ІНФОРМАЦІЙНЕ ПРАВО; ПРАВО ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

УДК 351.746:004.056.5(477) **DOI:** https://doi.org/10.32631/v.2025.2.33

Віктор Михайлович Василенко,
доктор юридичних наук, доцент,
Харківський національний університет
внутрішніх справ (перший проректор);
https://orcid.org/0000-0002-9313-861X,
e-mail: Vasylenko_Viktor@ukr.net

НАЦІОНАЛЬНА КІБЕРБЕЗПЕКА В УМОВАХ ДИДЖИТАЛІЗАЦІЇ СУСПІЛЬСТВА: РОЛЬ ПОЛІЦІЇ В ЗАХИСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

У статті акцентовано увагу на тому, що в сучасних умовах цифрової трансформації національна кібербезпека набула особливого значення як один із пріоритетних напрямів державної політики, спрямованої на захист суспільства, економіки та національних інтересів. У контексті воєнної агресії проти України, масових кібератак на державні органи й об'єкти стратегічного значення питання ефективного функціонування національної системи кібербезпеки стає особливо актуальним. Дослідження присвячене аналізу ролі поліції як одного із ключових суб'єктів системи кібербезпеки, що здійснює правоохоронну діяльність у кіберпросторі, запобігає кіберзлочинам і розслідує їх, взаємодіє з іншими органами державної влади, командами реагування на інциденти, суб'єктами приватного сектору та громадянським суспільством. Сформульовано висновки щодо необхідності впровадження системних підходів до підвищення ефективності діяльності поліції у сфері кібербезпеки з урахуванням європейських стандартів і міжнародного досвіду, що є важливим чинником формування національної стійкості перед кіберзагрозами.

Ключові слова: національна кібербезпека, критична інфраструктура, поліція, кіберзлочинність, кіберзагрози, CERT, взаємодія, цифрова трансформація, Будапештська конвенція про кіберзлочинність, NIS2.

Оглядова стаття

Постановка проблеми

Сучасна епоха характеризується стрімким переходом до цифрової форми організації суспільних процесів, що відкриває перед державою та громадянами як нові можливості, так і нові ризики. Активне впровадження цифрових технологій у системи державного управління, фінансовий сектор, енергетику, транспорт і комунікаційні мережі призводить до істотного зростання залежності критичної інфраструктури

від кіберпростору. Водночас кількість і складність кібератак на об'єкти цієї інфраструктури зростають у геометричній прогресії. Актуальність проблеми посилюється ще й тим, що Україна перебуває у стані збройної агресії з боку російської федерації, у межах якої кіберпростір використовується як один з інструментів ведення гібридної війни. За таких умов забезпечення стійкості критичної інфраструктури до кіберзагроз постає питанням національної безпеки. Одним із ключових елементів реагування на ці виклики є правоохоронна система держави, зокрема поліція, яка виконує функції попередження, виявлення, фіксації кіберзлочинів та розслідування інцидентів у кіберпросторі. Однак виникає низка системних проблем. По-перше, рівень цифрової зрілості та технічної спроможності правоохоронних органів у багатьох випадках не відповідає швидкості розвитку кіберзагроз. По-друге, законодавча й нормативно-правова база у сфері кібербезпеки не завжди дозволяє поліції ефективно діяти в міжвідомчому форматі, зокрема у взаємодії з іншими суб'єктами системи кібербезпеки (CERT, Службою безпеки України, Державною службою спеціального зв'язку та захисту інформації України, приватними компаніями – операторами критичної інфраструктури). По-третє, спостерігається фрагментарність координації зусиль, відсутність чітких регламентів обміну інформацією між поліцією, спеціалізованими командами реагування та приватним сектором. Крім того, відсутність належної підготовки кадрів, недостатнє фінансування підрозділів кіберполіції, брак сучасного програмно-аналітичного забезпечення негативно впливають на спроможність поліції ефективно реагувати на складні, багатоетапні та транснаціональні кібератаки. Особливу складність становить також проблема збору, обробки та використання цифрових доказів, що потребує оновлення методологічної бази криміналістики та слідчої практики.

Важливим аспектом є і правова колізійність у питаннях юрисдикції та процедурної взаємодії, зокрема в умовах транскордонної кіберзлочинності. Без узгодження національних стандартів із міжнародними інструментами (такими як Директива ЄС NIS2, Будапештська конвенція про кіберзлочинність) Національна поліція України не зможе повноцінно інтегруватися у глобальні механізми кібербезпеки й ефективно брати участь у міжнародних розслідуваннях.

