МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХЕРСОНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ БІЗНЕСУ І ПРАВА
КАФЕДРА НАЦІОНАЛЬНОГО, МІЖНАРОДНОГО ПРАВА
ТА
ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ

ПРОТИДІЯ КІБЕРЗЛОЧИНАМ: ТЕОРІЯ ТА ПРАКТИКА

Кваліфікаційна робота (проєкт)
на здобуття ступеня вищої освіти «магістр»

Виконав: здобувач ІІ курсу 10-283 М група
Спеціальності: 262 «Правоохоронна діяльність»
Освітньо-професійної програми «Правоохоронна діяльність»
Ващенко Денис Юрійович
Керівник **д.ю.н., проф. Стратонов В.М.**
Рецензент **д.ю.н., проф. Галунько В.М.**

Івано-Франківськ – 2025

ВСТУП

Актуальність теми. У сучасному світі кіберзлочинність стала одним із найнебезпечніших видів злочинної діяльності. З огляду на швидкий розвиток цифрових технологій і глобалізацію інформаційних потоків, зростаючу роль кіберпростору, у всіх сферах життя людства з'явилися нові форми злочинів, які становлять серйозну соціальну загрозу як для окремих громадян, так і для національної безпеки держав і всього світу в цілому. В Україні лише за 2022-2023 роки зафіксовано понад 4000 кібератак [11; 41]. І тому більшість вчених які займаються визначенням питання класифікації кіберзлочинності та методів боротьби. І тому, ми вирішили детально розглянути роботи таких науковців як: О.А.Баранов [1]., М.І. Саєнко [2], В.М. Стратонова [44-46], А.І. Марущак [3], А.Іллєнко [4], В. В. Топчія, О. М. Бодунової [5] та інших.

Так, О.А. Баранов у своїй праці «Про тлумачення та визначення терміну «кібербезпека» де автор запропонував власне бачення терміну «кібернетична безпека» та його співвідношення з поняттями кібер-загрози та кіберзлочинності [1].

А вже міжнародний досвід боротьби з комп'ютерною злочинністю та комп'ютерним шахрайством, який може бути використаний в Україні, проаналізував М.І. Саєнко у статті «Міжнародний досвід боротьби з комп'ютерною злочинністю та комп'ютерним шахрайством та можливості їх використання в Україні» [2].

Щодо проблеми міжнародного співробітництва у боротьбі з транснаціональною кіберзлочинністю розкрито відповідь дав А.І. Марущак у праці науковій роботі «Міжнародне співробітництво в боротьбі з транснаціональною кіберзлочинністю», наголосивши на ролі конвенцій та міжнародних інститутів у формуванні глобальної системи кіберзахисту [3].

Сучасні тенденції розвитку кіберзагроз, особливо у сфері критичної інфраструктури України, дослідила А. Іллєнко у статті «Сучасні кіберзагрози критичної інфраструктури України», де авторка наголошує на зростанні ролі державних структур у запобіганні кібератакам [4].

Окремі проблемні питання забезпечення кібербезпеки України в умовах цифрової трансформації та війни висвітлено в роботі В. В. Топчія та О. М. Бодунової «Проблемні питання забезпечення кібербезпеки в Україні», в якій автори звертають увагу на необхідність оновлення нормативно-правової бази та посилення публічно-приватної взаємодії [5].

Тому ми вважаэмо, що для України ця проблема є особливо актуальною з огляду на триваючу гібридну війну, в рамках якої кіберпростір постійно використовується як поле бою. Злочинці здійснюють кібератаки на об'єкти критичної інфраструктури, державні установи, енергетичні компанії та фінансові установи з метою дестабілізації соціально-економічної ситуації в країні.

Слід також зазначити, що цифровізація та розвиток державних послуг, таких як «Дія» та інші електронні пристрої, створюють значну потребу в нових підходах до боротьби з кіберзлочинністю.

Ми переконані, що в цьому контексті особливого значення набуває дослідження теоретичних основ та практичних механізмів боротьби з кіберзлочинністю. Я вірю, що ці результати допоможуть створити основу для вдосконалення національної стратегії кібербезпеки, підвищення ефективності правоохоронних органів та посилення захисту державного і приватного секторів від кіберзагроз.

Зв’язок роботи з науковими програмами, планами, темами. Кваліфікаційну роботу виконано в контексті наукових досліджень відповідно до Стратегія розвитку Національної академії правових наук України на 2021-2025 рр. (затверджено Постановою загальних борів НАПрН України від 26.03.21 р. від 12-21), тематики науково-дослідної роботи кафедри національного, міжнародного права та правоохоронної діяльності факультету бізнесу і права Херсонського державного університету «Теоретичні та практичні проблеми розвитку окремих галузей права» (номер державної реєстрації – 0124U002381). Тему кваліфікаційної роботи затверджено Вченою радою Херсонського державного університету (наказ №642-Д від 11.11.2024 р.)

Мета і завдання. Метою кваліфікаційної роботи є комплексне дослідження теоретичних основ, правових механізмів та практичних аспектів боротьби з кіберзлочинністю в Україні, а також розробка рекомендацій, механізмів та підвищення ефективності національної системи боротьби з кіберзлочинністю з урахуванням міжнародного досвіду та сучасних технологічних тенденцій.

Основні завдання, які необхідно вирішити для досягнення мети:

- Деталізувати поняття «кіберзлочин» та простежити еволюцію його розвитку в контексті міжнародного права.

- Проаналізувати класифікацію кіберзлочинів та визначити їх основні характеристики, що відрізняють їх від традиційних форм злочинності.

- Дослідити міжнародні правові та національні механізми боротьби з кіберзлочинами.

- Оцінити сучасний стан кіберзагроз в Україні та визначити ключові напрямки діяльності правоохоронних органів та спеціальних органів у цій сфері.

- Дослідити практичний приклад (випадок) фішингової кампанії проти державної установи як ілюстрацію типового кіберзлочину.

- Запропонувати модель вдосконалення системи виявлення та запобігання кіберзлочинам, орієнтовану на людський фактор та технологічні інновації.

- Сформулювати рекомендації щодо підвищення ефективності національної політики у сфері кібербезпеки та її приведення у відповідність до міжнародних стандартів (NIS2, ENISA, НАТО).

Об'єкт дослідження - це суспільні відносини, що виникають у сфері забезпечення кібербезпеки, а також правові та організаційні засади запобігання, виявлення та розслідування злочинів, учинених у кіберпросторі.

Предметом дослідження є система боротьби з кіберзлочинністю в Україні та світі в контексті сучасних викликів цифрової ери.

Методи та завдання. Метою цієї кваліфікаційної роботи є вивчення

теоретичних та проблемних питань, для чого було використано комбінацію загальних наукових та спеціальних методів, а саме:

• аналітичний метод – для вивчення теоретичних підходів до визначення сутності кіберзлочинів та їх типології;

• порівняльно-правовий метод – для аналізу міжнародних та національних нормативно-правових актів, що регулюють питання боротьби з кіберзлочинністю;

• системно-структурний метод – для виявлення взаємозв'язків між державними органами, що забезпечують кібербезпеку;

• емпіричний метод – для аналізу реального випадку фішингової атаки на державну установу;

• моделювання та прогнозування – для розробки рекомендацій щодо вдосконалення системи боротьби з кіберзлочинами та прогнозування ефективності запропонованих заходів.

Апробація результатів дослідження. Результати дослідження представлені на Міжнародній науково-практичній конференції «Стратегічні пріоритети розвитку економіки, менеджменту, сфери обслуговування та права в умовах інтеграційних процесі». (13-14 листопада 2025 року, Івано-Франківськ).

Публікації. Ващенко Д.Ю. Кіберзлочинність:актуальні виклики та методи протидії. *Стратегічні пріоритети розвитку економіки, менеджменту, сфери обслуговування та права в умовах інтеграційних процесів:* матеріали Міжнародної науково-практичної конференції (ХДУ, 13-14 листопада 2025 р.) / за ред. Мельникової К.В. Івано-Франківськ: ХДУ, 2025. С.515-517. https://doi.org/10.5281/zenodo.17938219

Структура та обсяг роботи. Робота складається зі вступу, трьох розділів, що включають дев’ять підрозділів, висновків, списку використаних джерел. Загальна кількість сторінок – 54, обсяг основного тексту – 45 сторінок, список використаних джерел – 4 сторінки (49 найменування).

РОЗДІЛ 1
ТЕОРЕТИКО-ПРАВОВІ ОСНОВИ ПРОТИДІЇ КІБЕРЗЛОЧИНАМ

1.1. Поняття, класифікація та еволюція кіберзлочинів

Як правило, поняття кіберзлочинності у сучасному розумінні вважається сукупністю протиправних дій, що вчиняються з використанням інформаційних та комунікаційних технологій і спрямовані на порушення конфіденційності, цілісності або доступності комп'ютерних систем, мереж та даних [1]. У визначенні, запропонованому Європолом, підкреслюється, що кіберзлочинність включає не тільки злочини, безпосередньо спрямовані проти комп'ютерних систем, але й традиційні злочини, в яких цифрові технології є основним інструментом їх вчинення [16]. Такий підхід відображає інтеграцію кіберпростору в усі сфери суспільного життя, де цифрова інфраструктура стає не тільки об'єктом, але й середовищем злочинної діяльності.

Сучасна класифікація кіберзлочинів базується на системному підході, який враховує як об'єкт нападу, так і характер використовуваних технологій. Першу групу складають злочини, спрямовані проти конфіденційності, цілісності та доступності інформації або комп'ютерних систем. Сюди входять несанкціонований доступ до даних, їх перехоплення, поширення шкідливого програмного забезпечення, атаки типу DDoS, а також діяльність, пов'язана з кібершпигунством [3;16]. Такі протиправні дії безпосередньо порушують функціональну стабільність інформаційних систем і становлять найбільшу загрозу для державних структур та об'єктів критичної інфраструктури.

Друга група включає так звані комп'ютерно-орієнтовані злочини, в яких інформаційні технології використовуються як інструмент для досягнення злочинної мети. Серед них найпоширенішими є фішинг, соціальне інженерство, кібершантаж (ransomware), онлайн-шахрайство та незаконне заволодіння цифровими активами [4;5;16]. У цьому випадку цифрове середовище є не метою, а

засобом для реалізації злочинних намірів, що значно ускладнює процеси ідентифікації злочинців та збору доказів.

Окрему категорію становлять злочини, пов'язані з контентом, тобто з незаконним створенням, поширенням або використанням інформаційних матеріалів. До цієї групи належать прояви кібербулінгу, публікація або поширення забороненого контенту, зокрема матеріалів, що пропагують насильство або порнографію, а також цифрове піратство, пов'язане з порушенням авторських та суміжних прав [6;1]. Особливістю цих злочинів є їх висока латентність і складність у визначенні юрисдикції, оскільки поширення контенту часто має транскордонний характер.

Сучасна кіберзлочинність має багатовимірний характер і включає як дії, спрямовані безпосередньо на інформаційні системи, так і злочини, в яких інформаційні технології використовуються як інструмент або середовище для досягнення незаконних цілей. Це вимагає постійного вдосконалення правових, технічних та організаційних механізмів боротьби з цією злочинністю, а також формування міжнародної координації в галузі кібербезпеки [16].

Таблиця 1.1

*Класифікація основних типів кіберзлочинів за цілями, методами впливу та наслідками**

Тип злочину	Основні цілі	Методи впливу	Типові наслідки
Ransomware	Організації, критична інфраструктура	Шифрування даних, вимога викупу	Фінансові втрати, зупинка роботи
Фішинг	Фізичні особи, співробітники	Соціальна інженерія, підроблені сайти	Викрадення облікових даних
DDoS-атаки	Онлайн-сервіси, урядові сайти	Перевантаження серверів	Відмова в обслуговуванні
Кібершпигунство	Державні установи, компанії	Цільові атаки, APT	Втрата конфіденційної інформації

*Примітка. Складено автором за даними джерел відповідно розділу 1 [3]

Ми впевнені, що комп’ютерна злочинність – одна з найнебезпечніших форм сучасної світової злочинності, яка зародилася в 20 столітті і активно продовжує розвивається в 21 столітті. На мою думку та думку інших провідних експертів, кіберзлочинність є логічним наслідком цифрової трансформації суспільства [5]. І тому розвиток інформаційно-комунікаційних технологій, технологій масової цифровізації економіки, управління та соціальної сфери створили нові можливості не лише для прогресу та розвитку, а й для протиправної та злочинної діяльності. І вже на початку 21 століття це явище постійно розвивається і змінюється від окремих технічних інцидентів до складних і організованих транснаціональних явищ, які щорічно завдають значних економічних, політичних і соціальних збитків державам, окремим громадянам і людству в цілому.

