КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (31), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.31.983
УДК 343.9:351.74

Макаліш Богдан Дмитрович
курсант другого курсу навчально-наукового інституту №4
Харківський національний університет внутрішніх справ, Кам'янець-Подільський, Україна
ORCID: 0009-0002-2500-2734
bohdan.makalish@gmail.com

Мойко Олександр Олександрович
курсант третього курсу навчально-наукового інституту №4
Харківський національний університет внутрішніх справ, Кам'янець-Подільський, Україна
ORCID: 0009-0000-3828-6196
joker-moyko@ukr.net

Лучик Василь Єфремович
доктор економічних наук, професор,
професор кафедри протидії кіберзлочинності
Харківський національний університет внутрішніх справ, Кам'янець-Подільський, Україна
ORCID: 0000-0001-6007-910X
luchik.vasil@gmail.com

СУЧАСНІ ВИКЛИКИ КІБЕРЗЛОЧИННОСТІ ТА РОЛЬ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ У ЇХ ПОДОЛАННІ

Анотація. Розглянуто сучасні виклики кіберзлочинності в умовах цифровізації та воєнного стану в Україні. Окреслено основні загрози: фішинг, соціальна інженерія, атаки на критичну інфраструктуру, deepfake-технології. Проаналізовано роль Національної поліції України у протидії кіберзагрозам, зокрема діяльність кіберпідрозділів, впровадження технологій OSINT, цифрових платформ, інформаційних кампаній. Визначено основні проблеми: кадровий дефіцит, технічна застарілість, відсутність уніфікованих методик. У фіналі запропоновано шляхи удосконалення системи кібербезпеки. Розглянуто додаткові виклики, з якими доводиться зустрічатися правоохоронцям, та які сучасні методи використовують кіберзлочинці.

Ключові слова: кіберзлочинність; Національна поліція України; фішинг; OSINT; цифрова безпека; критична інфраструктура; deepfake.

ВСТУП

Розвиток цифрових технологій відкрили безмежні можливості для комунікації, ведення бізнесу та управління. Водночас вони породили нові форми кримінальної діяльності, які мають здатність завдавати шкоду на великому масштабі із застосуванням найсучасніших технологій. Кіберзлочинці сьогодні беруть участь у найширшому спектрі незаконних дій у кіберпросторі − від банальних шахрайств, крадіжок персональних даних до більш складних кібератак на критичну інфраструктуру держави. За останні роки кількість таких злочинів зросла багаторазово, а їхня організованість та технічна складність досягли рівня, що вимагає від правоохоронних органів нових підходів і ресурсів.

З 2014 року Україна перебуває в центрі найбільшого кіберконфлікту в історії. Під час анексії Криму та війни на Донбасі Росія застосовувала масивні кібератаки. У 2015 році електромережа України зазнала атаки, внаслідок чого 230 000 людей залишилися без електрики. У 2017 році вірус NotPetya завдав збитків на мільярди доларів. Під час

вторгнення 2022 року кількість кібератак різко зросла. У 2023 році в Україні зафіксували 61 400 кіберзлочинів, що вчетверо більше, ніж у 2022 році. Мета полягала в тому, щоб створити хаос, дестабілізувати країну та підірвати довіру до влади. Україна в умовах війни, особливо гостро відчула ці загрози. З 2014 року і до сьогодні кібератаки на державні структури, енергетичні компанії, банки та інформаційні ресурси відбуваються постійно, завдаючи значних збитків і підриваючи національну безпеку. Лише у 2023 році було зафіксовано понад 300 потужних кібератак, що супроводжувалися спробами викрадення даних, блокування роботи інформаційних систем і масштабної дезінформації населення [3].

Аналіз останніх досліджень і публікацій. Проблеми формування системи кібербезпеки та роль Національної поліції у її забезпеченні залишаються актуальними, особливо після воєнної агресії рф проти України. Про це свідчать наукові праці фахівців даної тематики. При цьому про залучення суспільства у протидію кіберзлочинам свідчать експериментальні проекти взаємодії з громадськістю через Telegram-боти [1-2]. Запобігання й протидія кіберзлочинам неодноразово ставали приводом для наукових досліджень вчених Мазур Я., Довгань О., Литвинова Л., Дорогих С. [3, 7]. Проблеми визначення допустимості і належності цифрових (електронних) доказів у кримінальному процесі висвітлено у працях Метелева О., Шумило М. [5]. Використання розвідданих, їх аналіз та новітніх технологій, включаючи розпізнавання облич, деталізовано і доведено до методологічних рекомендацій у роботах Пашнєва Д., Шматкова Д., Коломійцева С., Манжая О., Носова В., Лучика В., Сердюка О. [11]. Проте, незважаючи на значний обсяг публікацій і досліджень з даної теми, в сучасних умовах гострою є потреба у розробці нових та удосконаленні відомих методів боротьби Національної поліції з кіберзлочинами.

Метою статті є дослідження сучасних викликів кіберзлочинності в умовах цифровізації та воєнного стану в Україні, а також аналіз ролі Національної поліції України у їх подоланні. Задля досягнення поставленої мети визначено такі наукові завдання:

– розкрити сутність і динаміку розвитку кіберзлочинності в умовах війни;

– охарактеризувати основні форми та методи кіберзлочинної діяльності, зокрема фішинг, соціальну інженерію, deepfake-технології, атаки на критичну інфраструктуру;

– проаналізувати діяльність кіберпідрозділів Національної поліції України, використання інструментів OSINT, цифрових платформ та міжнародної співпраці у сфері протидії кіберзагрозам;

– виявити основні проблеми у сфері кібербезпеки, зокрема кадровий дефіцит, технічну застарілість обладнання, відсутність уніфікованих методик розслідування;

– визначити шляхи удосконалення системи протидії кіберзлочинності та підвищення ефективності діяльності Національної поліції України у цьому напрямі.

