УДК 343.1
DOI https://doi.org/10.32782/2311-8040/2024-3-9

Ларченко Марина Олександрівна,
кандидат юридичних наук, доцент,
доцент кафедри політології, права та філософії
Ніжинський державний університет імені Миколи Гоголя,
вулиця Графська, 2, Ніжин, Чернігівська область, 16600, Україна;
доцент кафедри кібербезпеки та математичного моделювання,
Національний університет «Чернігівська політехніка»,
вулиця Шевченка, 95, Чернігів, 14027, Україна
ORCID: https://orcid.org/0000-0002-2643-980X

ДЕЯКІ ОСОБЛИВОСТІ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

Анотація. *У сучасному світі, де інформаційні технології інтегровані у всі сфери життя, кіберзлочини стають усе більш поширеними та складними. Вони включають крадіжку особистих даних, фінансові махінації, зломи інформаційних систем, розповсюдження шкідливого програмного забезпечення та інші форми злочинної діяльності в кіберпросторі. Метою статті є висвітлення основних аспектів та викликів, пов'язаних із розслідуванням кіберзлочинів.*

У статті проведено аналіз останніх наукових публікацій українських та зарубіжних авторів, що досліджують різні аспекти кіберзлочинності, включаючи правові, технічні та організаційні аспекти. Класифіковано кіберзлочини за кількома основними категоріями, такими як крадіжка даних, фінансові махінації, хакерські атаки, поширення шкідливого програмного забезпечення та кібертероризм. Умовно, кримінальне правопорушення може бути віднесене до кіберзлочину, якщо воно вчиняється з використанням комп'ютерних систем або телекомунікаційних мереж.

Основна частина статті присвячена методам розслідування кіберзлочинів, які включають кілька етапів: виявлення злочину, збір доказів, аналіз доказів, встановлення винуватців та притягнення до відповідальності. Виявлення злочину може бути досягнуто за допомогою моніторингу мережевого трафіку, аналізу логів та використання систем виявлення вторгнень. Збір доказів включає збирання цифрових слідів, таких як файли, електронна пошта, журнали подій, а аналіз доказів передбачає дослідження зібраних даних для виявлення ключової інформації. Встановлення винуватців є складним завданням, яке вимагає аналізу мережевих даних та співпраці з іншими правоохоронними органами. Притягнення до відповідальності вимагає ретельного документування всіх зібраних доказів та дотримання процедур, передбачених законодавством.

Підкреслюється важливість дотримання міжнародних стандартів та використання сучасних технологій для ефективного розслідування кіберзлочинів. Це включає використання спеціалізованого програмного забезпечення для збору та аналізу цифрових доказів, навчання фахівців з цифрової криміналістики та співпрацю з іншими правоохоронними органами на міжнародному рівні. Завдяки цьому можна досягти більш ефективної протидії кіберзлочинності та забезпечення безпеки у кіберпросторі.

Ключові слова: *кіберзлочинність, розслідування кіберзлочинів, збір цифрових доказів, аналіз доказів, міжнародне співробітництво, цифрова криміналістика.*

Larchenko Maryna. SOME FEATURES OF CYBER CRIMES INVESTIGATION

Abstract. *In today's world, where information technologies are integrated into all spheres of life, cybercrimes are becoming more and more common and complex. These include identity theft, financial fraud, hacking of information systems, distribution of malicious software and other forms of criminal activity in cyberspace. The purpose of the article is to highlight the main aspects and challenges related to the investigation of cybercrimes.*

The article analyzes the latest scientific publications of Ukrainian and foreign authors investigating various aspects of cybercrime, including legal, technical and organizational aspects. Cybercrime is classified into several main categories such as data theft, financial fraud, hacking attacks, malware distribution and cyber terrorism. Conditionally, a criminal offense can be classified as a cybercrime if it is committed using computer systems or telecommunication networks.

The main part of the article is devoted to the methods of investigating cybercrimes, which include several stages: detection of the crime, collection of evidence, analysis of evidence, identification of perpetrators and prosecution. Crime detection can be achieved by monitoring network traffic, analyzing logs and using intrusion detection

systems. Evidence gathering involves collecting digital traces such as files, email, event logs, and evidence analysis involves examining the collected data to uncover key information. Identifying the perpetrators is a complex task that requires analysis of network data and cooperation with other law enforcement agencies. Prosecution requires careful documentation of all evidence collected and compliance with procedures required by law.