Наукове визначення терміну «кіберзлочинність» ніколи не мало єдиного підходу через різні тлумачення, але більшість формулювань науковців сходяться на тому, що головну та визначальну роль відіграють інформаційні технології, які безпосередньо використовуються для вчинення злочинів у кіберпросторі. А в більшості міжнародних джерел і науковихих статтях поняття кіберзлочинності ґрунтується на використанні комп’ютера, Інтернету чи іншої інформаційно-комунікаційної системи як засобу, об’єкта чи середовища злочину [10].

Наприклад, важливо зазначити те, що у визначенні Encyclopaedia Britannica (2023) говориться про те, що кіберзлочинність – це використання комп'ютерних технологій для вчинення протиправних дій – шахрайства, крадіжки особистих даних, порушення авторських прав чи несанкціонованого доступу [15]. Також, схожий підхід займає Управління ООН з наркотиків і злочинності (UNODC, 2023), вона додає, що кіберзлочинність це будь-яке порушення закону через втручання в інформаційні системи, інтернет або дані, ці дії, як правило, та мають на меті порушення закону, незалежно від територіальної юрисдикції [25].

У міжнародному-правовому контексті найбільш впливовим визначенням інформаційної злочинності займається Будапештська конвенція про кіберзлочинність (Convention on Cybercrime, 2001), яка розглядає кіберзлочинність як протиправну діяльність, пов'язану з використанням комп'ютерних систем і даних

[7]. В цьому документі визначено чотири основні групи злочинів, а саме: порушення конфіденційності, цілісності та доступності інформації; комп'ютерне шахрайство та підробка; злочини, пов'язані з дитячою порнографією; а також порушення авторських та суміжних прав у цифровому середовищі. Це визначення стало основою, так званим базисом. для створення потужного та ефективного національного законодавства більшості держав-учасниць, включаючи Україну.

Основною складністю визначення поняття кіберзлочинності є її зумовлення міждисциплінарного характеру, тобто – вона поєднує технічні, правові та соціальні аспекти. По-перше, йдеться не тільки про незаконне використання комп'ютера або мережі інтернету, але й про будь-які дії, що підривають довіру до цифрової економіки держав, установ, організації, створюють постійні ризики для функціонування фінансових систем, критичної інфраструктури, безпеки персональних даних громадян та людей в цілому [12;15]. У цьому контексті, важливо зазначити, що кіберзлочинність вважається загрозою не лише для окремих користувачів, але й для національної безпеки загалом.

Класифікація та розслідування кіберзлочинів є одним з основних сфер досліджень сучасної кримінології та кіберправа. В науковій практиці поширеним методом є двочленна класифікація, розроблена у звітах Європейського парламенту (2024) та Європолу [11;16]. Вона поділяє злочини на дві категорії: злочини, що залежать від інформаційних і комунікаційних технологій (cyber-dependent crimes), та злочини, що підтримуються інформаційними технологіями (cyber-enabled crimes). До першої категорії належать злочини, які можуть бути скоєні лише в цифровому середовищі, зокрема хакерство, поширення шкідливого програмного забезпечення (malware), DDoS-атаки, вимагання за допомогою шифрування даних (ransomware) та кібертероризм. А до другої категорії належать традиційні злочини, які набули нових проявів завдяки використанню цифрових технологій, таких як: це фінансові махінації, онлайн-шахрайство, торгівля людьми, наркотиками або зброєю через мережу «даркнет» [11;16].

Крім того, класифікація кіберзлочинності групою українських дослідників як правило, пропонують ефективний та багаторівневий підхід, який враховує і

аналізує не тільки технічну складову, але й об'єкт нападу, мотиви протиправних дій та суспільно небезпечні наслідки [1;2;3;4;5;16]. Враховуючи це, кіберзлочини поділяються на три основні групи: проти інформаційних систем та даних, проти майна (зокрема фінансові злочини та крадіжки) та проти особи (до яких належать кібербулінг, онлайн-шантаж, переслідування тощо). Окремою категорією виступають злочини, які загрожують державним або військовим інтересам, особливо, кібершпигунство та атаки на критичну інфраструктуру, які в останні роки залишаються головним викликом для національної безпеки України [6;15].

Постійний розвиток кіберзлочинності, як правило, часто та тісно пов'язаний із загальним розвитком комп'ютерних технологій та розвитком цифровізації. Першими відомими випадками комп'ютерних злочинів датуються 60-ми роками 20 століття, коли злочинці массово здійснювали несанкціоновані маніпуляції з банківськими обчислювальними системами. А в 70-х роках вже з'явилися перші експериментальні комп’ютерns віруси, серед яких прославився вірус «Creeper», який продемонстрував здатність до самовідтворення. Протягом 80-х років, у 20 столітті з'являються перші хакерські спільноти/групи, а інцидент з «Morris worm» у 1988 році став першим великим випадком зараження комп'ютерних систем у мережі ARPANET, що фактично започатковує еру шкідливого програмного забезпечення. З того часу кіберзлочинність стає глобальним суспільно-небезпечним явищем, яке постійно та паралельно розвивається з технологічним прогресом і як правило, постійно змінює свої форми, масштаби та методи [5;11;12].

Вже у 90-х роках 20 століття розвиток Інтернету, починає відкривати нові можливості як для бізнесу, так і для злочинців. Загалом, саме тоді і з'являються перші випадки онлайн-шахрайства, крадіжок номерів кредитних карток та несанкціонованого доступу до урядових баз даних. У 2000-х роках ситуація кіберзлочинності набуває комерційного виміру: починають з'являтися злочинні організації, які спеціалізуються на фінансових атаках та торгівлі викраденими даними.

На початку 2010-х років почали поширюватися програми для здійснення шантажу, які стають однією з найприбутковіших форм злочинності. За даними

аналітичного звіту Webroot (2019), тільки в 2018–2019 роках збитки, спричинені атаками програм-вимагачів, у світі перевищили 8 мільярдів доларів, а загальні економічні збитки, спричинені кіберзлочинністю, у 2021 році досягають 6 трильйонів доларів (Cybersecurity Ventures, 2021) [10; 41;42].

Сьогодні кіберзлочинність має організований, структурований і високотехнологічний характер. Більшість злочинів скоюють не окремі особи, а скоординовані групи, які функціонують за принципом комерційних структур. Поширеним явищем став модель Cybercrime-as-a-Service, коли програмні засоби для атак продаються або орендуються в «темному» Інтернеті. Злочинці активно використовують штучний інтелект, генеративні моделі тексту та зображень, а також технології deepfake для створення фішингових кампаній нового покоління, що робить їх набагато складнішими для виявлення. Крім того, розвиток Інтернету речей (IoT) та хмарних послуг розширив сферу потенційних атак: вразливими стають також побутові прилади, транспорт, медичні пристрої [8;9;12].

У глобальному масштабі боротьба з кіберзлочинністю вимагає уніфікації законодавства та тісної міжнародної співпраці. Будапештська конвенція 2001 року, доповнена другим протоколом 2022 року, є основним міжнародним правовим інструментом у цій сфері, який встановлює механізми співпраці між державами, стандарти криміналізації діянь та процедури міжнародної правової допомоги [7]. Важливим є також створення національних стратегій кібербезпеки, які включають превентивні заходи, навчання персоналу та підвищення цифрової грамотності населення.

Розвиток кіберзлочинності відбувається паралельно з розвитком технологій та цифровізацією суспільства. Він пройшов шлях від поодиноких інцидентів до системного явища, яке має глобальний характер і впливає на політичну стабільність, економічну безпеку та особисте життя людини. Сучасна кіберзлочинність є не тільки технічним, але й соціальним явищем, яке вимагає міждисциплінарного підходу, що поєднує знання в галузі права, IT, психології та міжнародних відносин.

На мою думку, поняття кіберзлочинності сьогодні виходить далеко за межі технічного визначення. Це вже не просто злочини, вчинені за допомогою комп’ютерних технологій, а цілий соціально-правовий феномен, який охоплює сфери економіки, безпеки, політики та навіть культури. Я вважаю, що сучасна класифікація кіберзлочинів повинна враховувати не лише спосіб їх скоєння, а й мотиви, наслідки та рівень технологічного розвитку злочинців. Оскільки, кіберзлочинність потребує постійного наукового переосмислення, адже з кожним роком розвиваються цифрові технології, внаслідок чого з’являються нові види злочинів, які не вкладаються у традиційні правові категорії [1; 4; 5; 6].

1.2. Міжнародні та національні правові рамки протидії кіберзлочинності

Система боротьби з комп'ютерною злочинністю є багаторівневою і поєднує міжнародні, регіональні та національні правові механізми. У сучасному глобалізованому світі, де злочини в кіберпросторі не знають державних кордонів, питання координації та гармонізації законодавства є особливо актуальним. Ефективна боротьба з кіберзлочинністю можлива лише за умови тісної співпраці між державами, міжнародними організаціями, приватним сектором та науковими установами [16;21;25].

Аналізуючи міжнародно-правові рамки, можна абсолютно точно визначити те, що основним міжнародним документом у сфері боротьби з кіберзлочинністю є Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція), яка прийнята 23 листопада 2001 року [7; 21]. Це перший і на сьогодні найвпливовіший багатосторонній договір, спрямований на гармонізацію внутрішнього кримінального законодавства держав-учасниць, спрощення процедур міжнародного співробітництва та уніфікацію підходів до розслідування кіберзлочинності. Конвенція визначає чотири основні групи протиправних дій: злочини проти конфіденційності, цілісності та доступності комп'ютерних систем і даних (наприклад, несанкціонований доступ, перехоплення, втручання);

комп'ютерне шахрайство та підробка; злочини, пов'язані з дитячою порнографією; порушення авторських та суміжних прав у цифровому середовищі.

Окрім криміналізації певних діянь, Будапештська конвенція створює правові основи міжнародного співробітництва – механізми видачі, взаємної правової допомоги, оперативного зберігання електронних доказів, а також створення постійних контактних пунктів (24/7 network) для швидкого обміну інформацією між органами, що здійснюють кримінальне переслідування. Завдяки цим положенням конвенція залишається ефективним інструментом і через понад 20 років після її прийняття.

У 2022 році було прийнято другий додатковий протокол до Будапештської конвенції, який враховує нові технологічні виклики. Він встановлює процедуру доступу до збережених комп'ютерних даних, посилює співпрацю між державами та приватними компаніями (зокрема, постачальниками послуг та платформами для зберігання даних) та встановлює правила співпраці під час розслідування транскордонних комп'ютерних злочинів [7].

Паралельно з цим функціонують й інші міжнародні механізми. Організація Об'єднаних Націй через Управління з наркотиків та злочинності (UNODC) розробляє навчальні модулі, рекомендації та керівні принципи для гармонізації національного законодавства. Вони зосереджуються на принципах дотримання прав людини, зокрема захисту приватного життя в процесі розслідування [25]. Міжнародна організація кримінальної поліції (Інтерпол) координує міжнародні операції проти транснаціональних кібергруп, створює бази даних кіберінцидентів та організовує спільні розслідування.

На рівні Європейського Союзу важливу роль відіграють Європол та Агентство ЄС з кібербезпеки (ENISA). Європол щорічно публікує звіт «Оцінка загрози організованої злочинності в Інтернеті» (IOCTA), в якому аналізує тенденції злочинності в кіберпросторі, а ENISA формує політику кіберстійкості, готує рекомендації щодо кіберзахисту критичної інфраструктури та розробляє стандарти безпеки для держав-членів [13].

У глобальному масштабі також розглядається ініціатива щодо створення нової Конвенції ООН про кіберзлочинність, проект якої обговорюється з 2022 року. Її метою є доповнення та розширення положень Будапештської конвенції, що зробить їх універсальними для країн, які не є членами Ради Європи. Її прийняття очікується в найближчі роки [23].

Доречі, аналізуючи, національний правовий простір України. Можна визначити, що з 2005 року Україна є договірним членом Будапештської конвенції, що стало важливою віхою у формуванні власної системи кібербезпеки [27]. Нормативно-правова база нашої держави базується на принципах, закріплених у міжнародних документах, і включає низку спеціальних законів, підзаконних актів та стратегічних документів. Ключовим нормативним актом є Закон України «Про основні засади забезпечення кібербезпеки України» (2017), який визначає правові та організаційні засади формування системи кібербезпеки, розподіляє повноваження між державними органами та регулює питання захисту критичної інформаційної інфраструктури. Закон передбачає створення єдиної державної системи реагування на кіберінциденти (CERT-UA) та визначає співпрацю між суб'єктами сектору безпеки та оборони, зокрема Службою безпеки України, Міністерством оборони, Державною спеціальною службою, кіберпідрозділами Національної поліції тощо [26;43].