На цьому тлі постає проблема формування ефективної, інтегрованої, технологічно оснащеної моделі діяльності поліції у сфері кібербезпеки як складової загальнодержавної системи захисту критичної інфраструктури. Це вимагає не лише модернізації технічної бази та підготовки персоналу, а й глибокого перегляду організаційних структур, механізмів міжвідомчої взаємодії та процедур правового регулювання. Актуальним також є завдання побудови стійкої комунікації

між поліцією, суб'єктами критичної інфраструктури та громадянським суспільством з метою підвищення рівня кіберстійкості національної економіки загалом. Таким чином, проблема, що потребує наукового осмислення, полягає не лише в підвищенні спроможності поліції до протидії кіберзагрозам, а й у створенні цілісної моделі інтегрованої взаємодії поліції з іншими суб'єктами кібербезпеки в контексті сучасної диджиталізації держави з урахуванням стандартів європейського та міжнародного права.

Стан дослідження проблеми

Проблематика національної кібербезпеки, зокрема в контексті цифровізації суспільства та діяльності правоохоронних органів у сфері захисту критичної інфраструктури, в останнє десятиліття привертає дедалі більшу увагу як вітчизняних, так і зарубіжних дослідників. Активізація кіберзагроз, особливо в умовах гібридної війни проти України, зумовила появу великої кількості наукових праць, які аналізують як технічні, так і правові й організаційні аспекти протидії кіберзлочинності.

У вітчизняному правознавчому дискурсі важливе місце посідають праці, присвячені нормативному забезпеченню кібербезпеки (О. В. Волощук, П. В. Пашко), у яких розглядаються проблеми імплементації європейських стандартів у національне законодавство. Науковці наголошують на необхідності системної гармонізації української правової бази з положеннями Директиви ЄС NIS2 та Будапештської конвенції про кіберзлочинність з урахуванням реалій воєнного часу.

Значний внесок у розроблення організаційних моделей взаємодії правоохоронних органів із суб'єктами кібербезпеки зроблено у працях А. С. Барановського та І. М. Чепурного, які акцентують увагу на важливості створення ефективної міжвідомчої платформи для обміну оперативною інформацією між поліцією, CERT-структурами, підрозділами Служби безпеки України та приватними операторами критичної інфраструктури. Дослідники наголошують на наявності проблем у забезпеченні єдності стандартів реагування та уніфікації протоколів взаємодії.

Серед досліджень, зосереджених на практичних викликах діяльності кіберпідрозділів поліції, варто відмітити праці В. О. Дьяченка та С. В. Коваля, у яких аналізуються сучасні методи документування цифрових доказів, питання доказової сили таких матеріалів у кримінальному процесі, а також необхідність оновлення криміналістичних методик для розслідування складних кібератак. Окрема увага в цих дослідженнях приділяється проблемі збереження балансу між ефективністю оперативної діяльності та дотриманням прав людини в умовах використання електронних засобів контролю та спостереження.

У контексті європейського досвіду цифрової трансформації правоохоронних органів слід згадати публікації Х. Ріхтера та Д. Левіса, які аналізують практики взаємодії поліції із приватним сектором у країнах ЄС, механізми забезпечення прозорості використання алгоритмічних систем у правоохоронній діяльності, а також стандарти підготовки поліцейських кадрів до роботи в умовах цифрового середовища.

Попри наявність цінних наукових напрацювань, варто зазначити, що в літературі домінує фрагментарний підхід до розгляду проблеми: здебільшого аналізуються окремі аспекти (правові, технічні або організаційні) без цілісного бачення взаємозв'язку між діяльністю поліції та загальнодержавною системою кібербезпеки в умовах диджиталізації. Недостатньо опрацьованими залишаються питання ефективної інтеграції правоохоронної діяльності в єдину національну систему кіберзахисту критичної інфраструктури, розроблення процедур міжвідомчої взаємодії в умовах кібератак великого масштабу, а також ролі поліції в забезпеченні правової визначеності під час роботи із цифровими доказами. Крім того, у більшості публікацій поки що недостатньо враховано унікальний досвід України, набутий під час відбиття кіберзагроз у період повномасштабної агресії рф, а також необхідність адаптації світових стандартів до реалій воєнного та постконфліктного середовища. Саме тому подальший розвиток наукових досліджень у цьому напрямі залишається актуальним, із фокусом на створенні комплексної моделі участі поліції в системі національної кібербезпеки як в умовах кризи, так і з метою довгострокового підвищення кіберстійкості держави.