The importance of compliance with international standards and the use of modern technologies for the effective investigation of cybercrimes is emphasized. This includes the use of specialized software for the collection and analysis of digital evidence, the training of digital forensics specialists and collaboration with other law enforcement agencies internationally. Thanks to this, it is possible to achieve a more effective countermeasure against cybercrime and ensure security in cyberspace.

Key words: *cybercrime, cybercrime investigation, digital evidence collection, evidence analysis, international cooperation, digital forensics.*

Вступ. У сучасному світі, де інформаційні технології інтегровані у всі сфери життя, кіберзлочини стають усе більш поширеними та складними. Вони можуть включати крадіжку особистих даних, фінансові махінації, зломи інформаційних систем, розповсюдження шкідливого програмного забезпечення, та інші форми злочинної діяльності в кіберпросторі. Розслідування кіберзлочинів має свої особливості, які відрізняють його від традиційних методів кримінального розслідування.

Метою статті є висвітлення основних аспектів та викликів, пов'язаних із розслідуванням кіберзлочинів.

Матеріали та методи. Значна частина наукових робіт в Україні присвячена аналізу різних аспектів цього явища, включаючи правові, технічні та організаційні аспекти. Так, Кравцова М. О. у своєму дослідженні «Сучасний стан і напрями протидії кіберзлочинності в Україні» (2018) [1] звертає увагу на нормативно-правову базу України щодо кіберзлочинності та акцентує увагу на необхідності удосконалення законодавства для ефективної боротьби з кіберзлочинами. Автор зазначає, що основні проблеми полягають у недостатньому рівні правового регулювання та взаємодії між правоохоронними органами різних країн.

Савчук С. у статті «Кіберзлочинність: зміст та методи боротьби» (2009) [2] аналізує основні методи боротьби з кіберзлочинами, наголошуючи на важливості використання сучасних технологій та інноваційних підходів у розслідуванні. Автор вказує на необхідність постійного вдосконалення методів розслідування та підвищення кваліфікації фахівців у цій галузі.

Чернишов Г. М. у своїй статті «Кіберзлочинність як виклик глобалізації та загроза світовій безпеці: теоретичні основи дослідження» (2018) [3] акцентує увагу на глобальному характері кіберзлочинності та необхідності міжнародного співробітництва для ефективної боротьби з нею. Автор підкреслює важливість уніфікації міжнародних стандартів та законодавства для забезпечення ефективної взаємодії між країнами.

Також слід зазначити монографію Кравцової М. О. та Литвинова О. М. «Запобігання кіберзлочинності в Україні» (2016) [4], де детально розглядаються методи запобігання кіберзлочинам та підкреслюється важливість превентивних заходів.

Важливі англомовні публікації у сфері розслідування кіберзлочинів охоплюють широкий спектр тем, від технологічних інновацій до правових викликів. Ці дослідження мають загальносвітове значення та сприяють глибшому розумінню кіберзлочинності та методів її розслідування.

Технологічні інновації є однією з ключових тем у сучасних дослідженнях є використання штучного інтелекту (ШІ) та машинного навчання для боротьби з кіберзлочинами. Наприклад, у роботі «Artificial Intelligence and Machine Learning for Cybersecurity Applications and Challenges» (2023) автори аналізують, як ШІ допомагає виявляти аномалії у великих масивах даних, що може свідчити про злочинну діяльність. Вони також підкреслюють виклики, пов'язані з адаптацією ШІ до постійно змінюваного ландшафту кіберзлочинності [5].

У дослідженні «Digital Forensics: Current State of the Art» автори розглядають сучасні

методи та інструменти цифрової криміналістики. Вони акцентують увагу на важливості аналізу мобільних пристроїв, відновлення видалених даних та відстеження дій користувачів у системах. Особлива увага приділяється автоматизації процесів та використанню спеціалізованого програмного забезпечення для збору та аналізу цифрових доказів [6].

У статті «The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system» (2024) обговорюються правові виклики, з якими стикаються правоохоронні органи у різних країнах. Автори наголошують на необхідності гармонізації міжнародних стандартів та законодавства, що регулюють боротьбу з кіберзлочинністю. Вони також підкреслюють важливість міжнародного співробітництва та обміну інформацією між правоохоронними органами для ефективного розслідування кіберзлочинів [7].