На кримінальному рівні відповідальність за злочини у сфері використання комп'ютерних систем регулюється розділом XVI Кримінального кодексу України, який включає статті 361–363-2 [22]. Ці норми встановлюють покарання за несанкціонований доступ до інформаційних систем, створення та розповсюдження шкідливого програмного забезпечення, перехоплення інформації, втручання в роботу мереж або комп'ютерів, а також за незаконне використання електронних засобів платежу. В останні роки до цієї частини неодноразово вносилися зміни з метою приведення українського законодавства у відповідність до міжнародних стандартів та директив ЄС.

Крім того, у 2023 році було оновлено Стратегію кібербезпеки України, затверджену указом президента. Документ передбачає посилення державної та

приватної співпраці у сфері кіберзахисту, розвиток кадрового потенціалу, вдосконалення нормативної бази та підвищення стійкості критичної інфраструктури. Важливою новинкою стало визначення поняття «національна кіберстійкість» – здатність держави та суспільства забезпечити безперебійне функціонування в умовах кіберзагроз [24].

У 2025 році набув чинності новий закон України про кібербезпеку, який гармонізує національне законодавство з європейськими директивами NIS2 (Network and Information Security Directive). Він розширює перелік об'єктів критичної інфраструктури, запроваджує систему сертифікації кіберзахисту та підвищує вимоги до приватних компаній у сфері інформування про кіберінциденти [19].

Таким чином, Україна поступово створює комплексну систему боротьби з кіберзлочинністю, яка інтегрована в міжнародну правову архітектуру. Однак проблемними залишаються питання координації між відомствами, кадрового забезпечення, фінансування та практичної реалізації механізмів міжнародного співробітництва. Незважаючи на це, нормативно-правові засади, побудовані на основі Будапештської конвенції, забезпечують основу для подальшого зміцнення національної кіберстійкості та ефективної реакції на сучасні загрози в цифровому середовищі.

Розвиток підходів до боротьби з комп'ютерною злочинністю пройшов кілька ключових етапів:

Період 1970–1990: Початок кібербезпеки. Створення перших антивірусних програм (перший вірус «Brain» з'явився в 1986 році). Розробка криптографічних методів захисту. Поява перших міжмережевих фільтрів

Період 1990–2000: Створення правового поля. Прийняття перших міжнародних конвенцій. Створення спеціалізованих підрозділів у правоохоронних органах. Розробка стандартів інформаційної безпеки (ISO 27001)

Період 2000-2010: Інституціоналізація боротьби. Прийняття Будапештської конвенції (2001). Створення національних центрів CERT. Розвиток міжнародного співробітництва

Період 2010-дотепер: Комплексний підхід. Інтеграція штучного інтелекту та машинного навчання. Розвиток проективних методів захисту. Створення кібернетичних стратегій держав

Для України ключовим періодом став час після 2014 року, коли кібернетичні атаки стали частиною гібридної війни. За даними CERT-UA, лише в 2022-2023 роках Україна відбила понад 4000 масштабних кібернетичних атак [CERT-UA, 2023] [11].

І тому я абсолютно переконаний, що основою ефективної боротьби з кіберзлочинністю є гармонізація міжнародного та національного законодавства. Україна, приєднавшись до Будапештської конвенції, зробила важливий крок у напрямі інтеграції до європейської системи кіберзахисту. Водночас національні норми потребують подальшого вдосконалення для відповідності сучасним стандартам ЄС. На мою думку, ключовим викликом залишається не лише прийняття законів, а й забезпечення їх практичного виконання — особливо у сфері кримінального переслідування кіберзлочинців і міжнародного співробітництва [10; 12; 13; 21].

1.3. Проблеми та виклики у сфері кібербезпеки

Система міжнародного правового регулювання у сфері боротьби з комп'ютерною злочинністю виникла як реакція на глобалізацію цифрового простору, зростання кількості кібернетичних атак та складність їх характеру. Одним з найважливіших документів, що визначив основні принципи міжнародного співробітництва в цій сфері, є Конвенція Ради Європи про комп'ютерну злочинність (Будапештська конвенція), прийнята 23 листопада 2001 року. Це перший міжнародний багатосторонній договір, який встановлює єдині підходи до криміналізації злочинів, скоєних за допомогою комп'ютерних систем, а також до процедур збору цифрових доказів і механізмів міжнародного правового співробітництва [7;21;27].

Будапештська конвенція розрізняє чотири основні групи комп'ютерної злочинності:

- злочини проти конфіденційності, цілісності та доступності комп'ютерних систем і даних (несанкціонований доступ, перехоплення, втручання);
- комп'ютерне шахрайство та підробка;
- злочини, пов'язані з дитячою порнографією;
- порушення авторських та суміжних прав у цифровому середовищі.

Документ також встановлює процедурні механізми міжнародного співробітництва: зберігання даних, швидкий доступ до комп'ютерної інформації, видача, взаємна правова допомога, а також створення постійних контактних пунктів (мережа 24/7). Саме завдяки цим інструментам конвенція залишається актуальною і через більше ніж два десятиліття після її прийняття. У 2022 році було прийнято другий додатковий протокол, який розширив можливості транскордонного доступу до електронних доказів і встановив співпрацю держав з приватними компаніями, що зберігають інформацію [7].

У рамках Європейського Союзу велике значення має Директива (ЄС) 2022/2555 (NIS2), яка замінила попередню Директиву NIS від 2016 року. Вона встановлює єдині мінімальні вимоги до безпеки мережевих та інформаційних систем у ключових секторах – енергетиці, транспорті, фінансах, охороні здоров'я, цифрових послугах тощо. Документ також встановлює вимоги до управління ризиками, зобов'язує операторів критичних послуг повідомляти про інциденти безпеки та встановлює санкції за їх невиконання. NIS2 створює основу для створення єдиного простору кіберстійкості в рамках ЄС і є орієнтиром для країн-партнерів, зокрема України, яка поступово гармонізує своє національне законодавство з її положеннями [33].

Важливою складовою міжнародної нормативної системи є стандарти ISO/IEC 27000, які встановлюють вимоги до систем управління інформаційною безпекою (ISMS). Стандарти ISO/IEC 27001 та 27002 детально описують політики, процедури, технічні та організаційні заходи для захисту інформації. Їх застосування визнається в усьому світі як показник належного рівня безпеки, особливо під час аудиту критичної інфраструктури або оцінки кібернетичних ризиків.

Таблиця 1.2

*Порівняльна характеристика міжнародних та національних правових актів у сфері протидії кіберзлочинності**

Рівень регулювання	Нормативний акт / документ	Основні положення	Механізми реалізації	Значення для України
Міжнародний	Будапештська конвенція про кіберзлочинність (2001)	Визначає основні види кіберзлочинів, процедурні механізми збору цифрових доказів і взаємодії між державами.	Мережа 24/7, взаємна правова допомога, екстрадиція, збереження даних.	Сприяє уніфікації кримінального законодавства України з європейськими стандартами.
Міжнародний (ЄС)	Директива (ЄС) 2022/2555 – NIS2	Встановлює мінімальні вимоги до кіберзахисту критичної інфраструктури та управління ризиками.	Зобов’язання повідомляти про інциденти, аудит безпеки, санкції за порушення.	Використовується як орієнтир у гармонізації українського законодавства.
Міжнародний (технічний)	Стандарти ISO/IEC 27000 (27001, 27002)	Регламентують створення систем управління інформаційною безпекою.	Сертифікація, моніторинг, контроль доступу, оцінка ризиків.	Упроваджуються в державному та приватному секторах як доказ належного рівня кіберзахисту.
Національний	Закон України “Про основні засади забезпечення кібербезпеки України” (2017)	Визначає структуру національної системи кібербезпеки, її суб’єктів і	Координація через Держспецзв’язку, РНБО, CERT-UA, Кіберполіцію.	Створює нормативну базу національної кіберстійкості.

		принципи взаємодії.		
Національний (стратегічний)	Стратегія кібербезпеки України 2021–2025 рр.	Формує цілі державної політики у сфері кіберзахисту.	Міжнародне партнерство, публічно-приватне співробітництво, освіта.	Орієнтує розвиток законодавства відповідно до стандартів НАТО та ЄС.
Національний (кримінальний)	Кримінальний кодекс України (ст. 361–363-1)	Встановлює кримінальну відповідальність за кіберзлочини.	Розслідування Кіберполіцією, СБУ, прокуратурою.	Забезпечує правову основу притягнення до відповідальності за злочини в кіберпросторі.
Рівень регулювання	Нормативний акт / документ	Основні положення	Механізми реалізації	Значення для України

*Примітка. Складено автором за даними джерел відповідно розділу 1

Міжнародна співпраця у боротьбі з кіберзлочинністю також включає діяльність декількох організацій. Європол координує операції між країнами ЄС та партнерами, забезпечує обмін аналітичними даними та здійснює спільні слідчі дії. У 2024–2025 роках саме завдяки участі Європолу було ліквідовано кілька великих кіберзлочинних мереж, зокрема групу NoName057, яка здійснювала атаки на українські та європейські ресурси [16]. ENISA (Агентство ЄС з кібербезпеки) формує політику кіберстійкості, публікує щорічні аналітичні звіти про тенденції в кіберзлочинності та розробляє методичні рекомендації для урядів і приватних компаній [13].

Україна активно співпрацює з ENISA, обмінюється даними про загрози та бере участь у спільних тренінгах і симуляційних навчаннях. Окремим напрямком є співпраця в рамках НАТО, зокрема через Центр передового досвіду в галузі кіберзахисту (CCDCOE) в Таллінні, де Україна бере участь як партнер. Це дозволяє їй брати участь у міжнародних навчаннях, таких як Locked Shields, та спільних дослідженнях у галузі кіберзахисту [14;40].

Україна активно інтегрує міжнародні стандарти у свою правову систему. Основним нормативним актом є Закон України «Про основні засади забезпечення

кібербезпеки України» (2017) [26]. Цей документ визначає структуру національної системи кібербезпеки, її суб'єктів, повноваення державних органів, принципи співпраці між державним і приватним секторами, а також порядок реагування на кіберінциденти. Особливу роль у системі відіграє CERT-UA – урядова команда реагування на надзвичайні комп'ютерні події, яка координує виявлення та нейтралізацію кіберзагроз [11].

Кримінально-правовий аспект боротьби з кіберзлочинністю закріплений у Кримінальному кодексі України, розділ XVI «Злочини у сфері використання електронних обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж». До цієї категорії належать злочини, зазначені в статтях 361–363-1 КК України: «неправомірний доступ до комп'ютерних систем, створення або поширення шкідливого програмного забезпечення, втручання в діяльність інформаційних систем, незаконне використання електронних платіжних засобів. Таким чином, кримінальне право України гармонізоване з основними положеннями Будапештської конвенції» [22].

Стратегічним документом, що визначає політику держави в цій сфері, є Стратегія кібербезпеки України на 2021–2025 роки, затверджена указом Президента № 447/2021 [24]. У ній визначено ключові цілі: зміцнення національної кіберстійкості, нарощування кадрового потенціалу, розвиток системи захисту критичної інфраструктури, забезпечення міжнародної координації та підвищення рівня цифрової грамотності населення. У 2025 році Україна також прийняла новий закон про кібербезпеку, який передбачає гармонізацію з європейською директивою NIS2, розширює поняття критичної інформаційної інфраструктури та встановлює вимоги до сертифікації в галузі кіберзахисту [19].

Український правовий простір у сфері кібербезпеки базується на принципах міжнародного співробітництва, прозорості та взаємної сумісності. Він враховує сучасні тенденції у розвитку міжнародного права, а також потреби інтеграції з європейським та євроатлантичним простором.

Україна поступово розвиває міжнародне співробітництво в галузі кібербезпеки. Важливими партнерами є ENISA, Європол, Євроюст та НАТО

CCDCOE. Співпраця з цими структурами включає обмін технічними індикаторами компрометації, проведення спільних розслідувань, підготовку персоналу та створення єдиних стандартів реагування на інциденти. Українські фахівці беруть участь у міжнародних тренінгах та навчаннях, а також у робочих групах Ради Європи та ООН, які займаються розробкою нових стандартів кіберзаконодавства. Участь України в таких ініціативах не тільки підвищує рівень національної безпеки, але й сприяє гармонізації законодавства з європейськими та міжнародними стандартами. Це особливо важливо в контексті інтеграції України до Європейського Союзу, де питання кібербезпеки є одним із ключових критеріїв виконання умов країни-кандидата [13;14].