Мета і завдання дослідження

Метою статті є наукове обґрунтування ролі та місця поліції в системі забезпечення національної кібербезпеки в умовах активної диджиталізації суспільства, а також виявлення правових, організаційних і практичних механізмів ефективного залучення поліції до захисту критичної інфраструктури від кіберзагроз. У центрі дослідження перебувають такі *завдання*: розроблення концептуальної моделі міжвідомчої взаємодії поліції з іншими суб'єктами кібербезпеки – командами CERT, Службою безпеки України, органами сектору оборони та безпеки, а також операторами об'єктів критичної інфраструктури; оцінка сучасного стану нормативно-правового регулювання участі поліції у сфері кібербезпеки, визначення його відповідності міжнародним стандартам та актуальним загрозам; аналіз кадрових і технологічних чинників, що впливають на готовність поліції до виконання завдань у сфері кібербезпеки, зокрема визначення потреб у розвитку цифрової компетентності працівників, оновленні методів слідчої та оперативної діяльності, використанні сучасних аналітичних платформ.

Виклад основного матеріалу

Сучасна епоха позначена стрімкою диджиталізацією, яка проникає в усі сфери суспільного життя. Державні послуги дедалі активніше переходять у формат електронного врядування, економічні процеси стають залежними від цифрових платформ, а повсякденна діяльність громадян – від інформаційно-комунікаційних технологій. Однак поряд з очевидними перевагами цього процесу формуються й серйозні виклики: зокрема, кібератаки на критичну інфраструктуру держави стали одним із найнебезпечніших чинників загрози національній безпеці. Порушення стабільної роботи енергетичних об'єктів, транспортної мережі, фінансової системи може мати катастрофічні наслідки як для економіки, так і для суспільства загалом. Тому питання кіберзахисту цифрової інфраструктури закономірно перетворюється на один із ключових національних пріоритетів. За таких умов успішне протистояння кіберзагрозам потребує цілісної системи кібербезпеки, у межах якої відбувається об'єднання зусиль державних інституцій, приватного сектору та громадянського суспільства. Особливе місце в цій системі посідають органи поліції. Як структура, наділена повноваженнями щодо захисту прав громадян, охорони суспільного порядку та розслідування правопорушень, поліція відіграє важливу роль у забезпеченні законності в кіберпросторі. Її діяльність охоплює розслідування кіберзлочинів, притягнення винних до відповідальності, профілактику злочинних посягань у цифровому середовищі. Проте ефективність правоохоронної діяльності в цій сфері значною мірою залежить від здатності діяти у взаємодії з іншими суб'єктами кібербезпеки. Поліція не може працювати у відриві від фахових технічних структур, які мають відповідні ресурси для виявлення, аналізу та нейтралізації кіберінцидентів у режимі реального часу. Насамперед це стосується співпраці з урядовими командами реагування на інциденти (CERT/CSIRT), які виконують ключові функції з технічного захисту інформаційних систем і об'єктів критичної інфраструктури.

Важливим елементом системи кібербезпеки є взаємодія поліції з приватним сектором. Саме приватні компанії володіють значною часткою критичних IT-ресурсів і технологій, а отже, першими стикаються з кіберзагрозами. Для ефективного захисту необхідний постійний обмін інформацією між поліцією, бізнесом і технічними структурами щодо новітніх загроз, методів атак, шляхів нейтралізації. Таке партнерство дає змогу оперативніше реагувати на інциденти, підвищувати стійкість об'єктів критичної інфраструктури та формувати єдиний фронт боротьби з кіберзлочинністю. Не менш важливою є роль громадянського суспільства в системі кібербезпеки. Підвищення цифрової грамотності населення, формування культури кібергігієни, активна участь у спільних ініціативах із забезпечення

кібербезпеки сприяють зменшенню вразливості суспільства перед кіберзагрозами. Довіра між громадянами, бізнесом і державними органами стає запорукою ефективного функціонування кібербезпекового середовища. Практика розвинених країн демонструє: лише завдяки комплексному підходу і тісній взаємодії всіх зацікавлених сторін можна досягти належного рівня захисту цифрової інфраструктури. Досвід держав Європейського Союзу, США та інших країн підтверджує, що синергія зусиль правоохоронних органів, CERT-структур, приватного сектору і громадськості є ключовим чинником у протидії сучасним кіберзагрозам. Це відображено й у новітніх стратегічних документах ЄС, зокрема в Директиві NIS2, яка закріплює зобов'язання держав щодо розвитку багаторівневої системи кібербезпеки з урахуванням ролі поліції.