Публікація «Cybersecurity Risks of Blockchain Technology» (2020) досліджує потенціал використання блокчейн-технологій для захисту даних та протидії шахрайству. Автори підкреслюють, що децентралізовані бази даних можуть створити більш захищені системи для зберігання та передачі інформації. У той же час, вони зазначають, що ці технології можуть бути використані злочинцями для нових видів атак [8].

Дослідження «Cybersecurity of Quantum Computing: A New Frontier» (2023) розглядає вплив квантових обчислень на кібербезпеку. Автори прогнозують, що квантові технології можуть значно змінити методи захисту даних, але водночас створюють нові виклики для правоохоронних органів у розслідуванні кіберзлочинів [9].

Стаття «Security in Internet of Things: Issues, Challenges, and Solutions» (2019) аналізує нові вразливості, пов'язані зі зростанням кількості підключених до інтернету пристроїв. Автори пропонують методи захисту IoT-пристроїв, підкреслюючи важливість розробки стандартів безпеки та впровадження нових технологій для протидії кіберзлочинам [10].

Методи дослідження, використані в даній статті: 1) аналіз літератури та нормативно-правових актів. Огляд наукових праць, законодавчих документів та існуючих стандартів у сфері кіберзлочинності для визначення теоретичної бази дослідження; 2) контент-аналіз. Дослідження змісту цифрових доказів, зібраних з різних джерел, таких як комп'ютери, мобільні пристрої та мережеві сховища; 3) емпіричний аналіз. Використання реальних випадків кіберзлочинності для демонстрації практичних аспектів збору та аналізу цифрових доказів; 4) метод комп'ютерного моделювання. Використання спеціалізованого програмного забезпечення для моделювання хакерських атак та їх наслідків з метою оцінки ефективності методів захисту; 5) форензічний аналіз. Використання методів цифрової криміналістики для відновлення, ідентифікації та аналізу даних, що стосуються кіберзлочинів; 6) порівняльний аналіз. Порівняння підходів до розслідування кіберзлочинів у різних країнах для визначення кращих практик та ефективних методик; 7) метод кейсів (Case Study). Докладний аналіз конкретних випадків кіберзлочинності для розкриття складних аспектів та динаміки розслідування.

Ці методи забезпечили комплексний підхід до вивчення кіберзлочинності, що дозволяє краще розуміти її природу та розробляти ефективні стратегії запобігання.

Результати. Кіберзлочини можна класифікувати за кількома основними категоріями:

1) крадіжка даних: незаконне отримання особистої, фінансової або іншої конфіденційної інформації;

2) фінансові махінації: шахрайські дії, що включають використання кібертехнологій для незаконного отримання грошей або майна;

3) хакерські атаки: несанкціонований доступ до інформаційних систем з метою їх пошкодження, зламу або викрадення даних;

4) поширення шкідливого програмного забезпечення: створення та поширення вірусів, троянських програм, руткітів та інших типів зловмисного ПО;

5) кібертероризм: використання кібертехнологій для здійснення терористичних актів або загроз.

Неоднозначним у науковій літературі є питання про належність діяння до кіберзло-

чинів. На думку фахівців, в основу належності кримінального правопорушення до кіберзлочину (комп'ютерного кримінального правопорушення) закладають, зокрема, такі критерії:

– комп'ютерними називають ті кримінальні правопорушення, які законодавець об'єднав у Розділі XVI Особливої частини КК [1]. Умовно цей підхід можна назвати позитивістським, а ознакою, яка відрізняє кіберзлочини від інших та об'єднує їх у певну групу є родовий об'єкт цих кримінальних правопорушень;

– комп'ютерним є кримінальне правопорушення, яке вчиняється з використанням ЕОМ, телекомунікаційних систем, комп'ютерних мереж і мереж електрозв'язку [11; 4]. Тобто, на думку цих авторів, кіберзлочин відрізняється від інших видів кримінальних правопорушень знаряддям вчинення, яким є певна комп'ютерна система, комп'ютерна мережа чи мережа електрозв'язку;

– комп'ютерним є кримінальне правопорушення, предметом якого є комп'ютерна інформація, що обробляється в ЕОМ, АС, комп'ютерних мережах чи мережах електрозв'язку (А. А. Музика, Д. С. Азаров);

– кіберзлочином є кримінальне правопорушення, в якому комп'ютер є або предметом кримінального правопорушення, або знаряддям, або способом його вчинення [2];

– кіберзлочини – це кримінальні правопорушення, в яких кіберпростір є середовищем, предметом (метою) посягання та/або способом вчинення [3];

– кіберзлочин (комп'ютерне кримінальне правопорушення) – це суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України (стаття 1) [12].