МЕТОДИКА ДОСЛІДЖЕННЯ

Методологічною основою дослідження є системний, логічний і комплексний підходи, що дозволяють розглядати кіберзлочинність як багатовимірне соціально-правове явище. У роботі використано методи аналізу, синтезу, логічний, порівняльно-правовий, статистичний, історико-правовий, структурно-функціональний методи.

Порівняльно-правовий метод застосовано для аналізу національного та міжнародного досвіду протидії кіберзлочинності; статистичний метод — для узагальнення динаміки зростання кіберзлочинів в Україні у 2014–2024 роках; історико-

правовий — для простеження еволюції підходів до кібербезпеки в умовах гібридної війни; метод системного аналізу — для виявлення взаємозв'язку між діяльністю Національної поліції України, державною політикою кіберзахисту та міжнародними ініціативами у сфері цифрової безпеки.

Застосування комплексного підходу дало змогу об'єднати зібраний матеріал у цілісну наукову систему, визначити тенденції розвитку кіберзлочинності та шляхи підвищення ефективності протидії їй у сучасних умовах.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Одним із найбільш поширених і небезпечних методів кіберзлочинності залишаються фішингові атаки та соціальна інженерія, коли шахраї створюють підроблені сайти або розсилають листи, які імітують офіційні ресурси, аби отримати доступ до конфіденційної інформації або змусити користувачів передати свої персональні дані. В сучасних умовах ці методи набули нового рівня складності завдяки автоматизації і використанню штучного інтелекту, що дозволяє створювати персоналізовані та більш переконливі фішингові кампанії.

Поширеним явищем також стали організовані злочинні групи, які через створені call-центри за допомогою VOIP-телефонії і підроблених банківських ідентичностей здійснюють масштабні шахрайські операції. Прикладом є випадок у Києві у 2024 році, коли кіберполіція припинила діяльність злочинної групи, що ошукала понад 300 громадян на суму понад 20 мільйонів гривень [2, 4].

Особливо загрозливою для держави стала нова тенденція кібератак на критичну інфраструктуру України, що перебуває під постійним тиском в умовах війни. Ці атаки можуть призводити до тимчасового або тривалого припинення роботи енергетичних мереж, телекомунікацій, транспортних систем, а також підривати роботу державних служб і ресурсів, що негативно впливає на життя мільйонів громадян. Часто такі дії поєднуються з фізичними ударами, утворюючи комплексний фронт гібридної війни, де кіберпростір стає ареною стратегічного протистояння. Такі випадки неодноразово фіксувалися у 2023–2024 роках, коли зловмисники застосовували складні методи проникнення у захищені мережі та використовували сучасні інструменти для маскування своїх дій [3, 5].

Ці виклики формують складну, багатовимірну систему загроз, що потребує комплексної відповіді від державних інституцій, суспільства та бізнесу. Безпечний розвиток цифрової економіки і збереження національної безпеки залежить від здатності ефективно протидіяти кіберзлочинності, а також необхідності запроваджувати інноваційні технології захисту, підвищувати рівень цифрової грамотності населення і створювати умови для міжвідомчої та міжнародної співпраці.

Відповідь на виклики кіберзлочинності в Україні тісно пов'язана з діяльністю Національної поліції, а зокрема Департаменту кіберполіції, який відіграє ключову роль у забезпеченні безпеки у цифровому середовищі. Кіберполіція здійснює постійний моніторинг кіберзагроз, збирає інформацію про новітні методи злочинців, проводить розслідування щодо несанкціонованого втручання в інформаційні системи, незаконного збору і розповсюдження персональних даних, атак на державні сервіси, такі як портал «Дія». Важливим аспектом роботи є використання передових методик, зокрема OSINT (відкриті джерела інформації), що дозволяє виявляти загрози ще на початкових етапах, а також тісна міжнародна співпраця з INTERPOL, Europol та іншими правоохоронними органами [2].

З метою протидії ворожій кіберактивності основними суб'єктами забезпечення кібербезпеки держави за провідної ролі Адміністрації Держспецзв'язку здійснювалася взаємодія щодо кіберзахисту з державними органами та представниками критичної інфраструктури, розроблялися необхідні інструкції для користувачів із попередження та розпізнавання кібератак, а також захисту та усунення наслідків.

Також Україна продовжує поглиблювати співпрацю з партнерами у сфері кіберзахисту. Адже досвід України в боротьбі з кібератаками російського агресора допомагає не тільки нам, а й нашим партнерам у побудові дієвих національних та міжнародних систем кіберзахисту. Про зазначене свідчить інтерес міжнародної спільноти до інформації від українських фахівців на міжнародних заходах із кібербезпеки. Прикладами є недавня міжнародна конференція команд реагування на комп'ютерні надзвичайні події FIRST і міжнародна конференція з кібербезпеки Black Hat-2022. Україна постійно ділиться з партнерами даними про кіберзброю, яку застосовують російські хакери. З цього напряму в липні поточного року було підписано «Меморандум про взаєморозуміння між Держспецзв'язку та Урядовим офісом Республіки Словенія з інформаційної безпеки у сфері кіберзахисту» та відповідний документ щодо співпраці з Агентством з кібербезпеки та безпеки інфраструктури Департаменту національної безпеки Сполучених Штатів Америки (Cybersecurity and Infrastructure Security Agency). Аналогічно в серпні Україна уклала «Меморандум про взаєморозуміння у сфері кіберзахисту» з Республікою Польща.

Сучасний кіберпростір створює унікальне середовище, де криміналістичні сліди можуть бути передані на великі відстані, зберігаючись в цифровому вигляді необмежено довго. Ці особливості змусили криміналістику враховувати специфіку кіберпростору. В 2005 році українське законодавство ратифікувало Конвенцію про кіберзлочинність, згідно з якою кіберзлочини розділяються на чотири види.

Правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем – це перший вид кіберзлочинів. До цього типу правопорушень відносять: незаконний доступ, нелегальне перехоплення, втручання у дані, втручання в систему та зловживання пристроями [6, статті 2-6]

Правопорушення, пов'язані з шахрайством у сфері використання комп'ютерних систем. Такі дії мають на меті завдання матеріальних збитків через маніпуляції з комп'ютерними даними для незаконного отримання економічної вигоди. [6, статті 7-8]

Правопорушення, пов'язані зі змістом (контентом), що полягає у здійсненні умисних незаконних дій щодо вироблення, пропонування або надання доступу, розповсюдження дитячої порнографії, а також володіння такими файлами у своїй системі. [6, стаття 9]

Умисні дії, пов'язані з порушенням авторських та суміжних прав, відповідно до вимог Паризького акту від 42 липня 1971р, Бернської Конвенції про захист літературних і художніх творів, Угоди про торговельні аспекти прав інтелектуальної власності та Угоди ВОІВ про авторське право, а також національного законодавства України, полягають у незаконному відтворенні, розповсюдженні, публічному показі, наданні доступу до об'єктів авторського права через комп'ютерні мережі або в інший спосіб без згоди правовласника з метою отримання прибутку чи заподіяння шкоди власнику прав.. [6, стаття 10]

Існують також інші класифікації кіберзлочинів, проте запропонована конвенцією є найбільш популярною. В Україні кібербезпека координується низкою державних органів, а саме на Державну службу спеціального зв'язку та захисту інформації України, Національну поліцію України, Службу безпеки України, Міністерство оборони України

та Генеральний штаб Збройних Сил України, розвідувальні органи. В кожному із зазначених органів діють відповідні підрозділи. Проте, захист власної кібербезпеки є відповідальністю кожного користувача.

Найбільш розповсюджені кіберзлочини в Україні за 2023-2024 роки наведено на рис.1.

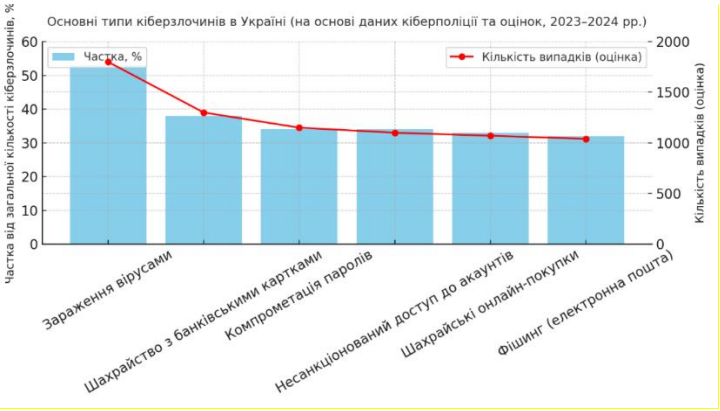

Рис. 1. Найбільш розповсюджені кіберзлочини в Україні за 2023-2024 роки
Джерело: [7, с. 64]

Окрему увагу кіберполіція приділяє протидії організованому кіберзлочинному бізнесу, що використовує технології VoIP для масового обману громадян через шахрайські call-центри. Припинення діяльності такої злочинної групи у Києві в 2024 році є яскравим прикладом ефективності правоохоронних органів, але водночас підкреслює масштаби та глибину проблеми. Для покращення ефективності роботи НПУ активно впроваджуються цифрові платформи, зокрема «Моя кібербезпека», що спрямовані на підвищення обізнаності населення про шахрайські схеми в месенджерах, банківське шахрайство та кібервіруси.

Експериментальні проекти взаємодії з громадськістю через Telegram-боти для сповіщення про підозрілі ресурси демонструють новий рівень залучення суспільства у протидію кіберзлочинам [1, 2].

Проте, незважаючи на активні заходи, діяльність кіберполіції ускладнюють значні проблеми. По-перше, існує критична нестача кваліфікованих фахівців у сфері кібербезпеки (рис. 2).

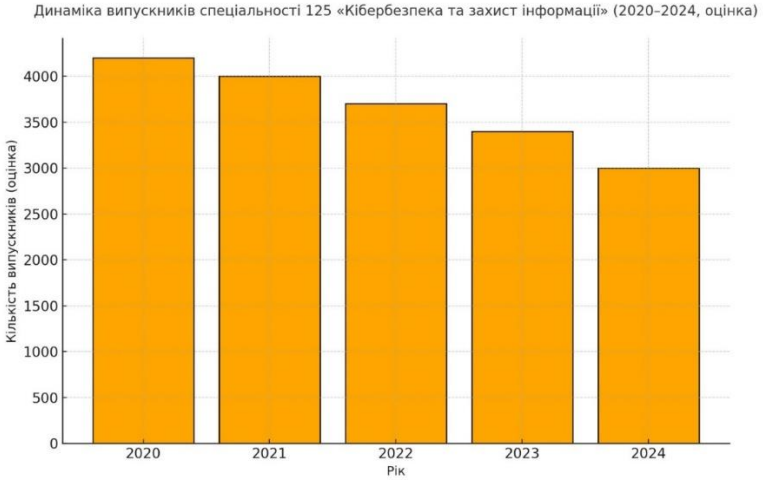

Рис.2. Динаміка випуску фахівців з кібербезпеки за 2020 – 2024 рр.
Джерело: [11-13]

Високотехнологічний характер кіберзлочинності вимагає постійного професійного розвитку, але кадровий дефіцит і відтік IT-спеціалістів суттєво знижують оперативність і якість розслідувань. По-друге, технічне забезпечення залишається застарілим і не відповідає рівню сучасних кіберзагроз, що ускладнює фіксацію та аналіз цифрових доказів. Ці фактори разом призводять до того, що значна частина кримінальних проваджень за статтями 361–363 Кримінального кодексу України не доходить до обвинувальних вироків через труднощі із збиранням, збереженням та адекватною оцінкою цифрових доказів [3, 4].