В українському контексті така модель також поступово формується. Законодавство України, зокрема закони «Про основні засади забезпечення кібербезпеки України» (2017) та «Про критичну інфраструктуру» (2021), визначає основні підходи до захисту цифрового простору та структурує взаємодію суб'єктів кібербезпеки. При цьому міжнародні зобов'язання України, зокрема участь у Будапештській конвенції про кіберзлочинність, забезпечують узгодженість національної системи з європейськими та світовими стандартами. У сучасних умовах кіберпростір перетворився на новий театр загроз, що потребує адекватної відповіді з боку всіх інституцій суспільства. Поліція як орган, що стоїть на сторожі законності, має відігравати в цьому процесі активну й координуючу роль, спираючись на партнерство з технічними структурами, бізнесом і громадськістю. Саме така модель здатна забезпечити належний рівень національної кіберстійкості в умовах глобальної цифрової трансформації.

Цифрова трансформація держави у XXI столітті суттєво змінила як механізми публічного управління, так і характер взаємодії між державою та громадянами. Упровадження електронного врядування, концепції «держава в смартфоні», цифрового документообігу та онлайн-сервісів забезпечило новий рівень прозорості, доступності й ефективності державних послуг. Водночас стрімкий розвиток цифрових технологій призвів до появи нових викликів і вразливостей. Критично важливі елементи функціонування держави та суспільства дедалі більше залежать від стабільності кіберпростору. Відсутність належного кіберзахисту або несанкціоноване втручання в роботу інформаційних систем можуть спричинити масштабні збої, паралізувати діяльність органів державної влади, бізнесу та соціальних інституцій[1]. Саме тому кібербезпека сьогодні розглядається як

[1] Critical Infrastructure Protection: National Cybersecurity Strategy Needs to Address Information Sharing Performance Measures and Methods // U.S.

невід'ємна складова національної безпеки, а захист критичної інформаційної інфраструктури визначено одним із пріоритетних напрямів державної політики у сфері безпеки. Критична інфраструктура охоплює найважливіші сектори життєзабезпечення держави: енергетику, транспорт, зв'язок, фінансову систему, охорону здоров'я, водопостачання, державне управління та оборону. Будь-які кіберінциденти у цих сферах можуть мати серйозні наслідки не лише для економіки, а й для громадської безпеки та соціальної стабільності. Забезпечення стійкості критичної інфраструктури в умовах сучасних кіберзагроз вимагає комплексного підходу, який передбачає не лише технічне зміцнення цифрових систем, але й ефективне правове регулювання, координацію дій усіх суб'єктів національної системи кібербезпеки, а також інтеграцію національних зусиль у міжнародну безпекову систему.

В Україні створено базові правові засади для розвитку національної системи кібербезпеки. Ключовим нормативно-правовим актом у цій сфері є Закон України «Про основні засади забезпечення кібербезпеки України». Цей Закон закріплює понятійний апарат, визначає принципи державної політики у сфері кібербезпеки, коло відповідальних суб'єктів та їхні повноваження. Національна система кібербезпеки має багаторівневу структуру, яка охоплює органи державної влади, правоохоронні органи, сили оборони, регуляторні установи, суб'єктів господарювання – операторів критичної інфраструктури, а також громадські організації, що діють у сфері кібербезпеки. Координація державної політики у сфері кібербезпеки покладена на Раду національної безпеки і оборони України, яка здійснює її через Національний координаційний центр кібербезпеки [1, с. 328]. Відповідно до чинного законодавства всі суб'єкти зобов'язані: запобігати використанню кіберпростору у злочинних цілях, своєчасно виявляти та реагувати на кіберінциденти, усувати їх наслідки, впроваджувати превентивні заходи та брати участь у міжвідомчому обміні інформацією.

Окрему роль у законодавчому забезпеченні кібербезпеки відіграє Закон України «Про критичну інфраструктуру», який заклав нормативну основу для класифікації об'єктів за рівнем критичності та встановив вимоги до їх кіберзахисту. Практична реалізація цих вимог деталізується в постановах Кабінету Міністрів України, які регламентують стандарти захисту мереж, систем, підходи до управління ризиками, а також процедури моніторингу безпеки. Крім внутрішнього законодавства, важливу роль у формуванні національної кіберполітики

Government Accountability Office : сайт. URL: https://www.gao.gov/products/gao-23-105468 (дата звернення: 18.05.2025).