У контексті сучасних викликів та загроз кіберзлочинності, на нашу думку, можна виділити кілька ключових видів таких злочинів.

1. Кіберзлочини у власному розумінні – це ті, які неможливо вчинити без використання інформаційних (комп'ютерних) систем. Вони включають прояви кримінально протиправної поведінки, що спрямовані проти інформаційних (комп'ютерних) систем або проти об'єктів чи предметів, що існують, зберігаються, передаються, обробляються у цих системах. Прикладами можуть бути злом комп'ютерних мереж, викрадення даних, несанкціонований доступ до інформації та саботаж комп'ютерних систем.

2. Кримінальні правопорушення, пов'язані з інформаційними (комп'ютерними) системами – це прояви кримінально протиправної поведінки, які вчиняються з використанням цих систем, але можуть здійснюватися і без них. Вони включають, зокрема, кіберпростір та інформаційні технології як інструменти чи засоби реалізації злочинної діяльності. Наприклад, шахрайство через інтернет, розповсюдження шкідливого програмного забезпечення або використання інформаційних технологій для планування та координації злочинів.

3. Злочини проти приватності та конфіденційності – це дії, спрямовані на порушення конфіденційності інформації, такі як крадіжка особистих даних, злом електронної пошти, незаконне перехоплення комунікацій та підробка документів в електронному вигляді.

4. Економічні кіберзлочини – це злочини, що спрямовані на отримання фінансової вигоди через використання комп'ютерних систем, включаючи банківське шахрайство, незаконні фінансові транзакції, відмивання грошей та фінансові піраміди в інтернеті.

5. Кібертероризм та кібершпигунство – ці злочини пов'язані з використанням інформаційних технологій для здійснення терористичних актів або шпигунської діяльності, включаючи атаки на критичну інфраструктуру, злам урядових або військових систем, а також викрадення державних та корпоративних таємниць.

Наведена класифікація кіберзлочинів дозволяє детально аналізувати та протидіяти різним видам кіберзлочинної діяльності.

Усі кіберзлочини мають низку специфічних характеристик, які ускладнюють їх розслідування. Перш за все йдеться про анонімність злочинців, бо інтернет дозволяє

ISSN 2311-8040

останнім діяти знеособлено, використовуючи віртуальні машини, підроблені або крадені ідентифікаційні дані. Також кіберзлочини часто мають глобальний характер, а саме здійснюються через кордони, що ускладнює взаємодію правоохоронних органів різних країн. Інший важливий аспект полягає в технологічній складності змісту цих діянь, бо злочинці використовують складні технологічні засоби та методи, що потребують спеціальних знань для їх викриття. І нарешті, швидкість поширення кіберзлочинів, що дозволяють реалізувати сучасні інформаційні технології, вимагає негайного реагування.

Можна виділити декілька загальних інноваційних підходів до розслідування кіберзлочинів.

По-перше, це використання штучного інтелекту (ШІ) та машинного навчання, що стають незамінними інструментами у розслідуванні кіберзлочинів. Ці технології дозволяють автоматизувати процеси аналізу великих обсягів даних, що значно прискорює виявлення підозрілої активності та ідентифікацію потенційних загроз. Наприклад, алгоритми машинного навчання можуть аналізувати мережевий трафік та виявляти аномалії, які можуть свідчити про зломи або інші кіберінциденти.

По-друге, саме цифрова криміналістика є ключовою складовою розслідування кіберзлочинів. Вона включає в себе методи збору, збереження, аналізу та презентації цифрових доказів. Сучасні інструменти цифрової криміналістики дозволяють проводити глибокий аналіз файлів, відновлювати видалені дані, а також відстежувати дії користувачів у системах. Важливою складовою є також аналіз мобільних пристроїв, адже вони часто використовуються злочинцями для здійснення незаконних дій.

По-третє, ефективне розслідування кіберзлочинів вимагає висококваліфікованих фахівців. Тому особливу увагу слід приділяти спеціалізованому навчанню та підготовці кадрів. Освітні програми мають включати курси з кібербезпеки, цифрової криміналістики, правових аспектів кіберзлочинності та сучасних технологій. Важливим аспектом є також постійне підвищення кваліфікації та обмін досвідом між фахівцями на міжнародних конференціях та семінарах.