Ще одним викликом є необхідність вдосконалення законодавчої бази та уніфікації стандартів проведення кіберрозслідувань. Відсутність чітких і єдиних норм збирання доказів у цифровому середовищі створює прогалини у кримінальному процесі і знижує ефективність судового розгляду. Для подолання цих проблем Національна поліція, співпрацюючи з науковими установами, активно працює над розробкою нових методичних рекомендацій і стандартів доказової бази, що враховують особливості кіберзлочинів [4].

Важливою складовою системи протидії кіберзлочинності є цифрова освіта населення. Підвищення рівня обізнаності громадян у сфері кібербезпеки дозволяє значно знизити ризики потрапляння у пастки шахраїв. Національна поліція у 2023 році реалізувала масштабні інформаційні кампанії, спрямовані на інформування населення про типові схеми кіберзлочинців, правила безпечної поведінки в інтернеті та використання сучасних захисних технологій. Особливо важливою стала робота з вразливими категоріями населення, які найчастіше стають жертвами кіберзлочинів [2].

У межах програми “Кібергігієна” за підтримки ОБСЄ викладачі кафедри протидії кіберзлочинності Харківського національного університету внутрішніх справ **беруть** активну участь у підготовці тренерів із цифрової безпеки. Проєкт був спрямований на підвищення рівня обізнаності у сфері кібергігієни серед курсантів і студентів закладів вищої освіти системи МВС. У рамках ініціативи під егідою ОБСЄ було підготовлено близько 50 тренерів із різних університетів, розроблено навчально-методичні матеріали, а також створено спеціалізовані навчальні класи для проведення занять із кібергігієни. Зокрема, викладачі ХНУВС долучилися до розроблення практичних занять, інтерактивних кейсів та настільної гри *CyberAlias*, що використовується у навчальному процесі для розвитку навичок безпечної поведінки в мережі.

Таким чином, протидія кіберзлочинності в Україні має бути неперервно комплексною і включати правоохоронні заходи, технічні засоби, міжнародне співробітництво та просвіту суспільства. Від успіху боротьби з кіберзлочинністю залежить можливість Національної поліції згодом адаптуватися до швидких змін технологій, залучати спеціалістів у галузі інформаційних технологій, створювати гнучкі міжвідомчі механізми, а також розвивати проактивні підходи до цифрової безпеки.

Незважаючи на значні успіхи Національної поліції України у сфері протидії кіберзлочинності, діяльність її кіберпідрозділів супроводжується низкою системних проблем, які істотно обмежують ефективність боротьби з новітніми викликами. Однією з ключових складностей є нестача кваліфікованих кадрів. Високотехнологічний характер кіберзлочинів вимагає фахівців із глибокими знаннями в галузі інформаційної безпеки, програмування, криптографії, а також сучасних методів цифрової криміналістики. В умовах високого попиту на IT-спеціалістів у приватному секторі, Національна поліція стикається із проблемою утримання кваліфікованих працівників, що призводить до дефіциту персоналу у ключових підрозділах [3, 4].

Проблема кібербезпеки особливо актуальна в умовах війни, коли ворожі хакерські групи здійснюють кібератаки не лише на державні установи, а й на звичайних користувачів. У такій ситуації важливо мати актуальні знання та інструменти для захисту себе та своїх близьких у цифровому просторі.

З метою забезпечення надійного функціонування кіберпростору в Україні розроблено й запроваджено комплекс законодавчих актів, спрямованих на регулювання питань інформаційної безпеки. Ці нормативно-правові документи визначають як права, так і обов'язки громадян у відповідній сфері, створюючи правову основу для захисту інформаційних систем, персональних даних та інших критично важливих ресурсів. Крім того, законодавство передбачає відповідальність за порушення вимог інформаційної безпеки.

Закон України «Про Національну поліцію» 2015 року надав правоохоронним органам розширені повноваження для створення та використання інформаційних баз даних. Проте, з огляду на численні переваги цих технологій, слід визнати, що при несанкціонованому їх використанні (без дотримання вимог закону), це може призвести до серйозних наслідків.

Доступ до персональних даних без належних повноважень, законної підстави чи обґрунтованої мети – поширеною є практика, коли працівники підрозділів протидії наркозлочинності масово витребовують з медичних закладів інформацію про осіб, які стоять на обліку. Суспільство досі не отримало чіткої відповіді щодо правових підстав для збору інформації про здоров'я людини, яка не вчинила правопорушень.

Обробка відеозаписів із нагрудних камер поліцейських та систем відеоспостереження – збір, доступ, формування баз та порядок зберігання такої інформації залишаються неврегульованими. Часто відеозаписи з камер з'являються в Інтернеті без дотримання законодавства про захист персональних даних.

Відсутність належної політики безпеки персональних даних – багато розпорядників даних не розробляють та не приймають внутрішніх нормативно-правових актів, що регулюють захист зібраних персональних даних.

Недостатньо прозоре управління у сфері захисту даних – міжнародні стандарти передбачають, що суспільство має право знати, які саме дані збираються, умови їх зберігання та порядок знищення. У більшості випадків інформація, що збирається і використовується поліцією, не архівується у форматах, які забезпечують належний рівень безпеки та конфіденційності, і не ведеться належний облік.

Ситуація із захистом даних вимагає вдосконалення політики безпеки та розвитку законодавчих механізмів для прозорого управління персональними даними.