У сучасних умовах правове забезпечення кібербезпеки України зазнає істотних змін, що зумовлено не тільки технологічним прогресом, а й тривалою гібридною війною, в рамках якої кіберпростір став повноцінним полем бою. З початку масштабної інвазії Російської Федерації в 2022 році Україна опинилася під безпрецедентною хвилею кібератак, спрямованих на об'єкти критичної інфраструктури, органи державної влади, фінансову систему, енергетику, медіаресурси та телекомунікаційні мережі. У відповідь на це держава суттєво оновила правові механізми реагування на інциденти, координацію між державними органами та співпрацю з міжнародними партнерами.

Важливу роль у національній системі кібербезпеки відіграє Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язок), яка координує діяльність інших суб'єктів у цій сфері. Під її егідою діє CERT-UA — урядова команда, що реагує на надзвичайні комп'ютерні події, яка забезпечує виявлення, аналіз та боротьбу з кіберінцидентами. У 2023–2025 роках CERT-UA зафіксувала тисячі спроб атак, переважно фішингових кампаній, DDoS-операцій та спроб несанкціонованого доступу до державних ресурсів [11;29]. Його діяльність не обмежується лише технічною реакцією: команда бере участь у створенні нормативної бази, зокрема у розробці галузевих стандартів кіберзахисту та методичних рекомендацій для державних установ та операторів критичної інфраструктури [12].

Рада національної безпеки і оборони України (РНБО) здійснює стратегічне управління у сфері кібербезпеки, затверджує національні програми та координує міжвідомчу співпрацю. Важливою ініціативою було створення Національного координаційного центру кібербезпеки (НКЦБ) при РНБОУ, який функціонує як аналітичний та оперативний центр для збору інформації про кіберзагрози, проведення аудитів та підготовки рішень для Президента України [20].

На рівні правоохоронних органів провідну роль відіграє кіберполіція, яка розслідує злочини, зазначені в статтях 361–363-1 Кримінального кодексу України. З 2022 року діяльність кіберполіції значно розширилася – були створені спеціалізовані підрозділи для аналізу цифрових доказів, виявлення злочинних мереж, пов'язаних з фінансовим шахрайством, операціями з криптовалютами та фішингом. Практика правозастосування свідчить про те, що ефективність розслідування кіберзлочинів зростає, проте залишається низка проблем – відсутність єдиних процесуальних механізмів збору електронних доказів, недостатня кількість експертів та повільна адаптація судової системи до нових видів доказів.

У 2024–2025 роках Україна активно працює над імплементацією директиви ЄС NIS2 у національне законодавство. На основі аналізу Міністерства цифрових технологій і комунікацій та Державної служби спеціального зв'язку було розроблено проект нового закону «Про кібербезпеку», який детально описує класифікацію об'єктів критичної інформаційної інфраструктури, вводить категорії «істотних» та «важливих» операторів, встановлює вимоги до управління ризиками, обов'язок повідомляти про інциденти та встановлює адміністративну відповідальність за невиконання цих обов'язків [19;18]. Одночасно триває адаптація українських стандартів до європейських – насамперед на основі серії ISO/IEC 27000, які впроваджуються у державному секторі.

Особливістю поточної фази розвитку правового поля є поєднання принципів національної кіберстійкості та колективної безпеки, що передбачає активну участь України в європейських та євроатлантичних механізмах. Україна бере участь у програмі EU Cyber Solidarity Act (2024), яка спрямована на створення

європейського механізму взаємодопомоги у разі масштабних кібератак. Крім того, в рамках NATO Cyber Defence Pledge проводиться навчання українських фахівців у галузі стратегічного планування, кібердипломатії та правової реакції на кіберінциденти.

Вагомим внеском у підвищення кіберстійкості є розвиток державно-приватного партнерства, яке закріплено в Стратегії кібербезпеки України на 2021–2025 роки [24]. Уряд стимулює співпрацю державних структур з провідними IT-компаніями, банківським сектором та телекомунікаційними операторами. Таке партнерство дозволяє швидко обмінюватися технічними показниками компрометації, координувати дії під час атак та підвищувати готовність до реагування. Водночас на рівні правозастосування залишається необхідність створити єдиний механізм сертифікації фахівців у галузі кіберзахисту, який би відповідав міжнародним стандартам ENISA [13].

В умовах воєнного стану важливе значення набули правові аспекти забезпечення кіберзахисту, які знаходяться на межі військового та цивільного права. На практиці це проявляється у посиленій координації між Збройними силами України, Службою безпеки України, Державною спеціальним службою та партнерами НАТО. Кібер сили Російської Федерації стали однією з головних загроз, тому українська державна адміністрація активно вдосконалює механізми оперативного реагування. Зокрема, у 2024 році було впроваджено систему багаторівневого моніторингу, яка дозволяє ідентифікувати джерела атак у режимі реального часу та автоматично обмежувати доступ до уражених ресурсів [38].

Зміни в законодавстві також стосуються вдосконалення процесуальних механізмів збору та використання електронних доказів. Зміни до кримінального кодексу, розроблені спільно з Міністерством юстиції, визначають статус цифрових доказів, порядок їх отримання, зберігання та перевірки їх автентичності. Це повинно підвищити ефективність розслідування кіберзлочинів та забезпечити відповідність міжнародним стандартам електронного правосуддя.

Ключовим напрямком розвитку є також формування національної культури кібербезпеки. Держава приділяє увагу освітнім ініціативам: у 2024 році було

запроваджено державну програму підготовки кадрів у сфері кіберзахисту у вищих навчальних закладах, а також серію навчальних курсів для державних службовців [39].

Зростає роль громадських організацій та підприємств у популяризації базових знань про цифрову безпеку серед населення. Таким чином, правова база кібербезпеки України продовжує розвиватися відповідно до міжнародних стандартів. Україна не тільки адаптує європейські стандарти, але й створює власну модель кіберстійкості, яка враховує умови воєнного стану, високий рівень гібридних загроз та необхідність інтеграції в спільний безпековий простір ЄС і НАТО. Цей процес є складним і багаторівневим, але саме він визначає основу сучасної системи правового забезпечення кіберзахисту держави.

Я впевнений, що однією з головних проблем сучасної протидії кіберзлочинності полягає у швидкому розвитку технологій, за яким не встигає правове регулювання. Також важливо зазначити те, що суттєвою перешкодою залишається дефіцит кадрів, недостатня координація між державними структурами та обмежене фінансування. На мою думку, важливою умовою підвищення ефективності системи кіберзахисту є розвиток міжнародного партнерства, спільні розслідування та обмін даними між державами. Оскільки, лише поєднання правових, технічних і освітніх заходів дозволить реально зменшити вплив кіберзлочинності на суспільство [15].

РОЗДІЛ 2
СУЧАСНИЙ СТАН КІБЕРЗАГРОЗ І МЕХАНІЗМИ ПРОТИДІЇ

2.1. Стан, розвиток і класифікація сучасних кіберзагроз

Здебільшого, розвиток цифрових технологій та масове впровадження хмарних сервісів, постійна зростаюча роль мобільних та віддалених робочих середовищ, а також військовий конфлікт/вторгнення, в якому перебуває Україна з 2014 року і особливо з 2022 року, призвели до відчутної зміни характеру кіберзагроз та кіберзлочинності. Якщо раніше переважали масові та автоматизовані атаки, які мали переважно фінансову мотивацію, то сьогодні вже більше починають поширюватись цілеспрямовані складні операції, за якими часто стоять організовані групи кіберзлочинців або навіть державні структури [11].

На мою думку, для України це має принципове та важливе значення, оскільки кіберпростір фактично став та стає одним із вимірів гібридної війни проти нашої держави, як правило: кібератаки супроводжуються інформаційними кампаніями, психологічними операціями, спробами вплинути на енергетичну або фінансову систему, а також постійними та небезпечними діями, спрямованими на підрив довіри громадянського суспільств або органів державної влади.

І тому важливо зазначити, що поява сучасних кіберзагроз відбувалася поступово. На ранніх, початкових етапах в 2000-них роках більшість кібер-атак були спрямовані на зловживання вразливістю операційних систем, веб-серверів або електронної пошти і мала, здебільшого, примітивний характер. Однак, поступова поява анонімних інфраструктур, криптовалют та «темних» ринків створила повноцінну кримінальну економіку в кіберпросторі. Вже з середини 2010-х років відбувся якісний перехід до моделі «кіберзлочинності як послуги» (Cybercrime-as-a-Service), коли інструменти для атак – так звані, фішингові набори, шкідливі програми, ботнети, інфраструктури для DDoS – почали відкрито продавати або здавати в оренду. Це почало значно знижувати поріг входу в

злочинну діяльність і дозволило менш технічно підготовленим злочинцям застосовувати атаки більш високого рівня.

Війна в Україні стала ще одним з головних каталізаторів складності загроз. Вже після 24 лютого 2022 року CERT-UA, Держспецзв'язок та інші державні органи почали фіксувати систематичне збільшення застосування кібератак одночасно з ракетними ударами та інформаційними кампаніями проти України. Відбулося розширення атак на урядові веб-ресурси, реєстри, банківські послуги, телекомунікаційні та енергетичні компанії [11].

І тому, більша частина атак мала виключно деструктивну мету, мету виведення з ладу інформаційних систем, шифрування або знищення даних, унеможливлення доступу до державних послуг. А інша частина на меті мала розвідувальний характер – зловмисники намагалися отримати конфіденційну інформацію про переміщення, розміщення військ, діяльність органів влади, внутрішню комунікацію [20].

По-перше, у сучасній науковій літературі переважає функціональна класифікація кіберзагроз, заснована на їхній меті, об'єкті атаки та використаних технологіях. По-друге, виділяються й загрози, які як правило, спрямовані проти конфіденційності, цілісності та доступності інформації та інформаційних систем (CIA-тріада). До цієї групи належать також несанкціонований доступ, перехоплення трафіку, втручання в роботу серверів, шкідливе кодування або шифрування даних.

А іншу групу складають кіберзагрози економічного характеру – фішинг, шахрайські операції, крадіжка облікових даних, підробка платіжних даних, атаки типу BEC (Business Email Compromise), які спрямовані на отримання прямої фінансової вигоди. Окремий шар складають деструктивні та політично мотивовані загрози – атаки типу DDoS, операції «wiper», цільові кампанії APT, головною метою яких є не прибуток, а вплив, деморалізація та порушення функціонування інфраструктури або збір розвідувальних даних [13].

Наразі, до одним з найнебезпечніших для України та європейського кіберпростору загалом належать такі типи загроз, як:

– атаки програм-вимагачів, які часто поєднують шифрування даних з їх крадіжкою та подальшим вимаганням;

– цілеспрямований фішинг (spear phishing), який використовується як перший крок у складних кібер-атаках;

– DDoS-атаки з політичною мотивацією, здебільше, спрямовані на державні бази, банки та ЗМІ;

– операції APT, які тривають довго, вони малопомітні і часто спрямовані на державні органи, оборонний і промисловий комплекс, енергетику, критичну інфраструктуру, та транспорт;

– атаки на ланцюги поставок (supply-chain attacks), коли компрометується не кінцева жертва, а її постачальник або постачальник програмного забезпечення [13;32].

Характерно, що за даними публічних звітів українських органів (CERT-UA, НКЦК) за 2023–2025 роки більшість інцидентів починалася саме з використанням людського фактору, створенням фішингового електронного листа та відкриття шкідливого вкладення, використання зламаних або повторно використаного паролю/паролей [11;20]. На мою думку, це ще раз підтверджує, що еволюція кіберзлочинності та загроз відбувається не тільки на технічному, але й на соціальному рівні, зловмисники чудово пристосовуються до поведінки користувачів і систем безпеки, постійно поєднуючи технічні та психологічні методи для досягання злочинних цілей.

У сучасному цифровому середовищі кіберзагрози дедалі стають складнішими, масштабнішими та скоординованими. Розвиток кіберзагроз пов'язаний не тільки з технологічним прогресом, але й із постійними змінами глобально соціально-політичного устрою. Більшість сучасних кібер загроз мають багатовимірний характер і поєднують технічні, економічні, інформаційно-психологічні та військово-політичні аспекти. Їхньою головною метою є порушення стабільності держав, пригнічення та дестабілізація економічних процесів, втручання у функціонування критичної інфраструктури [13; 15].