По-четверте, розслідування кіберзлочинів вимагає тісної співпраці між державними органами та приватним сектором. Публічно-приватне партнерство дозволяє об'єднувати ресурси, знання та технології для більш ефективного виявлення та запобігання кіберзлочинам. Наприклад, співпраця з технологічними компаніями може допомогти у швидкому виявленні нових загроз та розробці заходів протидії.

По-п’яте, уніфікація міжнародних стандартів та законодавства є важливим кроком у боротьбі з кіберзлочинністю. Спільні зусилля з розробки та впровадження міжнародних правових норм дозволяють забезпечити ефективну взаємодію між країнами у розслідуванні кіберзлочинів. Важливою складовою є також гармонізація процедур щодо збору та обміну доказами, а також забезпечення правової захищеності фахівців, які займаються розслідуванням.

Серед майбутніх тенденцій у боротьбі з кіберзлочинами виділяють розвиток квантових технологій, бо саме квантові обчислення мають потенціал значно змінити ландшафт кібербезпеки. Хоча ці технології можуть використовуватися для створення нових методів захисту даних, вони також можуть стати інструментом у руках злочинців. Тому важливо вже зараз досліджувати можливості квантових обчислень для протидії кіберзлочинам.

Інтернет речей (IoT) відкриває нові можливості для розвитку, але також створює нові вразливості. Зростання кількості підключених до інтернету пристроїв означає, що кіберзлочинці отримують більше можливостей для атак. Розробка методів захисту IoT-пристроїв є одним з пріоритетних напрямків у сфері кібербезпеки.

Великий потенціал для забезпечення безпеки даних та протидії шахрайству мають блокчейн-технології. Використання децентралізованих баз даних може допомогти у створенні більш захищених систем для зберігання та передачі інформації. Крім того,

блокчейн може використовуватися для створення прозорих систем обліку та верифікації транзакцій.

Розслідування кіберзлочинів має свої специфічні аспекти, які відрізняються від традиційних методів розслідування кримінальних правопорушень. Це зумовлено особливостями цифрових технологій та інформаційних систем, що використовуються злочинцями для здійснення протиправної діяльності.

Методологія розслідування кіберзлочинів поділяє цей процес на два основних етапи. Так підготовчий етап включає: 1) формування спеціалізованих команд, залучення фахівців з кібербезпеки, аналітиків даних, юристів та інших експертів; 2) забезпечення технічного обладнання, зокрема. використання сучасних інструментів для аналізу та збору доказів, таких як програмне забезпечення для цифрової криміналістики.

Етап збору та аналізу доказів теж має свої особливості. Він включає: 1) аналіз логфайлів серверів, мережевого трафіку та інших цифрових слідів, які можуть вказувати на діяльність злочинців; 2) використання спеціалізованого програмного забезпечення для вилучення даних з комп'ютерів, мобільних пристроїв та інших цифрових носіїв; 3) аналіз шкідливого програмного забезпечення, що полягає у вивченні коду вірусів, троянських програм та інших зловмисних програм для визначення їх походження та методів дії.

Розслідування кіберзлочинів часто вимагає тісної співпраці з іншими організаціями. Міжнародне співробітництво передбачає взаємодію з правоохоронними органами інших країн через Інтерпол, Європол та інші міжнародні організації. Це співробітництво включає обмін інформацією, координацію спільних операцій та підтримку у проведенні розслідувань, що виходять за межі національних юрисдикцій. Крім того, здійснюється співпраця з приватними компаніями, що надають послуги в галузі кібербезпеки, такими як розробники антивірусного програмного забезпечення, спеціалісти з аналізу загроз та консалтингові фірми. Важливу роль відіграють також постачальники інтернет-послуг та соціальних мереж, які можуть надавати необхідні дані для ідентифікації та відстеження кіберзлочинців. Співпраця з цими суб'єктами дозволяє отримувати цінну інформацію, що сприяє швидшому і точнішому виявленню кіберзлочинної діяльності.

Структуризація методів розслідування забезпечує більш точну і швидку ідентифікацію злочинних дій та залучення відповідних ресурсів для їх розслідування.