Отже, сучасний світ змінюється. Щороку зловмисники вигадують нові, раніше невідомі способи та стратегії для скоєння злочинів у сфері інформаційних технологій. Оскільки це відносно нова галузь, часто виникають ситуації, коли нові поняття, дії в інтернеті тощо ще не мають законодавчого підґрунтя. Міжнародні конвенції намагаються максимально швидко реагувати на ці виклики, щоб усі країни, що ратифікували такі конвенції, мали основу для створення власних законів у цій новій сфері. Незважаючи на постійні виклики та кібератаки з боку ворога, Україна активно розробляє законодавчі акти (закони, конвенції тощо) для регулювання ІТ-сфери, особливо в умовах правового режиму воєнного стану. Важливо відзначити, що реагування часто відбувається майже миттєво, завдяки чому законодавець ускладнює можливість повторного скоєння злочину тим самим способом.

Для моніторингу кіберінцидентів створено платформу Splunk Enterprise Security (ES), яка забезпечує централізований збір, аналіз та кореляцію подій у реальному часі.

Вона використовує штучний інтелект та машинне навчання для виявлення загроз, автоматизації реагування та управління ризиками. Splunk ES інтегрується з різними джерелами даних, такими як мережевий трафік, журнали подій та поведінковий аналіз, що дозволяє швидко ідентифікувати аномалії, пов'язані з кібератаками, та передавати їх до відповідних команд реагування.

Ще однією серйозною перешкодою є технічне забезпечення. На сьогодні обладнання та програмне забезпечення, що використовується в Департаменті кіберполіції, часто застарілі або не відповідають новітнім стандартам кібербезпеки. Це ускладнює оперативне виявлення та фіксацію цифрових доказів, а також знижує швидкість реагування на складні кібератаки, які постійно еволюціонують і набирають нових форм. Відсутність сучасних аналітичних інструментів та систем автоматичного виявлення кіберзагроз обмежує можливості для своєчасного блокування атак. [3]

Крім цього, одним із суттєвих викликів є нестача уніфікованих стандартів і методик збору, збереження та аналізу цифрових доказів, що призводить до проблем із доказовою базою у кримінальних провадженнях. Складність кіберзлочинів і специфіка інформаційних технологій вимагають детального і послідовного підходу до процесуальних дій. На практиці, недосконаліть законодавства та відсутність єдиних протоколів ускладнюють роботу слідчих, через що багато проваджень за статтями 361–363 ККУ не доходять до обвинувальних вироків. Це підриває довіру до системи правосуддя і стимулює злочинців до нових атак [4].

Також окремо необхідно виділити використання ІТ технологій наркозлочинцями. Сучасні технології дозволяють незаконно придбати наркотики дистанційно. Реклама «наркомагазинів» поширюється на стінах будівель, зупинках, через інтернет-сайти та месенджери (Telegram). У месенджерах створюються канали для продажу наркотиків, де публікуються інформація про товар, ціни, а також ведуться чати для спілкування покупців і працівників. При цьому клієнт та продавець не знають один одного та не зустрічаються щоб передати товар та отримати за нього гроші. Продавець може знаходитися в одній країні чи регіоні, а збут відбуватися в іншому.

Окрім того, що в сучасних умовах збут наркотиків відбувається без фізичного контакту між продавцем та покупцем, наркозловмисники та їх «клієнти» теж використовують різні сучасні методи приховування їх причетності до незаконного збуту наркотичних засобів, психотропних речовин або їх аналогів через мережу Інтернет.

З впровадженням штучного інтелекту у різні сфери життя зростають і виклики для кібербезпеки. У фахівців з кібербезпеки виникає дедалі більше занепокоєнь, щодо можливості використання хакерскими угрупуваннями потенціалу штучного інтелекту для проведення кібератак. Хоча країни поступово розробляють закони, нещодавні ініціативи, такі як Закон Європейського Союзу про штучний інтелект, свідчать про зростаюче визнання необхідності регуляторного нагляду. Темпи технологічного розвитку випереджають регуляторні заходи, змушуючи організації самостійно боротися з ризиками ШІ.

Нещодавні атаки на фінансові установи та великі компанії показують, що хакери застосовують генеративні моделі для масового створення шкідливих скриптів, автоматизованого введення команд у системи та навіть для підробки голосових або відеоповідомлень керівників з метою шахрайських транзакцій.

Для правоохоронних органів це створює подвійний виклик: з одного боку, необхідно впроваджувати власні ШІ-системи для прогнозування загроз і протидії кіберзлочинності; з іншого – відсутність чітких норм щодо збору, обробки та зберігання даних може призвести до порушення прав громадян. Наприклад, автоматизований аналіз

трафіку інтернет-користувачів або відеоспостереження без належних правових підстав може стати джерелом витоків або зловживань.

Варто зазначити, що проблема координації міжвідомчої взаємодії також залишається актуальною. Ефективна протидія кіберзагрозам вимагає тісної співпраці між правоохоронними органами, органами державної влади, приватним сектором і міжнародними партнерами. Невідповідність процедур обміну інформацією і затримки у реагуванні на кіберінциденти призводять до втрати часу, що може мати критичні наслідки в умовах загострення кіберзагроз [2, 3].

Нарешті, викликом залишається недостатня поінформованість широкого загалу населення про основи кібербезпеки. Без належної цифрової освіти громадяни залишаються вразливими до численних шахрайських схем і атак, що активізуються у періоди соціальної напруги чи воєнних конфліктів. Зусилля Національної поліції з інформування населення є важливими, проте вони потребують систематичного розширення та підтримки на державному рівні [2].