відіграють міжнародні правові акти. Україна активно гармонізує національні стандарти з європейськими нормами, зокрема з Директивою ЄС NIS2. Цей документ висуває високі вимоги до кіберстійкості операторів критичної інфраструктури, зобов'язує створювати ефективні механізми державного нагляду та регламентує оперативний обмін інформацією між суб'єктами кібербезпеки на національному й міжнародному рівнях [2, с. 132]. Особливу увагу приділено формуванню команд реагування на кіберінциденти (CSIRTs), які повинні стати ядром системи швидкого реагування на масштабні загрози в кіберпросторі. Міжнародним правовим інструментом, що становить основу боротьби з кіберзлочинністю, є Будапештська конвенція про кіберзлочинність, до якої Україна приєдналася у 2005 році. Ця конвенція зобов'язує держав-учасниць установити кримінальну відповідальність за ключові види кіберзлочинів, а також сприяє розвитку міжнародного співробітництва між правоохоронними органами в розслідуванні кіберінцидентів, екстрадиції правопорушників і забезпеченні правової допомоги.

Таким чином, національна система кібербезпеки України ґрунтується на комплексному поєднанні внутрішніх правових норм і міжнародно-правових зобов'язань, що дозволяє державі вибудовувати ефективну модель реагування на кіберзагрози в тісній взаємодії з європейськими та глобальними партнерами. Питання практичної імплементації цієї моделі значною мірою залежить від ефективної діяльності правоохоронних органів, зокрема Національної поліції України, яка є одним із ключових суб'єктів системи кібербезпеки. Її роль і завдання у сфері захисту критичної інфраструктури потребують окремого ґрунтовного дослідження.

Національна поліція України, зокрема її спеціалізований Департамент кіберполіції, є одним із ключових суб'єктів забезпечення кібербезпеки держави. Згідно із Законом України «Про основні засади забезпечення кібербезпеки України» на поліцію покладаються завдання із захисту прав і свобод людини, інтересів суспільства та держави від протиправних посягань у кіберпросторі, вжиття заходів із запобігання, виявлення, припинення та розкриття кіберзлочинів, а також підвищення обізнаності громадян щодо безпеки в кіберпросторі. Таким чином, поліція виконує як правоохоронну, так і профілактичну функції у сфері кібербезпеки: розслідує злочини, вчинені з використанням інформаційних технологій, і водночас інформує населення про нові кіберзагрози, попереджає кіберзлочинність [3, с. 37].

Департамент кіберполіції було утворено у 2015 році у структурі кримінальної поліції, що стало свідченням усвідомлення державою критичної необхідності мати спеціалізований підрозділ, орієнтований

на боротьбу з ІТ-злочинністю. Кіберполіція є міжрегіональним територіальним органом, її підрозділи діють по всій території України, а також вона інтегрована в міжнародні мережі співробітництва правоохоронців у сфері кібербезпеки. До основних завдань Департаменту кіберполіції належать: 1) реалізація державної політики у сфері протидії кіберзлочинності; 2) своєчасне інформування населення про появу новітніх кіберзлочинів і шахрайських схем; 3) впровадження сучасних програмно-технічних засобів для моніторингу кіберінцидентів, аналізу кіберзагроз і кіберзлочинів; 4) взаємодія з іноземними партнерами через цілодобову мережу контактних пунктів (24/7) для термінового обміну інформацією; 5) участь у підвищенні кваліфікації працівників поліції з використання інформаційних технологій та забезпечення діяльності глобальної мережі контактних пунктів, що об'єднує понад 90 країн світу; 7) безпосереднє запобігання кіберзлочинам та їх розслідування. Фактично ці напрями охоплюють як внутрішню діяльність (розкриття злочинів, профілактика в межах країни), так і зовнішню – активну міжнародну співпрацю[1]. Особливо важливою є інтеграція української кіберполіції у глобальні механізми міжнародного правоохоронного співробітництва. Вона є активним учасником міжнародної мережі 24/7 Network, створеної відповідно до положень Будапештської конвенції про кіберзлочинність, співпрацює з Європолом (зокрема, через Європейський центр з протидії кіберзлочинності – ЕС3) та Інтерполом, а також бере участь у спільних транснаціональних кібероперераціях. Таке співробітництво забезпечує можливість швидкого реагування на транскордонні кіберзагрози в режимі реального часу, адже злочинці часто діють поза межами юрисдикції, використовуючи мережу Інтернет, і лише колективні дії можуть їх зупинити.