Окремо слід сказати про наявні проблеми та виклики в розслідуванні кіберзлочинів. Їх можна представити за двома основними напрямками. Так, технічні виклики можуть бути представлені у вигляді шифрування даних, що ускладнює доступ до інформації. Іншим поширеним напрямком є анонімність та підробка ідентифікаційних даних: використання VPN, проксі-серверів та інших методів для приховування особистості. Ну і нарешті, постійне оновлення та вдосконалення злочинцями своїх технологій і методів.

Юридичні виклики можуть бути пов’язані, в першу чергу, з недосконалістю законодавства, а саме з відсутністю єдиних міжнародних стандартів та законів, що регулюють боротьбу з кіберзлочинами. Крім цього, у країнах романо-германської системи права, до яких належить і Україна, наявне помітне відставання законодавства від розвитку технологій через складність процедури зміни законів, корупційні ризики тощо. Свій вплив на процес реалізують також юрисдикційні проблеми, зокрема, визначення, які країни мають право розслідувати та судити конкретний злочин. І нарешті, не можна відкидати захист приватності, що має полягати в утриманні балансу між дотриманням прав особистості та необхідністю розслідування кіберзлочинів.

Організаційні виклики, у свою чергу, включають нестачу кадрів, що проявляється у дефіциті кваліфікованих фахівців з кібербезпеки; необхідність ефективної координації між різними правоохоронними органами та організаціями; необхідність залучення значних фінансових ресурсів, що існує в умовах обмеженості бюджетів, що виділяються на розслідування кіберзлочинів.

Висновки. Таким чином, розслідування кіберзлочинів є складним і багатоаспектним процесом, що вимагає спеціальних знань та технічних засобів. Інноваційні підходи, такі як використання штучного інтелекту, розвиток цифрової криміналістики, спеціалізоване навчання кадрів та міжнародне співробітництво, є ключовими факторами успіху у боротьбі з кіберзлочинністю. Майбутні тенденції, такі як розвиток квантових технологій, захист IoT-пристроїв та використання блокчейн, визначатимуть подальший напрямок розвитку цієї сфери. Незважаючи на численні виклики, сучасні методи та технології дозволяють ефективно боротися з кіберзлочинністю, захищаючи інформаційні системи та особисті дані громадян. Постійне вдосконалення методології розслідування та підвищення рівня підготовки фахівців, ефективна взаємодія між державними органами, приватним сектором та міжнародною спільнотою є необхідними умовами для забезпечення кібербезпеки у сучасному світі.

Список використаних джерел:

1. Кравцова М.О. Сучасний стан і напрями протидії кіберзлочинності в Україні. *Вісник кримінологічної асоціації України*. 2018. № 2 (19). С. 157. URL : http://dspace.univd.edu.ua/xmlui/handle/123456789/3848.

2. Савчук Н.В. Кіберзлочинність: зміст та методи боротьби. 2009. С. 338–342. URL : http://tppe.econom.univ.kiev.ua/data/2009_19/zb19_48.pdf.

3. Чернишов Г. М. Кіберзлочинність як виклик глобалізації та загроза світовій безпеці: теоретичні основи дослідження. *Прикарпатський юридичний вісник.* 2018. № 3. С. 158–162.

4. Кравцова М.О., Литвинов О.М. Запобігання кіберзлочинності в Україні : монографія. Харків : Панов, 2016. С. 19.

5. Sinha Aditya, Singla Kunal, Victor Teresa Matoso. Artificial Intelligence and Machine Learning for Cybersecurity Applications and Challenges. *Journal of Information Security*, 2023. Vol. 15 No. 3. https://doi.org/10.4018/978-1-6684-9317-5.ch007.

6. Raghavan Sriram. Digital forensic research: Current state of the art. *CSI Transactions on ICT.* 2012. 1. https://doi.org/10.1007/s40012-012-0008-7.

7. Amoo Olukunle, Atadoga Akoh, Abrahams Temitayo, Farayola Oluwatoyin, Osasona Femi, Ayinla Benjamin. The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system. *World Journal of Advanced Research and Reviews*. 2024. 21. P. 205–217. https://doi.org/10.30574/wjarr.2024.21.2.0438.

8. Abdelwahab Ihab, Ramadan Nagy, Hefny Hesham. Cybersecurity Risks of Blockchain Technology. *International Journal of Computer Applications*. 2020. 177. P. 8–14. https://doi.org/10.5120/ijca2020919922.