Штучний інтелект став ще одним важливим елементом кібербезпеки, забезпечуючи виявлення загроз у режимі реального часу. Його алгоритми аналізують поведінку користувачів і пристроїв, визначають аномалії у мережевому трафіку та ідентифікують шкідливе програмне забезпечення. Найбільш цінною є здатність ШІ до автоматичного реагування – блокування загроз без втручання людини, що значно скорочує час реагування. Машинне навчання дозволяє системам постійно вдосконалюватися, адаптуючись до нових сценаріїв атак. Це особливо важливо для критичної інфраструктури, де кожна секунда затримки у виявленні загрози може мати серйозні наслідки.

Додатковим компонентом кіберзахисту є навчання НАТО Locked Shields – найбільше у світі моделювання кібератак, що проводиться в Естонії. Під час цих навчань міжнародні команди відпрацьовують захист критичної інфраструктури від масованих атак, симулюючи сценарії, подібні до реальних загроз. Учасники повинні швидко ідентифікувати та нейтралізувати атаки на енергосистеми, фінансові установи та телекомунікації. Locked Shields також покращує координацію між союзниками, дозволяючи обмінюватися найкращими практиками у сфері кібербезпеки.

Міжнародні ініціативи з протидії кібератакам включають програму CyberEast – Програма, що реалізується Радою Європи, сприяє поліпшенню кіберстійкості та реагування органів кримінального правосуддя в країнах Східного Партнерства та зосереджена на двох ключових складових. Перша – це розробка технічних механізмів та механізмів співпраці, що підвищують кібербезпеку та готовність до кібератак, а друга – повне впровадження ефективної системи боротьби з кіберзлочинністю. [5].

Усі ці проблеми свідчать про необхідність комплексного реформування підходів до кібербезпеки в Україні, що має включати модернізацію технічної бази, підвищення кваліфікації кадрів, удосконалення законодавства, а також активне залучення громадськості до формування культури цифрової безпеки. Тільки так можна створити ефективну систему протидії кіберзлочинності, яка відповідатиме сучасним загрозам і сприятиме зміцненню національної безпеки [3, 4].

Сучасна кіберзлочинність є надзвичайно динамічним і багатогранним явищем, що суттєво загострюється під впливом як технологічного прогресу, так і геополітичних викликів, зокрема війни в Україні. Злочинці все частіше використовують складні методи, зокрема фішинг, соціальну інженерію, шкідливе програмне забезпечення і штучний інтелект, для досягнення своїх цілей, що негативно впливає на безпеку держави, економіку та психологічний стан суспільства. Особливу небезпеку становлять

кібератаки на критичну інфраструктуру, які підривають фундаментальні сфери життєдіяльності країни, а також застосування технологій deepfake для інформаційної війни [1, 3, 4].

Для протидії цим загрозам Національна поліція України, зокрема Департамент кіберполіції, активно застосовує сучасні технології моніторингу, розслідування та міжнародної співпраці. Успішні операції з припинення діяльності організованих злочинних груп, використання методів OSINT, впровадження інформаційних кампаній та взаємодія з громадськістю через цифрові платформи є прикладами ефективного реагування. Проте існують суттєві виклики, пов'язані з дефіцитом кваліфікованих фахівців, застарілим технічним забезпеченням та недосконалістю законодавчої бази, що ускладнює фіксацію та судове розглядання кіберзлочинів [2-4].

Департаментом кіберполіції зареєстровано 2,5 тис. кіберзлочинів, повідомлено про підозру 1,7 тис. особам у вчиненні 3,5 тис. кримінальних правопорушень, закінчено досудове розслідування по 4,4 тис. кримінальним правопорушенням, а скеровано до суду з обвинувальним актом понад 4 тис. справ. Потерпілим забезпечено відшкодування понад 168,6 млн грн, що становить 42,5% від завданих кримінальними правопорушеннями збитків [9].

Слід зауважити, що за час дії воєнного стану зловмисники підлаштовувалися під тренди суспільства, тому набули поширення заволодіння коштами громадян під виглядом надання послуг з оформлення документів для чоловіків призовного віку, незаконного перетину кордону, шахрайства, пов'язані із торгівлею військового спорядження та наданням волонтерської допомоги, оренди квартир для внутрішньо переміщених осіб, їх перевезень в безпечні регіони.

Загалом, у зазначеній сфері, поліцейські оголосили про підозру більше ніж 700 особам, 620 правоохоронці вручили обвинувальні акти у вчиненні кримінальних правопорушень. Окрема увага підрозділів ДКП спрямовувалися на протидію найбільш поширеним різновидам шахрайств – дзвінкам від імені працівників банківських установ та фішингу. Завдяки послідовній співпраці з фахівцями Національного банку України та Держспецзв'язку, у 2024 році обмежено доступ до доменних імен, які зловмисники масово використовували у протиправній діяльності, у тому числі для створення фішингових посилань.

Спільно з іноземними колегами українські поліцейські ініціювали та забезпечили участь у проведенні 17 міжнародних поліцейських операцій. У результаті було нейтралізовано загрозу з боку кількох потужних хакерських об'єднань, злочинна діяльність яких охоплювала країни усього світу.

Основні кількісні показники діяльності підрозділів кіберполіції України, а також дані щодо шахрайства, спрямованого на державні ресурси в умовах воєнного стану наведено у табл. 1-2.

Таблиця 1

Основні кількісні показники діяльності підрозділів кіберполіції України за 2023–2024 роки

Показник	Кількість
Зареєстровано кіберзлочинів	2 500
Повідомлено про підозру особам	1 700
Кримінальних правопорушень (за підозрами)	3 500
Закінчено досудове розслідування	4 400

Скеровано до суду з обвинувальним актом (не менше)	4 000
Відшкодовано потерпілим (млн грн)	168.6
Частка від загальної шкоди (%)	42.5
Орієнтовна загальна шкода (млн грн, розрахунок)	396.7

Таблиця 2

Шахрайства, пов'язані з воєнним станом

Показник	Кількість
Оголошено про підозру (воєнний стан, шахрайства)	700
Вручені обвинувальні акти (воєнний стан, шахрайства)	620

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У сучасних умовах кіберзлочинність стала одним із найнебезпечніших викликів національній безпеці України. Злочинці дедалі активніше використовують фішинг, соціальну інженерію, шкідливе ПЗ, VoIP, deepfake-технології та штучний інтелект, що посилює масштаби атак та їхній вплив. Особливо небезпечними є кібератаки на критичну інфраструктуру, які у поєднанні з інформаційними впливами формують гібридну загрозу в умовах війни.