За даними ENISA Threat Landscape 2023–2024, найактивнішими типами атак досі залишаються фішинг-кампанії, тобто, операції з застосуванням програм-вимагачів, хакерські атаки на корпоративні акаунти, DDoS-атаки та складні багатовекторні операції, що часто поєднують кілька методів впливу [13]. Україна є однією з найбільш атакованих держав Європи. Цікаво те, що CERT-UA у своїх аналітичних звітах за 2023–2025 роки зазначає, що більшість атак мають гібридний характер і спрямовані на державний сектор, енергетику та телекомунікації [11].

Як показує інформація, головною, так званою особливістю українського кіберпростору є його роль як «поля бою» в сучасній гібридній війні. За оцінками Національного координаційного центру з питань кібербезпеки при РНБО України, у 2024 році кількість спроб вторгнення в критичні системи зросла на 25 %, причому, більшість з них мали політичну мотивацію [20]. Аналізування структури атак вказує те, що найбільшу загрозу становлять цільові APT-кампанії, які здійснюють державні або наближені до них хакерські угруповання [20].

І тому ми впевнені, що класифікація сучасних кіберзагроз включає в себе, як технічні (несанкціонований доступ, хакерство, шкідливе програмне забезпечення), так і поведінкові (соціальна інженерія, фішинг, шахрайство) компоненти. ENISA розрізняє три основні рівні загроз:

1. Масові автоматизовані атаки, спрямовані на широке коло користувачів.
2. Цільові атаки проти конкретних організацій.
3. Гібридні кібер-операції, що поєднують технічні дії з інформаційним впливом[13].

Враховуючи всю інформацію, яку виклав вище, я вважаю, що у контексті України необхідно приділити особливу увагу кібератакам на енергетичні системи. Вже 2024 році CERT-UA зафіксувала понад 250 спроб втручання в інформаційні мережі енергетичних компаній, що свідчить про зростання частки атак на критичну інфраструктуру [11]. І тому, за даними Міністерства цифрової трансформації, одним з основних напрямків державної політики є розвиток кіберстійкості таких об'єктів [18].

На мою думку, сучасні кіберзагрози мають системний і стратегічний характер, адже вони спрямовані не лише на злам систем, а й на підрив довіри до державних інституцій. Україна сьогодні виступає як своєрідний «щит Європи» у сфері кібероборони, тому її досвід є унікальним. Я вважаю, що ефективна класифікація кіберзагроз повинна враховувати не лише технічну природу атак, а й їх геополітичну мотивацію. Оскільки, головним пріоритетом має стати створення системи прогнозування й аналітики кіберризиків, заснованої на постійному моніторингу та міжнародному співробітництві [11; 13; 15].

2.2. Методи виявлення, захисту та роль людського фактору

Так, у відповідь на постійно зростаючу складність кібернетичних загроз за останнє десятиліття було створено багаторівневу модель кібернетичного захисту, яка передбачає одночасне застосування превентивних, детективних заходів протидії. Однак, жоден з рівнів сам по собі не може забезпечити повний захист, і тому більшість сучасних організацій, державних і приватних – впроваджують комплексні та ефективні системи безпеки, які поєднують засоби контролю на рівні мережі, пристроїв та додаткових послуг для користувачів.

Важливим є те, що одним з основних інструментів виявлення атак залишаються системи IDS/IPS (Intrusion Detection/Prevention Systems). Ці системи мають на меті виконання безперервного аналізу мережевого трафіку, вони порівнюють його з відомими сигнатурами атак та поведінковими моделями і в разі виявлення підозрілої активності ідентифікують їх та сповіщають адміністратора (IDS) або блокують трафік (IPS). Головними, рекомендаціями міжнародних та національних органів (зокрема NIST SP 800-53 та інструкції Державної спеціальної комунікації) вважають ці системи обов'язковим елементом базового захисту корпоративної мережі, оскільки вони часто дозволяють фіксувати як масові інтернет-атаки, так і внутрішні несанкціоновані дії [35].

Необхідно також додати те, що подальшим, якісним розвитком цієї концепції стали рішення класу EDR (Endpoint Detection and Response). Бо на відміну від

мережевих систем, EDR фокусується на поведінці конкретних технічних пристроїв, робочих станцій, ноутбуків, серверів, віртуальних машин. Оскільки, ці системи збирають телеметрію з кінцевих точок (запущені процеси, файли, мережеві підключення), та аналізують їх в режимі реального часу, виявляючи навіть малопомітні відхилення, як правило, характерні для початкових етапів складних атак (наприклад, APT). Я вважаю, що це є особливо важливо для України, де значна кількість фішингових кампаній спрямовані саме на робочі станції державних службовців і військових. Використання EDR дозволяє виявляти атаку, перш ніж вона вийде за межі одного комп'ютера [12].

Вже іншим основним елементом сучасної системи кіберзахисту є SIEM (Security Information and Event Management). Ці системи збирають журнали подій із серверів, мережевих пристроїв, засобів безпеки, робочих станцій, хмарних сервісів і вже на основі кореляції цих даних виявляють складні інциденти, які неможливо було би зафіксувати на одному рівні. І тому, для державних органів та об'єктів критичної інфраструктури саме системи SIEM почали ставати центром ситуаційної обізнаності: вони дозволяють бачити загальну картину ситуації, і в подальшому реагувати не на кожну подію окремо, а на інцидент як сукупність пов'язаних між собою подій. Всі українські державні органи та великі компанії в останні роки почали активно переходити на модель побудови SOC (Security Operations Centre) на базі SIEM, що відповідає сучасним підходам кібербезпеки ЄС та НАТО [12].

Визначною тенденцією в 2023–2025 роках є активне застосування штучного інтелекту та машинного навчання в системах виявлення загроз. Я вважаю та абсолютно впевнений, що причиною цього є те, що сучасні атаки часто не мають чіткої сигнатури, вони часто є унікальними та поєднують кілька технік. Як правило, алгоритми ML здатні створювати поведінкові профілі користувачів і пристрої та виявляти аномалії, наприклад, раптовий доступ до незвичайних джерел, незвичні та нетипові обсяги завантажених даних, підозрілі спроби аутентифікації. І тому, я розумію, що для українського контексту це дійсно важливо також тому, що значна

частина кібер-атак здійснюється нерезидентними групами, тому їх класичні сигнатури виявляються гірше [37].

Практично вся більшість міжнародних звітів, на які я ссилався у даній роботі (ENISA Threat Landscape, IBM Security, Verizon DBIR), підкреслюють, що людський фактор досі залишається однією з найслабших ланок в будь-якій системі кібербезпеки. Переважна більшість успішних атак починається з того, що співробітник відкриває шкідливий файл та переходить за фішинговим посиланням, в подальшому вводить свої облікові дані у фальшивій формі або використовує один і той самий пароль у декількох сервісах. Тому часто більшість сучасних систем захисту обов'язково включають організаційні та освітні заходи [13;17;30].

Я вважаю, що однією з найефективніших форм профілактики є регулярне/постійне навчання персоналу з елементами практичних вправ. Оскільки, такі програми не повинні обмежуватися одноразовим інструктажем чи лекцією, вони повинні бути регулярними, щоквартальними або принаймні щорічними. Вони повинні включати такі теми, як розпізнавання фішингу, здійснення безпечної роботи з електронною поштою, використання багатофакторної автентифікації та правилами роботи з хмарними сервісами та захистом мобільних пристроїв. Важливо відмітити, що досвід, на який посилаються українські державні органи та провідні постачальники (CERT-UA, KnowBe4), вказує те, що після впровадження системних та ефективних навчальних програм якісно зменшить кількість успішних фішингових на 60–90 відсотків [11;30].

І тому, однією з важливих складових є застосування симуляційних атак та тестування їх на проникнення. Цінність цього методу полягає в тому, що він показує реальний стан безпеки, а не формальний. Бо, коли в організації проводиться контрольована фішингова розсилка, яка потім аналізується, та які співробітники перейшли за посиланням і ввели пароль, дозволяє дуже точно оцінити рівень ризику і скоригувати навчання. Вже сьогодні, такий підхід починає використовуватись в державному секторі України – за участю CERT-UA, Держспецзв'язку та іноземних партнерів (ENISA, NATO CCDCOE) [11;13;14].

Але, не менш важливим напрямком є розроблення та впровадження ефективних та сучасних внутрішніх політик інформаційної безпеки. Як правило, політика встановлює правила доступу, порядки обробки та зберігання даних, використання зовнішніх носіїв, порядок підключення віддалених співробітників, вимоги до паролів, умови реагування на інциденти, тощо. І тому, якщо політика відсутня або не оновлюється, навіть дорогі технічні засоби не гарантують безпеки, оскільки, співробітники будуть діяти на власний розсуд. Важливо те, що Українські органи влади (Мінцифра, Держспецзв'язок) наразі розробляють типові політики для органів державної влади з метою уніфікації підходів та підвищення ефективності загального рівня кіберстійкості [18;12].

Розвиток сучасних цифрових технологій зумовив необхідність створення комплексних систем для боротьби з кіберзагрозами. Виявлення та нейтралізація інцидентів сьогодні будується на багаторівневій архітектурі захисту, яка часто поєднує технічні засоби, аналітичні методи та людський контроль. Сучасні підходи які базуються на інтеграції технологій IDS/IPS, EDR, SIEM та штучного інтелекту, дозволяють виявляти атаки в режимі реального часу [35; 12].

І тому, системи IDS/IPS (Intrusion Detection and Prevention Systems) дозволяють моніторити мережевий трафік і виявляти нетипові події. Згідно з рекомендаціями NIST [35], їх ефективність значно підвищується в поєднанні з централізованими системами обробки даних – SIEM, які збирають і корелюють протоколи подій з усіх вузлів мережі [12]. Такі технології активно впроваджуються в Україні, зокрема в рамках проектів ДССЗЗІ та CERT-UA [12; 11].

Також одним з важливих напрямків розвитку є системи EDR (Endpoint Detection and Response), вони аналізують поведінку користувачів та пристроїв. Вони дозволяють виявляти ознаки інфікування на ранніх стадіях, що є особливо важливим для запобігання атакам типу ransomware [17]. Тобто, використання алгоритмів машинного навчання дозволяє значно ефективніше визначати та виявляти нові загрози ще до їх активної фази [37].

Особливу роль також відіграє людський фактор, який як я вказував раніше, залишається найвразливішою ланкою системи кіберзахисту. За даними IBM

Security [17], приблизно 16 % інцидентів спричинені ненавмисними діями співробітників. ENISA повідомляє, що понад 80 % успішних фішингових атак починаються з елементарного порушення правил кібергігієни [30]. І тому провідні організації впроваджують регулярні тренінги з безпеки, симуляційні фішингові кампанії та внутрішні політики кіберосвіти [30].

На мою думку, до найбільш ефективних та найкращих практик в Україні належать програми DSSZZI та освітні ініціативи CERT-UA, які в 2024 році охопили понад 250 державних органів. У відповідності до їх звітів, рівень успішного виявлення тестових атак після тренінгів зріс на 60 % [11]. У рамках співпраці з ENISA та NATO CCDCOE також організовуються національні кібертренінги, які дають змогу перевіряти готовність державних структур до кризових ситуацій [13;14].

Таким чином, сучасним підходом до виявлення та захисту від кіберзагроз у державному та приватному секторі України базується на принципах поєднання технічних рішень (IDS/IPS, EDR, SIEM, AI), організаційних заходів (політики, правила, аудит) та людського компонента (навчання, симуляційні атаки, контроль доступу). Я впевнений, що тільки така комбінація дозволяє протистояти багатогранним атакам, які сьогодні здійснюються проти українських інституцій і не тільки.

Я переконаний, що у сучасних умовах боротьба з кіберзагрозами — це насамперед боротьба за компетентність і свідомість користувачів. Жодна технологія не може повністю компенсувати людські помилки, тому підготовка кадрів має бути постійною. На мою думку, навчання, імітаційні атаки та розвиток корпоративної культури безпеки — це не просто допоміжні інструменти, а основа ефективного кіберзахисту. Отже, я вважаю, що майбутнє кібербезпеки України залежить від поєднання інноваційних технологій і високої цифрової культури працівників [12; 17; 37; 30].

2.3. Організаційно-правові механізми та міжнародна співпраця у сфері кібербезпеки

Отже, як я з’ясував, жодна, навіть найдосконаліша технічна система захисту не буде ефективною без відповідної правової та інституційної бази. За останні 7–8 років в Україні було створено потужну та цілісну нормативно-правову базу в галузі кібербезпеки, яка поступово наближається до європейських стандартів. Головною оновою, тобто, фундаментом, наріжним каменем, є Закон України «Про основні засади забезпечення кібербезпеки України» від 2017 року, який визначив суб'єктів національної системи кібербезпеки (Рада національної безпеки і оборони, Державна спеціальна служба, Служба безпеки, Міністерство оборони, Національна поліція, НБУ тощо), та принципи їхньої співпраці, а також поняття об'єктів критичної інформаційної інфраструктури. На мою думку, саме цей закон заклав основи для створення урядової команди CERT-UA та визначив її функції як національного координатора управління інцидентами, кіберзагрозами [26;11].

