи та інших міжнародних організацій, зокрема шляхом імплементації положень Будапештської конвенції про кіберзлочинність. Удосконалення нормативно-правової бази має охоплювати не лише оновлення Кримінального кодексу України та Закону «Про основи забезпечення кібербезпеки України», а й запровадження чітких механізмів взаємодії між державними установами, приватним сектором та міжнародними партнерами. Крім того, важливо розробити ефективні процедури для розслідування кіберзлочинів, що враховуватимуть специфіку цифрових доказів та швидкоплинність кіберзагроз.

Окрім правового аспекту, значну роль у зміцненні кібербезпеки відіграє впровадження сучасних технологій для кіберзахисту. У сучасних умовах держава має активно використовувати штучний інтелект, машинне навчання та аналітику об’ємної інформації для виявлення та попередження кіберзагроз. Розвиток національної системи моніторингу кіберінцидентів, створення єдиної бази даних про кібератаки та обмін інформацією між державними органами та приватними компаніями сприятиме швидкому реагуванню на потенційні загрози. Важливим напрямом також є впровадження механізмів багаторівневої автентифікації, шифрування інформації та захисту критичної інфраструктури.

Окремим викликом у сфері запобігання кіберзлочинності є недостатній рівень цифрової грамотності населення. Багато громадян та державних службовців не володіють базовими навичками кібергігієни, що збільшує

ISSN: 3041-2110

ризики фішингових атак, витоку персональної інформації та інших форм шахрайства. Підвищення рівня кіберкультури може бути досягнуте шляхом запровадження освітніх програм з кібербезпеки у школах, університетах та на рівні корпоративного навчання. Державні інформаційні кампанії, роз'яснювальні заходи та створення онлайн-платформ з рекомендаціями щодо безпечного користування інтернетом сприятимуть формуванню відповідальної поведінки в цифровому середовищі.

Таким чином, ефективне запобігання кіберзлочинності вимагає комплексного підходу: удосконалення законодавства, інтеграцію сучасних технологій у систему кіберзахисту та підвищення цифрової грамотності суспільства. Україна має орієнтуватися на міжнародний досвід та адаптувати найкращі практики для посилення власної кібербезпеки, що є необхідною умовою для захисту національних інтересів у цифрову епоху.

Висновки. Аналіз правових механізмів запобігання кіберзлочинності в Україні свідчить про те, що, незважаючи на значні кроки у розвитку нормативно-правової бази та посилення міжнародної співпраці, існує низка викликів, які потребують негайного вирішення.

Кіберзагрози стають дедалі складнішими, а зловмисники використовують новітні технології для уникнення захисних механізмів, що створює постійну необхідність удосконалення підходів до кібербезпеки.

Дослідження підтвердило, що ефективне протистояння кіберзлочинності можливе лише за умови комплексного підходу, який поєднує вдосконалення законодавства, впровадження інноваційних технологій у систему кіберзахисту та підвищення цифрової грамотності громадян.

Для підвищення ефективності правового регулювання кібербезпеки необхідно гармонізувати українське законодавство з міжнародними стандартами, зокрема адаптувати правові механізми до вимог Європейського Союзу та Будапештської конвенції про кіберзлочинність.

ISSN: 3041-2110

Важливим напрямом є розробка та впровадження ефективних процедур розслідування кіберзлочинів, а також нормативне врегулювання збору та аналізу цифрових доказів. Крім того, потребує вдосконалення координація між державними органами, приватним сектором і міжнародними партнерами для оперативного обміну інформацією про кіберзагрози.

У сфері правозастосовної практики ключовим завданням є підвищення кваліфікації правоохоронних органів та спеціалізованих установ у сфері кібербезпеки. Необхідно розширювати можливості Національної поліції України, Служби безпеки України та інших відповідальних органів у питаннях виявлення, запобігання та розслідування кіберзлочинів, а також забезпечити їхню технічну оснащеність. Необхідним є розвиток механізмів кіберзахисту критичної інфраструктури, зокрема шляхом впровадження сучасних систем моніторингу та реагування на кібератаки.

Перспективи подальших досліджень у сфері кібербезпеки полягають у вивченні новітніх методів боротьби з кіберзлочинністю, аналізі світового досвіду у сфері захисту інформаційного простору та пошуку інноваційних рішень для протидії цифровим загрозам. Особливу увагу варто приділити використанню штучного інтелекту та машинного навчання для автоматизованого виявлення та нейтралізації кібератак. Також перспективним напрямом є розробка стратегій інформаційної безпеки на рівні державних і приватних структур, що дозволить створити ефективну систему кіберзахисту та мінімізувати ризики для національної безпеки.

Таким чином, подальший розвиток правових механізмів кібербезпеки в Україні має бути спрямований на посилення нормативного регулювання, впровадження інноваційних технологій та підвищення загального рівня цифрової культури. Лише комплексний підхід дозволить ефективно протидіяти кіберзлочинності та забезпечити стабільний розвиток цифрової інфраструктури держави в умовах сучасних викликів.