На нашу думку, роль поліції у сфері національної кібербезпеки полягає в тому, щоб стояти на сторожі закону в кіберпросторі – своєчасно виявляти та припиняти злочинні посягання, розслідувати інциденти, притягати винних до відповідальності, а також профілактувати нові загрози через взаємодію із суспільством. Поліція виконує функцію ключової ланки між технічною сферою кіберзахисту та правовою системою: трансформуючи технічний факт кіберінциденту в юридичну площину, тобто в межі кримінального провадження. Водночас ефективність цієї діяльності значною мірою залежить від співпраці з іншими підрозділами.

З огляду на комплексний характер сучасних кіберзагроз жоден суб'єкт – ні держава, ні бізнес, ні, тим більше, окремі громадяни – не

[1] Кіберполіція : офіц. сайт. URL: https://cyberpolice.gov.ua/ (дата звернення: 18.05.2025).

здатен самостійно гарантувати кібербезпеку. Для ефективної протидії кіберзагрозам необхідна синергія зусиль усіх учасників кіберпростору. Ключову роль у цьому процесі відіграють урядові команди реагування на комп'ютерні надзвичайні події, такі як CERT-UA в Україні чи національні CSIRT у країнах Європейського Союзу. Вони відповідають за моніторинг і технічне реагування на кіберінциденти: відслідковують атаки, надають рекомендації щодо ліквідації їх наслідків, підвищують готовність систем до атак[1]. Поліція ж здійснює кримінальне розслідування і переслідування зловмисників. Ці функції різні, але доповнюють одна одну[2]. Ефективна протидія серйозним інцидентам потребує спільної роботи CERT і поліції: технічні фахівці повинні швидко інформувати правоохоронців, якщо атака має злочинний характер, а поліцейські – надавати зворотну інформацію про потрібні докази, координувати дії для збереження слідів злому [4, с. 105]. В українських реаліях така співпраця закріплена нормативно. Закон України «Про основні засади забезпечення кібербезпеки України» прямо вказує, що одним із завдань CERT-UA є взаємодія із правоохоронними органами та своєчасне їх інформування про кібератаки [5, с. 120]. Коли CERT-UA (функціонує при Державній службі спеціального зв'язку та захисту інформації України) фіксує атаку на об'єкт критичної інфраструктури, вона негайно повідомляє про це Департамент кіберполіції та Службу безпеки України[3]. Показовим прикладом ефективної міжвідомчої взаємодії стала масована кібератака, здійснена 15 лютого 2022 року на українські банки та органи державної влади (через DDoS та деструктивні malware). Урядова команда реагування CERT-UA оперативно зафіксувала інцидент і залучила Департамент кіберполіції для розслідування, зокрема відслідковування каналів управління ботнетами, що здійснювали DDoS-атаки[4]. У Європейському Союзі тема співпраці між CSIRT і правоохоронними органами вважається одним із ключових пріоритетів кіберстратегії. Європейське агентство

---

1 Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX // База даних (БД) «Законодавство України» / Верховна Рада (ВР) України. URL: https://zakon.rada.gov.ua/laws/show/1882-20 (дата звернення: 18.05.2025).

2 Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 18.05.2025).

3 Урядова команда CERT-UA в 2023 році опрацювала 2543 кіберінциденти // Державна служба спеціального зв'язку та захисту інформації України : офіц. сайт. 08.02.2024. URL: https://cip.gov.ua/ua/news/uryadova-komanda-cert-ua-v-2023-roci-opracuvala-2543-kiberincidenti (дата звернення: 18.05.2025).

4 Інформація щодо кібератак 15 лютого 2022 року // CERT-UA : сайт. 18.02.2022. URL: https://cert.gov.ua/article/37139 (дата звернення: 18.05.2025).