Другим базовим документом стала Стратегія кібербезпеки України на 2021–2025 роки, затверджена указом президента України. Стратегія визначила пріоритети державної політики, такі як: підвищення стійкості державних інформаційних ресурсів, захист критичної інфраструктури, розвиток людського потенціалу, зміцнення науково-освітньої складової, і, що дуже важливо, розширення міжнародного співробітництва з ЄС і НАТО. Ця стратегія передбачає гармонізацію українського законодавства з директивами ЄС у сфері кібербезпеки, зокрема з NIS2. Це стало дійсно особливо актуальним у 2024–2025 роках [24].

Вже в 2025 році, як ми зазначали, була прийнята нова редакція закону про кібербезпеку, яка, по суті, переносить ключові положення NIS2 у національне середовище, починають вводитись обов'язкові повідомлення про інциденти, детально конкретизується перелік секторів і компаній, які належать до критичних і важливих, посилюється відповідальність за порушення цих вимог, розширюються повноваження наглядових органів. А це означає, що Україна переходить від декларативної моделі кібербезпеки до моделі регулятивної відповідальності, коли

не тільки держава, але й підприємства повинні та зобов'язані підтримувати належний рівень захисту кіберзахисту [19].

Важливо зазначити, що однією з головних рис української моделі є тісна міжвідомча координація, яку забезпечує РНБО через Національний координаційний центр кібербезпеки. Цей орган збирає повну та достовірну інформацію про загрози, організовує міжгалузеві тренінги, координує реагування у разі масштабних інцидентів (наприклад, сучасних DDoS-атак на банківський сектор та урядові портали) та забезпечує комунікацію з міжнародними партнерами. Саме через НККБ відбувається значна частина обміну інформацією з ЄС, НАТО та країнами-партнерами [20].

Особливим значенням є міжнародне співробітництво. Оскільки, Україна є членом Будапештської конвенції про кіберзлочинність і бере активну участь в її оновленні (другий додатковий протокол від 2022 року). А це у свою чергу відкриває доступ до механізмів швидкого транскордонного отримання електронних доказів, що на мою думку, є надзвичайно важливим у ситуації, коли значна частина злочинної інфраструктури знаходиться за межами України [7]. Постійна Співпраця з Європолом та Євроюстом дозволяє залучити європейські правоохоронні органи до розслідування складних справ, що як правило, мають багатонаціональний характер [16].

Також треба зазначити, що важливою платформою є також ENISA – Агентство ЄС з кібербезпеки, яке не тільки публікує щорічні огляди кіберзагроз, але й організовує навчання, розробляє сучасні рекомендації щодо захисту критичної інфраструктури та перевіряє готовність держав до кібератак, які є актуальними у наш час [13]. Доречі, Україна, яка має статус партнерської держави ЄС та країни-кандидата, бере постійну та активну участь у цих процесах, що дозволяє їй працювати за європейськими стандартами ще до офіційного членства [13].

Правова система України в сфері кібербезпеки ґрунтується на поєднанні національних правових норм та міжнародних зобов'язань. Основою є Закон України «Про основні засади забезпечення кібербезпеки України» [26], який

визначає правові рамки діяльності суб'єктів кібербезпеки, механізми координації між органами державної влади, а також принципи співпраці з приватним сектором та міжнародними партнерами.

Важливо приділити увагу Указу Президента України № 447/2021 «Про стратегію кібербезпеки України» [24], який визначає цілі державної політики до 2025 року, який має на меті: створення єдиного простору кіберзахисту, гармонізацію законодавства з директивою ЄС NIS2 [33], розвиток національної системи моніторингу та підготовка фахівців. Вже у 2024 році Міністерство цифрової трансформації представило проект нового закону «Про кібербезпеку», спрямованого на гармонізацію українських норм з європейськими стандартами [19; 18].

На рівні міжнародного співробітництва ключову роль відіграє участь України в Будапештській конвенції [7; 21; 27], співпраця з ENISA [13] та NATO CCDCOE [14; 40], а також активна взаємодія з Євро полом та CERT-EU. В рамках цієї співпраці постійно проводяться спільні тренінги, обмін технічними індикаторами компрометації, координація під час міжнародних розслідувань кіберзлочинів [16; 3].

Державна служба спеціального зв'язку та захисту інформації (DSSZZI) є головним координатором реалізації політики кіберзахисту, а Національний координаційний центр кібербезпеки при РНБО є аналітичним центром, що реагує на інциденти. CERT-UA забезпечує оперативне моніторингу та реагування на кібернетичні атаки, надає державним і приватним структурам аналітичні звіти, попередження та рекомендації [11; 12].

Міжнародні партнери активно підтримують Україну в розвитку кібернетичної безпеки. Так, в рамках ENISA та НАТО CCDCOE у 2024–2025 роках було проведено серію тренінгів, під час яких українські фахівці відпрацьовували сценарії кібернетичних атак на критичну інфраструктуру. Я вважаю, що такі ініціативи якісно підвищують рівень інтеграції України в європейську систему кібернетичної безпеки [14]. Я впевнено можу сказати те, що українська модель кібербезпеки поступово трансформується, відповідно до європейських стандартів.

А поєднання законодавчих реформ, інституційного зміцнення та міжнародної координації є головним ключем до підвищення кіберстійкості нашої держави [6; 26; 28].

Важливою складовою є співпраця з НАТО, насамперед через Центр передового досвіду в галузі кіберзахисту (CCDCOE) в Таллінні та участь у навчаннях типу Locked Shields. Ці навчання імітують багатовимірні атаки на державні органи, ЗМІ, енергетику, телекомунікації та дають змогу відпрацювати технічні, правові та комунікаційні аспекти реагування. Для України це є дійсно критично важливим, оскільки реальні інциденти у 2022–2025 роках показали, що атака рідко є лише технічною – вона завжди супроводжується інформаційною або психологічною підтримкою, спробою викликати паніку або виправдати дії агресора [34; 40].

Організаційні та правові механізми також включають публічно-приватне партнерство. Держава не може самостійно захистити всі ресурси, особливо з огляду на те, що значна частина критичної інфраструктури (енергетика, телекомунікації, транспорт, банки) перебуває у приватній власності. Тому в Україні впроваджується модель обов'язкового обміну інформацією про інциденти, а приватні компанії інформують державні органи про атаки, що д в свою чергу надає індикатори компрометації, аналізи, рекомендації, а іноді й допомогу у відновленні. Така модель успішно працює в ЄС і США, і її перенесення в українські реалії є логічним [18; 5].

Підсумовуючи все вище викладене, можна констатувати, що українська система боротьби з кіберзагрозами вже сьогодні не є суто реактивною – вона поступово стає проактивною, тобто здатною не тільки фіксувати інциденти, а й запобігати їм завдяки регуляторним вимогам, спільній освіті, централізованому моніторингу, постійній співпраці з міжнародними організаціями та постійному підвищенню обізнаності користувачів [30].

На мою думку, саме системний підхід до організації кібербезпеки робить державу стійкою до зовнішніх загроз. Україна поступово формує ефективну правову базу, яка поєднує національні інтереси з міжнародними зобов’язаннями.

Я вважаю, що співпраця з ENISA, НАТО CCDCOE та Європолом відкриває нові можливості для обміну досвідом і технологіями. Це зумовить подальше вдосконалення нормативного регулювання, розбудову національної інфраструктури кіберзахисту, а активна участь у міжнародних ініціативах є ключовим шляхом забезпечення кіберстійкості України [13; 26; 28].

РОЗДІЛ 3
ПРАКТИЧНІ АСПЕКТИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ КІБЕРБЕЗПЕКИ УКРАЇНИ

3.1. Аналіз реального кейсу: фішингова кампанія проти державної установи

Фішингові кампанії проти органів державної влади України в 2024–2025 роках набули систематичного характеру та добре спланованих операцій, що поєднують технічні та соціально-інженерні методи. У відповідності з офіційними попередженнями CERT-UA та Національного координаційного центру з кібербезпеки при РНБО України, більшість складних інцидентів у державному секторі починаються саме з фішингового електронного листа, який імітував службове повідомлення або оновлення політики доступу [11; 20; 29].

Як правило, першим кроком такої кампанії є дослідження відкритих джерел, зловмисники починають збирати інформацію про співробітників установи з офіційного веб-сайту, публічних закупівель, соціальних мереж, профільних спільнот. А це в свою чергу, передусім, дозволяє їм персоналізувати електронні листи, тобто, звертатися до адресатів по імені, згадувати реальні проекти або навіть внутрішні відділи. Саме персоналізація значно збільшує відсоток відкриттів і переходів за посиланнями [31; 32].

Так, ENISA у своєму звіті за 2025 рік зазначає, що в державному секторі найкраще працюють листи з такими темами, як «оновлення засобів захисту», «перевірка облікового запису», «воєнний стан/робота в умовах обмежень», «підтвердження доступу до державних реєстрів» [31; 30]. І тому, українські установи часто стають мішенню саме таких листів, оскільки вони маскуються як реальний службовий контекст.

Листи надсилаються або з підроблених доменів, які дуже схожі на gov.ua, або з уже скомпрометованих поштових скриньок інших державних органів. У такому

випадку для адресата це виглядає як звичайна міжвідомча кореспонденція, і ймовірність того, що він перейде за посиланням, значно зростає [11; 29].

Перехід за посиланням веде на сторінку, яка імітує вхід в службову пошту або внутрішній портал. А вже там користувач вводить свої облікові дані, які негайно надсилаються зловмиснику. Потім зловмисники намагаються закріпити свою позицію у внутрішній мережі: створюють правила електронної пошти для приховування своєї діяльності, аналізують внутрішні каталоги та шукають інші відділи, які можна атакувати вже з «легітимного» облікового запису. Як зазначає CERT-UA за 2025 рік прямо вказано, що такі фішингові кампанії далі використовувалися як підготовчий етап до кібершпигунства або деструктивних дій проти державних ресурсів [29; 11].

Особливо небезпечними є багатоканальні атаки, коли електронний лист дублюється в месенджері або телефоні: «ми щойно надіслали вам інструкції, будь ласка, виконайте їх». Це вже не просто фішинг, а елемент психологічного тиску. Саме такі комбіновані сценарії були зафіксовані в 2024–2025 роках європейськими та українськими кіберцентрами [32; 37].

На мій погляд, фішинг проти українських державних органів сьогодні не є незначною загрозою, а першим ланцюжком складних операцій, які можуть закінчитися викраденням документів, доступом до реєстрів або навіть шифруванням окремих сегментів мережі. Тому на такий лист має реагувати не тільки IT-відділ установи, але й національні суб'єкти кібербезпеки, з подальшим обміном індикаторами компрометації між усіма органами. [31; 11; 12; 20; 29; 37]

3.2. Розробка моделі виявлення шкідливих листів та оцінка ефективності навчання персоналу

Як правило, однієї лише технічної фільтрації недостатньо, особливо тоді, коли зловмисники використовують україномовні, стилістично коректні листи й компрометовані державні домени. Тому для українського держсектору доцільно впроваджувати багаторівневу модель, у якій поєднані:

- периметрові засоби (шлюз, фільтри, правила прийому пошти);
- засоби контролю кінцевих пристроїв;
- системне навчання персоналу;
- централізований збір і аналіз інцидентів.

На периметрі має діяти єдиний підхід до всіх та пов'язаних доменів: SPF, DKIM, DMARC та обов'язкове нотування пошти, маркування зовнішніх листів, автоматичне сканування вкладень у «пісочниці». Так, ENISA у рекомендаціях для публічного сектору прямо зазначає, що різнорідність поштових політик у межах однієї держави створює прогалини, через які проходять цілеспрямовані атаки [31; 32]. А це означає, що в українських реаліях виникає потреба у централізованому державному поштовому шлюзі або принаймні в типовій політиці, яку затверджує Держспецзв'язку [12].

Також, важливим елементом є контроль поведінки користувачів. Навіть якщо лист пройшов фільтр, система має побачити, що працівник відкрив незвичне вкладення, перейшов на невідомий домен або спробував ввести пароль на зовнішньому ресурсі. Для цього застосовують EDR та UEBA-рішення, які постійно вчаться на звичній поведінці працівника і сигналізують про аномалії. А це особливо цінно проти нових фішингових кампаній, для яких ще немає сигнатур [12; 35].