ISSN: 3041-2110

Список використаних джерел

1. Саєнко М.І., Савела Є.А., Тополянський Ю.Ю. Міжнародний досвід протидії кіберзлочинності та кібершахрайству. *Науковий вісник Ужгородського Національного Університету.* 2021. Випуск 64. DOI https://doi.org/10.24144/2307-3322.2021.64.7
2. Аніщук В.В., Зицик С.Г. Проблема протидії кіберзлочинності: порівняльно-правовий аналіз. *Науковий вісник Ужгородського Національного Університету.* 2024. Випуск 83. DOI https://doi.org/10.24144/2307-3322.2024.83.3.2
3. Козій А., Марченко Т., Шевченко В. Актуальні проблеми протидії кіберзлочинності в Україні. *Theoretical foundations of state and law*. 2022. P. 59–65. URL: https://doi.org/10.46299/isg.2022.mono.legal.1.2.3 (date of access: 18.01.2025).
4. Коцман І. І. Державне регулювання протидії кіберзлочинності в Україні: поняття та основні напрямки. *Public management and administration in Ukraine.* 2024. № 40. С. 245–252. URL: https://doi.org/10.32782/pma2663-5240-2024.40.41 (дата звернення: 18.01.2025).
5. Лугіна Н. А., Лучук А. М. Порівняльний аналіз вітчизняного та європейського законодавства з питань запобігання кіберзлочинності. *Ірпінський юридичний часопис*. 2023. № 1(10). С. 180–186. URL: https://doi.org/10.33244/2617-4154-1(10)-2023-180-186 (дата звернення: 18.01.2025).
6. Мордань Є. Ю., Бардакова В. В., Сокол Л. В. Удосконалення вітчизняної системи протидії кіберзлочинності та кібершахрайству на основі впровадження міжнародного досвіду. *Efektyvna ekonomika*. 2023. № 10. URL: https://doi.org/10.32702/2307-2105.2023.10.38 (дата звернення: 18.01.2025).
7. Сащенко М. Проблемні аспекти запобігання кіберзлочинності в Україні. *Молодий вчений.* 2022. № 1 (101). С. 17–20. URL:

https://doi.org/10.32839/2304-5809/2022-1-101-4 (дата звернення: 18.01.2025).

8. Флис І. Правове реформування кіберзахисту. *Expert paradigm of law and public administration.* 2024. № 4(32). С. 44–51. URL: https://doi.org/10.32689/2617-9660-2024-4(32)-44-51 (дата звернення: 18.01.2025)
9. Хахановський В. Г., Гавловський В. Д. Кримінально-правове забезпечення протидії кіберзлочинності, особливості кваліфікації кіберзлочинів в Україні. *Європейський правничий часопис*. 2023. № 1. С. 38–45. URL: https://doi.org/10.36919/elj.1.2023.37 (дата звернення: 18.01.2025).
10. Якимчук М. Ю. Особливості правового регулювання протидії кіберзлочинності в Україні: порівняльно-правовий аспект. New Ukrainian law. 2021. № 4. С. 182–186. URL: https://doi.org/10.51989/nul.2021.4.27 (дата звернення: 18.01.2025).
11. Genesis of legal regulation web and the model of the electronic jurisdiction of the metaverse / O. Kostenko et al. Bratislava law review. 2022. Vol. 6, no. 2. P. 21–36. URL: https://doi.org/10.46282/blr.2022.6.2.316 (date of access: 18.01.2025).
12. Kharytonenko I. Правові засади забезпечення кібербезпеки України в умовах цифрового комунікативного середовища. *Law review of kyiv university of law.* 2023. № 2. С. 61–64. URL: https://doi.org/10.36695/2219-5521.2.2023.12 (дата звернення: 18.01.2025).
13. Metaverse: model criminal code / O. Kostenko et al. *Baltic journal of economic studies.* 2023. Vol. 9, no. 4. P. 134–147. URL: https://doi.org/10.30525/2256-0742/2023-9-4-134-147 (date of access: 18.01.2025).
14. Кримінальний кодекс України : Кодекс України від 05.04.2001 № 2341-III: станом на 01.02.2025. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 18.01.2025).

 ISSN: 3041-2110

15. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : станом на 28.06.25. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 18.01.2025).
16. Про Стратегію кібербезпеки України : Рішення Ради національної безпеки і оборони України від 14.05.2021 : станом на 28.08.2021. URL: https://zakon.rada.gov.ua/laws/show/n0055525-21#Text (дата звернення: 18.01.2025).
17. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 07.09.2005 № 2824-IV: станом на 14.10.2010. URL: https://zakon.rada.gov.ua/laws/show/2824-15#Text (дата звернення: 18.01.2025).
18. Меморандум про взаєморозуміння між Україною та Європейським поліцейським офісом щодо встановлення захищеної лінії зв'язку : Меморандум України від 11.03.2015: станом на 04.06.2015. URL: https://zakon.rada.gov.ua/laws/show/984_a12#Text (дата звернення: 18.01.2025).

ISSN: 3041-2110