з кібербезпеки ENISA підготувало низку рекомендацій та аналітичних звітів, спрямованих на покращення координації між цими двома групами суб'єктів. ENISA наголошує, що традиційно команди реагування і поліція мають відмінності в культурах реагування: технарі фокусуються на нейтралізації інциденту «тут і зараз» (відновити роботу, закрити уразливість), а слідчі – на зборі доказів для суду, що може вимагати більше часу і формальностей [6, с. 857]. Тому важливо вибудувати довіру і зрозуміти потреби одне одного. Одним з успішних прикладів є створення у країнах ЄС спільних платформ обміну інформацією про інциденти, доступних як для CSIRT, так і для поліції. Такі платформи дозволяють у режимі реального часу ділитися інформацією про нові види атак, IoC (індикатори компрометації), підозрілі домени тощо [7, с. 175]. Учасники співпраці виробляють протоколи: які саме дані команди CERT можуть передавати поліції без порушення вимог конфіденційності, як ці дані можуть бути використані правоохоронними органами у кримінальному провадженні, як поліція, у свою чергу, може надавати зворотну аналітичну інформацію CERT. В Україні важливим кроком у цьому напрямі стало створення Національної телекомунікаційної платформи кібербезпеки – проєкту під координацією Ради національної безпеки і оборони України. Ця платформа фактично є інформаційною системою обміну кіберінформацією, до якої входять державні органи, Національна поліція та низка великих приватних компаній – операторів критичної інфраструктури [8, с. 601]. Очікується, що цей механізм дозволить забезпечити скоординованість дій і своєчасне вжиття заходів для запобігання або нейтралізації атак.

Ми переконані, що синергія між поліцією, CERT, приватним сектором і громадянським суспільством є наріжним каменем національної кіберстійкості. Кожен із цих учасників відіграє унікальну роль: поліція привносить свої особливі повноваження та компетенції – право на примус, досвід проведення розслідувань, можливість притягнення до відповідальності; CERT забезпечує технічну глибину та швидкість реагування; приватний сектор володіє ресурсами, інфраструктурою, ноу-хау та як основна мішень кібератак має пряму зацікавленість у співпраці; громадянське суспільство додає гнучкості, інноваційності та легітимності державним діям (через суспільний контроль і просвіту). Коли всі ці елементи взаємодіють злагоджено й скоординовано – кібербезпека держави виходить на якісно новий рівень. Український та міжнародний досвід переконливо доводять правдивість цього твердження.

Висновки

Підсумовуючи, можна констатувати: в умовах стрімкої цифровізації національна кібербезпека стає одним із ключових елементів

загальної системи безпеки держави. Захист критичної цифрової інфраструктури потребує постійного оновлення правових механізмів, розвитку міжвідомчої взаємодії та залучення всіх суб'єктів – як державних, так і недержавних. У цьому процесі роль поліції є фундаментальною: саме вона забезпечує правозастосовний вимір боротьби з кіберзлочинністю, проводить розслідування кіберінцидентів і виступає гарантом дотримання законності в кіберпросторі. Для ефективного виконання цих функцій необхідно забезпечити: високий кадровий потенціал, використання сучасних технологій і тісну координацію з іншими органами системи кібербезпеки. Водночас забезпечення належного рівня кіберзахисту неможливе без партнерства із приватним сектором, який володіє ресурсами, інфраструктурою та експертизою, а також без активної участі громадянського суспільства, яке сприяє формуванню культури кібергігієни, відповідальності та прозорості. Підвищення стійкості національної кібербезпеки вимагає не лише впровадження сучасних міжнародних стандартів, а й гнучкої адаптації до динамічно змінюваних загроз, зокрема складних багаторівневих атак із використанням новітніх технологій. Правоохоронна система має діяти гнучко, випереджально і скоординовано, демонструючи здатність ефективно реагувати на виклики нового цифрового середовища. У цьому контексті важливим є подальший розвиток міжвідомчих протоколів взаємодії, вдосконалення правових підходів до використання електронних доказів, розширення міжнародного співробітництва та підтримка постійного професійного розвитку персоналу поліції. Сталий розвиток кібербезпеки можливий лише за умови інтегрованого підходу, коли поліція, інші державні органи, бізнес та громадяни об'єднують зусилля для формування єдиного безпечного кіберпростору. Саме цей підхід має стати основою державної політики у сфері кібербезпеки, здатної гарантувати надійний захист національних інтересів в епоху цифрових трансформацій.

Список бібліографічних посилань: 1. Бережной С. М. Завдання Служби безпеки України як суб'єкта захисту державного суверенітету та територіальної цілісності. *Держава та регіони. Серія: Право.* 2023. № 2 (80). С. 326–330. DOI: https://doi.org/10.32782/1813-338X-2023.2.57. **2.** Гора І. В., Батюк О. В. Окремі питання захисту об'єктів критичної інфраструктури: зарубіжний досвід. *Соціально-правові студії.* 2021. Вип. 1 (11). С. 132–139. **3.** Джафарова О. В., Лещенко Д. С. Національна поліція України в системі суб'єктів забезпечення національної безпеки // Міжнародна та національна безпека: теоретичні і прикладні аспекти : матеріали VIII Міжнар. наук.-практ. конф. (м. Дніпро, 15 берез. 2024 р.) : у 2 ч. / МВС України ; Нац. поліція України ; Дніпропетровськ. держ. ун-т внутр. справ та ін. Дніпро : ДДУВС, 2024. Ч. 1.