На нашу думку, чесно кажучи, вирішальний елементом є навчання персоналу. Як говорить досвід SANS та NIST щодо органів влади показує: якщо немає регулярних (раз на квартал) фішингових симуляцій, рівень кліків тримається

на рівні 25–35 %, і цього достатньо зловмисникам, щоб кожна масова розсилка давала кілька робочих обліків [35; 30]. Якщо ж симуляції робити регулярно й одразу навчати та пояснять тим, хто помилився, показник можна опустити до 5–8 % навіть у великих колективах. А це важливо, щоб сценарії більшості симульованих атак в українському контексті, відповідали актуальності , тобто, відбувалися перевірки в умовах воєнного стану, у взаємодії з CERT-UA, внаслідок цього навчання буде максимально ефективним [32; 35].

Останній елементом є — централізований аналіз. Тобто державний SOC або НКЦК мають бачити, які типи фішингу зараз заходять по органах, та з яких доменів ідуть атаки, які листи проходять фільтри. Це дало змогу би швидко сформувати технічні індикатори та розіслати їх усім відомствам, а це те, що вже практикується в Україні з 2022 року, але потребує більшої автоматизації та модернізації [20; 29].

Ми вважаємо, що для України вкрай важливо та необхідно зосередити увагу на інвестиції в цифрові технології та підвищення кваліфікації співробітників. В свою чергу, в такій зв’язці ефективність кібербезпеки значно зросте. Оскільки, неефективність нівелює всю роботу кіберзахисників. [12; 29; 31; 32; 34; 35; 46; 48]

3.3. Пріоритети розвитку та практичні рекомендації щодо вдосконалення кібербезпеки України

Події 2022–2025 років показали нам, що українська модель кіберзахисту працює, але вона все ще є неоднорідною, є відомства, що мають власні SOC, а є органи місцевого самоврядування, де досі немає ані MFA, ані протоколювання подій. Тому, я вважаю, що подальший розвиток повинен бути спрямований на уніфікацію, централізацію та глибшу інтеграцію з європейським кіберпростором [20; 5; 28].

Основні напрями розвитку системи кібербезпеки України наведено у таблиці

Таблиця 3.1 Пріоритетні напрямки вдосконалення системи кібербезпеки України (2025-майбутнє)

№	Напрям	Ключова мета	Очікуваний

			результат
1	Гармонізація з NIS2	Адаптація законодавства до стандартів ЄС	Єдиний рівень кіберзахисту в усіх секторах
2	Основні ініціативи	Кіберосвіта для держслужбовців і населення	Підвищення культури кібергігієни
3	Державно-приватне партнерство	Координація між державою та бізнесом	Оперативне реагування на кіберінциденти
4	Національний SOC	Централізований моніторинг інцидентів	Зменшення часу реагування, підвищення стійкості
5	Міжнародна співпраця	Участь у програмах ENISA, CCDCOE, НАТО	Поглиблення інтеграції в європейський кіберпростір

*Примітка. Складено автором за даними джерел відповідно розділу 3

Дані в таблиці 3.1, вимагає створення ефективної системи кібербезпеки України і не тільки технічних рішень, а й розвитку нормативних, освітніх та інституційних компонентів. Важливо забезпечити гармонізацію законодавства з директивою NIS2, створення національного SOC для моніторингу інцидентів, а також розширення міжнародного співробітництва. Такий підхід дозволить перейти до моделі проактивного управління ризиками, зміцнити довіру громадян до цифрових послуг та підвищити стійкість держави до зовнішніх кіберзагроз [33].

Насамперед, необхідно завершити гармонізацію з директивою (ЄС) (NIS2). А це означає що, необхідно буде визначити перелік істотних та важливих суб'єктів, затвердити для них обов'язкові мінімальні вимоги, запровадити обов'язок повідомляти про інциденти та визначити санкції у разі невиконання. Адже, європейські аналітичні центри підкреслюють, що без елемента примусу частина організацій завжди буде відкладати впровадження заходів безпеки – не з поганих намірів, а через брак ресурсів або персоналу [33].

Особливо важливим напрямком є посилення моніторингу на національному рівні. CCDCOE у своїх публікаціях про Україну прямо пише, що ми маємо багато технічних даних про атаки, але вони розрізнені між окремими відомствами,

і держава потребує єдиної стратегії в режимі реального часу [28]. Тобто, це означає створення або розширення національного SOC, куди будуть надсилатися протоколи подій, дані про фішингові кампанії, IOC та результати модельованих атак.

Також необхідна формалізація державно-приватного партнерства. Значна частина критичної інфраструктури (телекомунікації, енергетика, транспорт) в Україні нас знаходиться в приватній власності. Тому обмін індикаторами компрометації, спільні тренінги та спільні плани реагування повинні бути описані не в меморандумах про співпрацю , а в конкретних діях [18; 5].

Приорітетом є кібернетична освіта. Тут вже йдеться не про одноразові тренінги, а про систему, я вважаю, що необхідно проводити короткий обов'язковий курс для всіх державних службовців, створювати розширені програми для IT-персоналу, здійснювати підготовку кібер юристів, без яких в подальшому часі важко буде працювати з міжнародними запитами та цифровими доказами, здійснювати підтримку університетських програм у сфері кіберзахисту. Той самий NIST у SP 800-50 прямо підкреслює, що для державних органів навчання має бути рольовим, а не «одним для всіх» [35].

І нарешті, питання стійкості. Більшість масових кібернетичних атак на телекомунікації або державні веб-сервіси в Європі в 2024–2025 роках показали, що навіть одна успішна атака може мати інформаційний ефект, який є несумісним з технічними наслідками [34]. Україна, яка перебуває у стані війни, повинна мати резервні локації, хмарні резервні копії та плани швидкого відновлення інформації.

Тому я вважаю, що Україна досягне найбільшого ефекту не шляхом придбання додаткової системи захисту, а шляхом встановлення мінімального стандарту кібербезпеки як обов'язкового для всіх, хто працює з критичною інформацією. Тим самим, ми досягнемо того, що всі інциденти будуть негайно видимими на всіх рівнях. У цьому напрямку рухаються країни ЄС, і, я впевнений, що ми досягнемо успіху при раціональній державній політиці. [20; 18; 35; 12; 5; 33; 34; 49].

ВИСНОВКИ

В процесі наукової роботи було комплексно досліджено теоретичні основи та правові механізми, сучасні загрози та практичні аспекти боротьби з комп'ютерною злочинністю в Україні. Результати роботи підтвердили те, що кіберзлочинність є одним із найсерйозніших викликів для сучасного світу, який вимагає постійної систематичної, між інституційної та міжнародної співпраці.

Аналізуючи теоретичні підходи показує, що поняття кіберзлочинності на сьогодні має багатовимірний характер. І тому, у міжнародній практиці його визначення охоплює як злочини, які спрямовані безпосередньо на комп'ютерні системи (наприклад, несанкціонований доступ, DDoS-атаки, шкідливе програмне забезпечення), так і злочини, в яких цифрові технології є інструментом для досягнення злочинної мети (онлайн-шахрайство, фішинг, кібербулінг тощо). Як правило, цей підхід закріплений у Будапештській конвенції Ради Європи від 2001 року, яка стала основним міжнародним правовим документом та головним орієнтиром у сфері кібербезпеки.

Вивчення історичного розвитку кіберзлочинності дозволило дійти висновку, що кіберзлочинність пройшла шлях від поодиноких випадків технічного втручання в 1960-1980 роках до потужного глобального явища в 21 столітті, тому, сьогодні кіберзлочинність має організований і комерційний характер, оскільки всі відомі такі моделі, як Cybercrime-as-a-Service, які функціонують, як ринок кримінальних послуг. Ми вважаємо, що особливо небезпечними стали ті кібернетичні атаки, які здійснюються під егідою державних структур або спонсорованих груп, оскільки вони поєднують сучасні технічні інновації зі стратегічними цілями.

Аналіз міжнародних та національних правових рамок вказує на те, що правове поле боротьби з кіберзлочинністю в Україні поступово гармонізується з європейськими стандартами. Закон України «Про основні засади забезпечення кібербезпеки України» (2017), Стратегія кібербезпеки (2021–2025) та проект нового закону про імплементацію директиви NIS2 складають основу, так званий базис, фундамент нормативної системи. Однак, великою проблемою залишається

питання практичної реалізації, а саме: нестача фахівців, необхідність швидкого реагування на інциденти, слабка координація між органами державної влади, тому важливим результатом дослідження є висновок, що Україна фактично стала полігоном для випробування нових кіберзагроз у рамках гібридної війни, як би сумно це не звучало. Вже з 2022 року було зафіксовано тисячі атак на державні ресурси, об’єкти енергетики, транспорт і комунікації. Так, найчастіше використовуються фішингові кампанії, атаки програм-вимагачів та DDoS-операції. Діяльність CERT-UA та Державної служби спеціального зв'язку показує, що держава здатна ефективно реагувати на ці проблеми, але головним завданням залишається запобігання загрозам та підвищення стійкості інформаційних систем.

На прикладі аналізу реального випадку фішингової атаки проти державної установи було показано, що навіть технічно захищені організації залишаються вразливими через людський фактор. Оскільки, зазвичай, саме помилки співробітників, відсутність елементарної кібергігієни та ігнорування політик безпеки найчастіше призводять до компрометації систем. Тому вважаємо, що одним з ключових рекомендацій є розробка систематичних програм навчання персоналу та регулярні симуляційні тренінги (фішинг-симуляція). Це підтверджують звіти ENISA та IBM, згідно з якими компанії, які проводять такі тренінги, зменшують кількість інцидентів на 60–80.

Також необхідно зазначити те, шо другою важливою частиною практичної частини була розробка моделі для виявлення шкідливих електронних листів. Оскільки, її ефективність базується на поєднанні технічного аналізу вмісту та поведінкових ознак користувачів. Така модель може бути реалізована у вигляді розширення корпоративної електронної поштової системи з інтеграцією алгоритмів машинного навчання, що дозволить швидко блокувати підозрілі повідомлення та запобігати витоку даних.

Також, особлива увага в роботі приділяється питанню національних пріоритетів розвитку кібербезпеки України з перспективою на майбутнє. Серед найважливіших з них: є гармонізація з директивою NIS2, створення національного центру моніторингу кіберінцидентів (SOC), розвиток кіберосвіти,

зміцнення державно-приватного партнерства та участь у міжнародних програмах НАТО та ENISA. Реалізація цих напрямків дозволить перейти від реактивного до проактивного моделі кіберзахисту, коли загрози виявляються ще до їх реалізації. Одним з ключових факторів ефективної боротьби з кіберзлочинністю є усвідомлення та відповідальність кожного користувача. Навіть найкращі технології не можуть забезпечити повний захист без відповідного рівня цифрової культури населення. Тому питання освіти, просвіти та формування навичок безпечної поведінки в Інтернеті повинні стати стратегічним пріоритетом державної політики. На основі узагальнення результатів можна зробити кілька загальних висновків: Кіберзлочинність є багатовимірним і транснаціональним явищем, яке вимагає єдності правових, технічних та освітніх підходів. Міжнародна співпраця (через Будапештську конвенцію, ENISA, NATO CCDCOE) є основою формування колективної кібербезпеки. Україна поступово створює власну ефективну систему боротьби з кіберзлочинністю, але їй потрібно посилити кадрові, технічні та освітні можливості. Практична ефективність системи кіберзахисту залежить не тільки від технічних засобів, але й від організаційної культури, рівня підготовки персоналу та чіткої співпраці між державними та приватними структурами. Подальший розвиток сфери кібербезпеки повинен базуватися на поєднанні наукових досліджень, державної підтримки та міжнародного досвіду.