9. Scanlon T. Cybersecurity of Quantum Computing: A New Frontier. Carnegie Mellon University, Software Engineering Institute's Insights (blog), Accessed July 24, 2024. https://doi.org/10.58012/rzmt-m258.

10. Aldowah Hanan, Rehman Shafiq, Umar Irfan. Security in Internet of Things: Issues, Challenges, and Solutions. 2019. https://doi.org/10.1007/978-3-319-99007-1_38.

11. Біленчук П.Д., Зубань М.А. Комп'ютерні злочини: соціально-правові і кримінолого-криміналістичні аспекти : навч. посібник. Київ : Українська академія внутрішніх справ, 1994. С. 6.

12. Закон України. Про основні засади забезпечення кібербезпеки України. 05.10.2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

References:

1. Kravtsova, M.O. (2018). Suchasnyi stan i napriamy protydii kiberzlochynnosti v Ukraini [The current state and directions of combating cybercrime in Ukraine]. *Visnyk kryminolohichnoi asotsiatsii Ukrainy*. № 2 (19). S. 157. Retrieved from: http://dspace.univd.edu.ua/xmlui/handle/123456789/3848 [in Ukrainian].

2. Savchuk, N.V. (2009). Kiberzlochynnist: zmist ta metody borotby [Cybercrime: content and methods of combat]. S. 338–342. Retrieved from: http://tppe.econom.univ.kiev.ua/data/2009_19/zb19_48.pdf [in Ukrainian].

3. Chernyshov, H.M. (2018). Kiberzlochynnist yak vyklyk hlobalizatsii ta zahroza svitovii bezpetsi: teoretychni osnovy doslidzhennia [Cybercrime as a challenge of globalization and a threat to world security: theoretical foundations of the study]. *Prykarpatskyi yurydychnyi visnyk*. № 3. S. 158–162 [in Ukrainian].

4. Kravtsova, M.O., & Lytvynov, O.M. (2016). *Zapobihannia kiberzlochynnosti v Ukraïni [Prevention of cybercrime in Ukraine] : monohrafiia.* Kharkiv : Panov. S. 19 [in Ukrainian].

5. Sinha, Aditya, Singla, Kunal, & Victor, Teresa Matoso. (2023). Artificial Intelligence and Machine Learning for Cybersecurity Applications and Challenges. *Journal of Information Security*, Vol. 15 No. 3. https://doi.org/10.4018/978-1-6684-9317-5.ch007 [in English].

6. Raghavan, Sriram (2012). Digital forensic research: Current state of the art. CSI Transactions on ICT. 1. https://doi.org/10.1007/s40012-012-0008-7 [in English].

7. Amoo, Olukunle, Atadoga, Akoh, Abrahams, Temitayo, Farayola, Oluwatoyin, Osasona, Femi, & Ayinla, Benjamin. (2024). The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system. *World Journal of Advanced Research and Reviews.* 21. P. 205–217. https://doi.org/10.30574/wjarr.2024.21.2.0438 [in English].

8. Abdelwahab, Ihab, Ramadan, Nagy, & Hefny, Hesham (2020). Cybersecurity Risks of Blockchain Technology. *International Journal of Computer Applications.* 177. P. 8–14. https://doi.org/10.5120/ijca2020919922 [in English].

9. Scanlon, T. (2024). Cybersecurity of Quantum Computing: A New Frontier. Carnegie Mellon University, Software Engineering Institute's Insights (blog), Accessed July 24. https://doi.org/10.58012/rzmt-m258 [in English].

10. Aldowah, Hanan, Rehman, Shafiq, & Umar, Irfan (2019). Security in Internet of Things: Issues, Challenges, and Solutions. https://doi.org/10.1007/978-3-319-99007-1_38 [in English].

11. Bilenchuk, P.D., & Zuban, M.A. (1994). *Komp'iuterni zlochyny: sotsialno-pravovi i kryminoloho-kryminalistychni aspekty [Computer crimes: socio-legal and criminological-forensic aspects]* : navch. posibnyk. Kyiv : Ukraïnska akademiia vnutrishnikh sprav. S. 6 [in Ukrainian].

12. Zakon Ukrainy. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy [About the main principles of ensuring cyber security of Ukraine]. 05.10.2017 roku № 2163-VIII. Retrieved from: https://zakon.rada.gov.ua/laws/show/2163-19#Text [in Ukrainian]