С. 36–38. **4.** Зінченко Д. А. Стратегія боротьби з кіберзлочинністю в умовах глобалізації інформаційних просторів // Застосування інформаційних технологій у правоохоронній діяльності : матеріали круглого столу (м. Харків, 14 груд. 2023 р.) / МВС України, Харків. нац. ун-т внутр. справ. Харків, 2023. С. 105–107. **5.** Зінченко Д. А., Макарова О. П. Аналіз ризиків і стратегій захисту від кібератак у сучасному цифровому світі // Протидія кіберзлочинності та торгівлі людьми : зб. матеріалів Міжнар. наук.-практ. конф. (м. Вінниця, 31 трав. 2023 р.) / МВС України, Харків. нац. ун-т внутр. справ, Наук. парк «Наука та безпека». Вінниця, 2023. С. 118–121. **6.** Лучик С. Д., Лучик В. Є. Кібербезпека в умовах війни: соціальні аспекти. *Наука і техніка сьогодні.* 2024. № 7 (35). С. 857–870. DOI: https://doi.org/10.52058/2786-6025-2024-7(35)-857-870. **7.** Макарова О. П. Використання цифрових технологій в діяльності поліції для боротьби зі злочинністю // Правова наука і державотворення в Україні в контексті правової інтеграції : матеріали XIII Міжнар. наук.-практ. конф. (м. Суми, 21–22 трав. 2021 р.) / МВС України, Харків. нац. ун-т внутр. справ, Сумська філія. Суми : Ельдорадо, 2021. С. 174–176. **8.** Ширяєв Д. О. Кібербезпека та сучасний світ // Актуальні проблеми сучасної науки в дослідженнях молодих учених, курсантів та студентів : тези доп. Всеукр. наук.-практ. конф. (м. Вінниця, 17 трав. 2023 р.) / МВС України, Харків. нац. ун-т внутр. справ, Наук. парк «Наука та безпека». Вінниця, 2023. С. 600–602.

Надійшла до редколегії 20.05.2025

Прийнята до опублікування 13.06.2025

Vasylenko V. M. National Cybersecurity in the Context of Society Digitalization: the Role of Police in Protecting Critical Infrastructure

In the modern context of accelerated digital transformation, national cybersecurity has become a critical element of state policy aimed at protecting society, the economy, and national interests. The active integration of information and communication technologies into all spheres of public administration, economic processes, and everyday life not only generates new opportunities but also creates significant risks associated with cybercrime and the resilience of critical infrastructure. Against the backdrop of military aggression against Ukraine and large-scale cyberattacks targeting government agencies and strategic facilities, the effective operation of the national cybersecurity system is of particular relevance. This study focuses on analyzing the role of the police as a key actor within the cybersecurity system, responsible for law enforcement activities in cyberspace, prevention and investigation of cybercrime, and cooperation with other government bodies, incident response teams (CERT/CSIRT), private sector entities, and civil society organizations. The purpose of the research is to identify current approaches to shaping an effective model of police interaction in ensuring national cybersecurity and to explore legal, organizational, and practical aspects of police engagement in protecting critical infrastructure. The study reviews the current legal framework in Ukraine on cybersecurity, including the Law of Ukraine "On Basic Principles of Ensuring Cybersecurity of

Ukraine", the Law "On Critical Infrastructure", as well as European and international documents such as the NIS2 Directive and the Budapest Convention on Cybercrime. The research methodology is based on systemic, comparative-legal, analytical, and formal-legal methods. The scientific novelty lies in the comprehensive examination of the legal regulation of police activities in cybersecurity and the identification of key directions for improving interagency cooperation amid growing cyber threats. The theoretical significance of the study lies in enhancing the academic understanding of the police's role in ensuring cybersecurity and in developing legal mechanisms for their activities. The practical significance lies in formulating recommendations for improving legal regulations and enhancing collaboration between the police, CERT structures, private companies, and civil society. The research concludes that systemic approaches must be adopted to increase the effectiveness of police work in cybersecurity, aligned with European standards and international best practices, as a crucial factor in strengthening national resilience against cyber threats.

Keywords: national cybersecurity, critical infrastructure, police, cybercrime, cyber threats, CERT, cooperation, digital transformation, Budapest Convention, NIS2.