Національна поліція України, зокрема Департамент кіберполіції, відіграє ключову роль у системі кіберзахисту. Використання методів OSINT, міжнародна співпраця, цифрові платформи для взаємодії з населенням і інформаційні кампанії – все це сприяє підвищенню ефективності боротьби з кіберзлочинністю. Проте наявні проблеми – дефіцит кадрів, застаріла техніка, недосконале законодавство та слабка цифрова обізнаність населення – стримують подальший прогрес [10].

Для ефективної протидії кіберзлочинності необхідно впровадити комплексний підхід: модернізувати технічну базу кіберпідрозділів, вдосконалити нормативно-правову базу, уніфікувати методики розслідувань, покращити підготовку кадрів та розвивати цифрову просвіту населення. Важливими залишаються міжнародна співпраця та міжвідомча координація. Розвиток технологій, цифровізація суспільства та залежність від кіберінфраструктури створили нові виклики для безпеки країн. Кібератаки стали потужним інструментом тиску, саботажу та дестабілізації, дозволяючи впливати на цілі країни без перетину фізичних кордонів. У світі, де цифрова залежність зростає, кібербезпека має стати пріоритетом для кожної країни. Посилення інфраструктури, міжнародна співпраця в сфері кіберзахисту та цифрова освіта громадян допоможуть запобігти майбутнім катастрофам.

Головним викликом для будь-якої країни є не лише реагування на атаки, а й створення стійких систем кіберзахисту. Україна, зіткнувшись з постійними кіберпротистояннями, продемонструвала важливість міжнародної підтримки в цій боротьбі. Лише за умови скоординованих зусиль держави, правоохоронних органів, суспільства та бізнесу можна створити ефективну систему кібербезпеки, здатну протистояти сучасним цифровим загрозам і забезпечити національну стійкість у цифровому середовищі.

Подальші дослідження мають бути спрямовані на розроблення інтегрованої системи протидії кіберзагрозам, яка поєднає правові, організаційні та технічні

інструменти. Першочерговим завданням є вдосконалення нормативно-правової бази у сфері кібербезпеки та розроблення єдиних стандартів реагування на кіберінциденти, що дозволить забезпечити узгодженість дій між державними органами, правоохоронцями та приватним сектором.

Перспективним напрямом є впровадження інтелектуальних технологій аналізу даних, штучного інтелекту та OSINT-методів для раннього виявлення кіберзагроз. Це дозволить перейти від реагування до превентивних заходів, зокрема прогнозування атак на критичну інфраструктуру. Водночас потребує уваги підготовка висококваліфікованих кадрів та створення системи безперервної кіберосвіти для фахівців Національної поліції.

Майбутні наукові розвідки повинні бути спрямовані на посилення міжнародного співробітництва у сфері кіберзахисту, розроблення спільних стандартів обміну цифровими доказами та удосконалення механізмів координації між правоохоронними структурами різних країн. Комплексна реалізація цих напрямів сприятиме підвищенню стійкості України до сучасних кіберзагроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cyber Police Department of the National Police of Ukraine. (2024). *Public report for 2023* (42 p.). Ministry of Internal Affairs of Ukraine.
2. OSCE Project Co-ordinator in Ukraine (closed). (2025). *Organization for Security and Co-operation in Europe | OSCE*. https://www.osce.org/project-coordinator-in-ukraine-closed (accessed 03.07.2025)
3. Mazur, Ya. P. (2024). Main cyber threats in the context of information warfare. *Analytical and Comparative Jurisprudence (Electronic Scientific Edition)*, 599–604.
4. Metelev, O. P., & Shumylo, M. Ye. (2019). Problems of determining the admissibility and relevance of digital (electronic) evidence in criminal proceedings. *Journal of Criminal Justice, 3*, 224–238.
5. Ministry of Internal Affairs of Ukraine. (2023). *Cybersecurity strategy of Ukraine until 2025*. Kyiv.
6. Convention on Cybercrime. (2001, November 23). https://zakon.rada.gov.ua/laws/show/994_575
7. Dovhan, O. (Ed.). (2024). *Cybersecurity in the information society: Information and analytical digest* (No. S, 316 p.). State Scientific Institution "Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine"; Vernadsky National Library of Ukraine.
8. Cyber Police of Ukraine. (2025). *Report on the activities of the Cyber Police Department of the National Police of Ukraine in 2024*. https://cyberpolice.gov.ua/news/zvitpro-diyalnist-departamentu-kiberpolicziyi-naczionalnoyi-policziyi-ukrayiny-u--roczi-7074/b (accessed 07.05.2025)
9. ArmyInform. (2022, September 10). *How to ensure the protection of Ukraine's cyberspace amid Russia's armed aggression.* https://armyinform.com.ua/2022/09/10/yak-zabezpechyty-zahyst-kiberprostoru-ukrayiny-na-tli-zbrojnoyi-agresiyi-rf/ (accessed 07.05.2025)
10. Pashniev, D. V., Shmatkov, D. I., Kolomiitsev, S. O., Manzhai, O. V., Nosov, V. V., Luchyk, V. Ye., & Serdiuk, O. O. (2024). *AI and OSINT tools and methods for tracing missing, deported or forcibly displaced children: Guidelines for the use of open source intelligence and new technologies, including facial recognition* (80 p.). Ministry of Internal Affairs of Ukraine; Kharkiv National University of Internal Affairs; Educational and Scientific Institute No. 4.
11. Department of Computer Science and Cybersecurity, Lesya Ukrainka Volyn National University. (2025). *Graduates – Faculty of Information Technology and Mathematics.* https://cs.vnu.edu.ua/?page_id=35 (accessed 09.10.2025)
12. National Agency for Higher Education Quality Assurance. (2023). *Доповідь про якість вищої освіти в Україні.* https://naqa.gov.ua/wp-content/uploads/2023/04/Доповідь-про-якість-вищої-освіти-в-Україні.pdf (accessed 09.10.2025)
13. Nikolaev, Ye., Rii, H., & Shemelynets, I. (2023). *Higher education in Ukraine: Changes caused by the war: Analytical report* (94 p.). Borys Grinchenko Kyiv University.

.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (31), 2025
ISSN 2663 - 4023

Makalish Bohdan
cadet of the second year of educational and scientific institute № 4
Kharkiv National University of Internal Affairs, Kamianets-Podilskyi, Ukraine
ORCID: 0009-0002-2500-2734
bohdan.makalish@gmail.com

Moiko Oleksandr
cadet of the third year of educational and scientific institute № 4
Kharkiv National University of Internal Affairs, Kamianets-Podilskyi, Ukraine
ORCID: 0009-0000-3828-6196
joker-moyko@ukr.net

Luchyk Vasil
Doctor of Economics, Professor, Professor of the Department of Cybercrime Counteraction
Kharkiv National University of Internal Affairs, Kamianets-Podilskyi, Ukraine
ORCID: 0000-0001-6007-910X
luchik.vasil@gmail.com

MODERN CHALLENGES OF CYBERCRIME AND THE ROLE OF THE NATIONAL POLICE OF UKRAINE IN OVERCOMING THEM

Abstract. The article examines the modern challenges of cybercrime in the conditions of digitalization and martial law in Ukraine. The main threats are identified, such as phishing, social engineering, attacks on critical infrastructure, and deepfake technologies. The role of the National Police of Ukraine in countering cyber threats is analyzed, including the work of cyber units, the use of OSINT technologies, digital platforms, and information campaigns. The main problems are defined: staff shortage, outdated technical equipment, and the lack of unified methods. Finally, ways to improve the cybersecurity system are proposed. Additional challenges faced by law enforcement officers are considered, as well as the modern methods used by cybercriminals.

Keywords: cybercrime; National Police of Ukraine; phishing; OSINT; digital security; critical infrastructure; deepfake.

REFERENCES

1. Cyber Police Department of the National Police of Ukraine. (2024). *Public report for 2023* (42 p.). Ministry of Internal Affairs of Ukraine.
2. OSCE Project Co-ordinator in Ukraine (closed). (2025). *Organization for Security and Co-operation in Europe | OSCE*. https://www.osce.org/project-coordinator-in-ukraine-closed (accessed 03.07.2025)
3. Mazur, Ya. P. (2024). Main cyber threats in the context of information warfare. *Analytical and Comparative Jurisprudence (Electronic Scientific Edition)*, 599–604.
4. Metelev, O. P., & Shumylo, M. Ye. (2019). Problems of determining the admissibility and relevance of digital (electronic) evidence in criminal proceedings. *Journal of Criminal Justice, 3*, 224–238.
5. Ministry of Internal Affairs of Ukraine. (2023). *Cybersecurity strategy of Ukraine until 2025.* Kyiv.
6. Convention on Cybercrime. (2001, November 23). https://zakon.rada.gov.ua/laws/show/994_575
7. Dovhan, O. (Ed.). (2024). *Cybersecurity in the information society: Information and analytical digest* (No. S, 316 p.). State Scientific Institution "Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine"; Vernadsky National Library of Ukraine.
8. Cyber Police of Ukraine. (2025). *Report on the activities of the Cyber Police Department of the National Police of Ukraine in 2024.* https://cyberpolice.gov.ua/news/zvitpro-diyalnist-departamentu-kiberpolicziyi-naczionalnoyi-policziyi-ukrayiny-u--roczi-7074/b (accessed 07.05.2025)
9. ArmyInform. (2022, September 10). *How to ensure the protection of Ukraine's cyberspace amid Russia's armed aggression.* https://armyinform.com.ua/2022/09/10/yak-zabezpechyty-zahyst-kiberprostoru-ukrayiny-na-tli-zbrojnoyi-agresiyi-rf/ (accessed 07.05.2025)

10. Pashniev, D. V., Shmatkov, D. I., Kolomiitsev, S. O., Manzhai, O. V., Nosov, V. V., Luchyk, V. Ye., & Serdiuk, O. O. (2024). *AI and OSINT tools and methods for tracing missing, deported or forcibly displaced children: Guidelines for the use of open source intelligence and new technologies, including facial recognition* (80 p.). Ministry of Internal Affairs of Ukraine; Kharkiv National University of Internal Affairs; Educational and Scientific Institute No. 4.
11. Department of Computer Science and Cybersecurity, Lesya Ukrainka Volyn National University. (2025). *Graduates – Faculty of Information Technology and Mathematics.* https://cs.vnu.edu.ua/?page_id=35 (accessed 09.10.2025)
12. National Agency for Higher Education Quality Assurance. (2023). *Доповідь про якість вищої освіти в Україні.* https://naqa.gov.ua/wp-content/uploads/2023/04/Доповідь-про-якість-вищої-освіти-в-Україні.pdf (accessed 09.10.2025)
13. Nikolaev, Ye., Rii, H., & Shemelynets, I. (2023). *Higher education in Ukraine: Changes caused by the war: Analytical report* (94 p.). Borys Grinchenko Kyiv University.