Отже, боротьба з кіберзлочинністю є не лише завданням технічного чи правового характеру, а й стратегічною складовою державної політики. Вона вимагає довгострокової стратегії та планування, стабільного фінансування, формування національної культури кібербезпеки та зміцнення міжнародного партнерства. Оскільки, саме поєднання цих факторів здатне забезпечити цифрову стійкість України та ефективний захист її інформаційної суверенітету в умовах сучасних глобальних викликів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Баранов О. А. Про тлумачення та визначення поняття “кібербезпека”. Правова інформатика. 2014. № 2 (42). С. 54–62 URL: https://ippi.org.ua/baranov-oa-pro-tlumachennya-ta-viznachennya-ponyattya%E2%80%9Ckiberbezpeka%E2%80%9D

2. Саєнко М. І. Міжнародний досвід протидії кіберзлочинності та кібершахрайству та можливості його використання в Україні. *Вісник УжНУ. Серія: Право*. 2021. № 74 URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2021/08/74.pdf

3. Марущак А. І. Міжнародне співробітництво у боротьбі з транснаціональною кіберзлочинністю. Інформація і право. 2018. № 3(26). С. 104–110. URL: https://ippi.org.ua/sites/default/files/12_9.pdf

4. Ільєнко А. «Сучасні кіберзагрози критичної інфраструктури України» // Кібербезпека: освіта, наука, техніка. 2025. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/719

5. Топчій В. В., Бодунова О. М. «Проблемні питання забезпечення кібербезпеки в Україні». 2025 URL: https://app-journal.in.ua/wp-content/uploads/2025/02/112.pdf

6. Аналітична стаття Національного університету “Львівська політехніка” правові аспекти забезпечення кібербезпеки в україні: сучасні виклики та роль національного законодавства, 2024. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2024/may/34615/47.pdf

7. Будапештська конвенція про кіберзлочинність (Convention on Cybercrime). Рада Європи, 2001. URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

8. Cisco Systems. What is Cybercrime? 2024. URL: https://www.cisco.com/site/us/en/learn/topics/security/what-is-cybercrime.html

9. Convention on Cybercrime (Budapest Convention). Council of Europe, 2001. URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

10. Cybersecurity Ventures. Cybercrime Damages Report 2021. URL: https://cybersecurityventures.com/annual-cybercrime-report-2017/

11. Державна служба спеціального зв’язку та захисту інформації України (ДССЗЗІ). CERT-UA. Аналітичні звіти про кіберінциденти за 2023–2025 роки. Київ: ДССЗЗІ, 2025. URL: https://cert.gov.ua

12. ДССЗЗІ; CERT-UA. Методичні рекомендації щодо впровадження систем виявлення та реагування на кіберінциденти. Київ: ДССЗЗІ, 2024. URL: https://cert.gov.ua/recommendations

13. ENISA – European Union Agency for Cybersecurity. ENISA Threat Landscape Афіни, 2024. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

14. ENISA / NATO CCDCOE. Матеріали спільних кібернавчань для країн-партнерів. Таллін. Брюссель, 2024–2025. URL: https://ccdcoe. org/library/publications

15. Encyclopaedia Britannica. Cybercrime. 2023. URL: https://www.britannica.com/topic/cybercrime

16. Europol. Internet Organised Crime Threat Assessment (IOCTA) 2023. URL: https://www.europol.europa.eu/publication-events/main-reports/internetorganised-crime-threat-assessment-iocta-2023

17. IBM Security. Cost of a Data Breach Report 2023. Армонк, 2023. URL: https://www.ibm.com/reports/data-breach

18. Кабінет Міністрів України. Законодавство у сфері кіберзахисту об'єктів критичної інформаційної інфраструктури. Міністерство цифрової трансформації України, 2024. URL: https://thedigital.gov.ua/

19. Міністерство цифрової трансформації України. Проєкт Закону України про кібербезпеку (імплементація NIS2). Офіційний портал, 2024–2025. URL: https://thedigital.gov.ua/

20. Національний координаційний центр кібербезпеки при РНБО України. Огляд стану кіберзагроз та кібероборони України за 2024 рік. Київ: РНБО, 2024. URL: https://www.rnbo.gov.ua/

21. Рада Європи. Конвенція про кіберзлочинність (Будапештська конвенція). Страсбург, 2001 (ратифікована Україною у 2005 р.). URL: https://zakon.rada.gov.ua/laws/show/994_575

22. Рада національної безпеки і оборони України. Національний координаційний центр кібербезпеки. Огляд стану кіберзагроз та кібероборони України у 2024 році. URL: https://www.rnbo.gov.ua/

23. Стаття. Договір ООН про кіберзлочинність: проблеми дефініцій та захисту цифрових прав. Інститут масової інформації / NetFreedom, 2024. URL: https://imi.org.ua/articles/un-cybercrime-treaty-analysis

24. Указ Президента України № 447/2021. Про Стратегію кібербезпеки України. Офіційний вісник Президента України, 2021. URL: https://www.president.gov.ua/documents/4472021-40013

25. United Nations Office on Drugs and Crime (UNODC). Cybercrime in Brief. 2023. URL: https://www.unodc.org/e4j/en/cybercrime/module-1/key-issues/cybercrime-in-brief.html

26. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII. Відомості Верховної Ради України, 2017, № 45, ст. 403.URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

27. Закон України «Про ратифікацію Конвенції про кіберзлочинність» № 2824-IV від 7 вересня 2005 року. Відомості Верховної Ради України, 2005, № 39, ст. 484. URL: https://zakon.rada.gov.ua/laws/show/2824-15

28. CCDCOE. National Cybersecurity Governance: Ukraine. 2024. URL:https://ccdcoe.org/uploads/2024/08/National-Cybersecurity-Governance_Ukraine_Davydiuk_Potii_2024.pdf

29. CERT-UA. Cyber Threat Overview and Defense Strategies in 2025. URL: https://www.cip.gov.ua/en/faqs/cyber-threat-overview-and-defensestrategies-in-2025-cert-ua-s-experience

30. ENISA. Awareness and Cyber Hygiene. 2024. URL: https:// www.enisa.europa.eu/topics/awareness-and-cyber-hygiene

31. ENISA. ENISA Threat Landscape 2025. 2025. URL: https://www. enisa.europa.eu/publications/enisa-threat-landscape-2025

32. ENISA. Threat Landscape. 2024. URL: https://www.enisa. europa.eu/topics/cyber-threats/threat-landscape

33. European Institute of Public Administration (EIPA). The NIS2 Directive: The Road Map to Strengthen Cybersecurity. 2025. URL: https://www.eipa.eu/wp-content/uploads/2025/02/BLOG_NIS2_FEB25.pdf

34. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Building Resilience in the Face of Russian Cyber Aggression: Ukraine as the Frontline of European Cyber Defence. Tallinn, 2025. URL: https://ccdcoe.org/library/publications/

35. NIST. Role-Based Security Training in Federal Agencies. SP 800-50 (updated 2024).URL: https://csrc.nist.gov/publications/detail/sp/800-50/final

36. Рада національної безпеки і оборони України. Національний координаційний центр кібербезпеки. Огляд стану кіберзагроз та кібероборони України – 2024. URL: https://www.rnbo.gov.ua

37. The Record / CERT-UA. Russian hackers turn to AI as old tactics fail, Ukrainian CERT 2025.URL: https://therecord.media/russian-hackers-turn-to-ai-ukraine-cert

38. Wired. Hacker group linked to Russian military claims credit for cyberattack on Ukrainian telecom. 2024.URL: https://www.wired.com/story/ukraine-kyivstar-solntsepek-sandworm-gru/

39. ENISA. Cybersecurity Skills Development in the EU and Beyond. Афіни: ENISA, 2020. URL: https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union

40. NATO CCDCOE. Locked Shields 2025 – Lessons Learned in National Cyber DefenseCooperation.URL:https://ccdcoe.org/uploads/2024/10/2025_NATO_CCD_COE_Training_Catalogue_final.pdf

41. Cybersecurity Ventures. Cybercrime to Cost the World $6 Trillion Annually by 2021. URL: https://cybersecurityventures.com/wpcontent/uploads/2021/01/Cyberwarfare-2021-Report.pdf

42. Webroot. 2019 Threat Report: Ransomware Losses Exceed $8 Billion. 2019.URL:https://wwwcdn.webroot.com/9315/5113/6179/2019_Webroot_Threat_Report_US_Online.pdf

43. CERT-UA. Annual Cyber Threat Report 2023. Київ: ДССЗЗІ, 2023. URL: https://cip.gov.ua/en/news/uryadova-komanda-cert-ua-v-2023-roci-opracyuvala-2543-kiberincidenti

44. Стратонов В.М. «Комп'ютерні злочини» окремі особливості та характеристики. Науковий вісник Дніпропетровського державного університету внутрішніх справ. 2020. №2. С.134-141. URL: https://visnik.dduvs.in.ua/?page_id=48

45. Стратонов В., Слінько Д., Слінько С. «Деякі види комп'ютерної злочинності та кіберзлочинності в Україні» *Доступ до правосуддя у Східній Європі* 2021, *Т4,* 3(11) С. *191–197* URL: https://ajee-journal.com/some-types-of-computer-crime-and-cybercrime-in-ukraine https://doi.org/10.33327/AJEE-18-4.3-n000078

46. Violetta E. Konovalova, Vasyl M. Stratonov, & Iryna V. Savelieva (2021). Biometric personal data and their use in the investigation of criminal offences. *Journal of the National Academy of Legal Sciences of Ukraine*, (4), P. 289-300 URL: https://visnyk.kh.ua/uk/journals/visnik-naprnu-4-2021-r/biometrichni-personalni-dani-ta-yikh-vikoristannya-v-rozsliduvanni-kriminalnikh-pravoporushen

47. Стратонов В., Дзюрбель А. ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ТА ІНФОРМАЦІЙНИХ МОЖЛИВОСТЕЙ У СТВОРЕННІ ПРОФІЛЯ ЗЛОЧИНЦЯ. Науковий вісник Херсонського державного університету**. С**ерія: «Юридичні науки» Випуск 5. 2024. Гельветика, 2024. С.21-27 URL: https://lj.journal.kspu.edu/index.php/lj/issue/view/20

48. Стратонов В. АКТУАЛЬНІ НАПРЯМИ ВИКОРИСТАННЯ ЕЛЕКТРОННИХ ІНФОРМАЦІЙНИХ СИСТЕМ В УМОВАХ ВОЄННОГО СТАНУ. Науковий вісник Херсонського державного університету**.** Серія: «Юридичні науки» Випуск 1. 2025. Гельветика, 2025. С. 36-42 DOI https://doi.org/10.32999/ksu2307-8049/2025-1-6 URL: https://lj.journal.kspu.edu/index.php/lj/article/view/ 463/ 417

49. Стратонов В. ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ У ВИЯВЛЕННІ ТА ДОКУМЕНТУВАННІ ФАКТІВ ЕКСПЛУАТАЦІЇ ЛЮДИНИ ПІД ЧАС ЗБРОЙНИХ КОНФЛІКТІВ: ДОКАЗОВА БАЗА В МІЖНАРОДНИХ СУДАХ Вчені записки ТНУ імені В.І. Вернадского. Серія: юридичні науки Том 36 (75) №1. 2025. С.173-178 DOI https://doi.org/10.32782/TNU-2707-0581/2025.1/28 URL:https://www.juris.vernadskyjournals.in.ua/journals/2025/1 _2025/30.pdf

50. Стратонов В.М. ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ У ВИЯВЛЕННІ ТА ДОКУМЕНТУВАННІ ФАКТІВ ЕКСПЛУАТАЦІЇ ЛЮДИНИ ПІД

ЧАС ЗБРОЙНИХ КОНФЛІКТІВ: ДОКАЗОВА БАЗА В МІЖНАРОДНИХ СУДАХ. Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки. Том 36 (75), №1. 2025. С. 173-178. DOI: https://doi.org/10.32782/TNU-2707-0581/2025.1/28

51. Стратонов В.М. АКТУАЛЬНІ НАПРЯМИ ВИКОРИСТАННЯ ЕЛЕКТРОННИХ ІНФОРМАЦІЙНИХ СИСТЕМ В УМОВАХ ВОЄННОГО СТАНУ. Науковий вісник Херсонського державного університету. Серія: «Юридичні науки». Випуск 1. 2025. Гельветика, 2025. С. 36–42. https://doi.org/10.32999/ksu2307-8049/2025-1-6 ; https://lj.journal.kspu.edu/index.php/lj/article/view/463/417

52. Стратонов В.М. ЕЛЕКТРОННЕ СУДОЧИНСТВО В УКРАЇНІ: АНАЛІЗ ВІТЧИЗНЯНОГО ЗАКОНОДАВСТВА. Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки. Том 35 (74), № 6. 2024. С. 122–128. https://www.juris.vernadskyjournals.in.ua/journals/2024/6_2024/23.pdf

53. Стратонов В.М. ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ТА ІНФОРМАЦІЙНИХ МОЖЛИВОСТЕЙ У СТВОРЕННІ ПРОФІЛЯ ЗЛОЧИНЦЯ. Науковий вісник Херсонського державного університету. Серія: «Юридичні науки». Випуск 5. 2024. Гельветика, 2024. С. 21-27. https://lj.journal.kspu.edu/index.php/lj/issue/view/20

54. Стратонов В., Проценко М.В. Штучний інтелект у судочинстві України: нормативно-правове визначення. Криміналістика і судова експертиза: міжвідом. наук.-метод. зб. / Київський НДІ судових експертиз; редкол.: Д. В. Журавльов (голов. ред.), О. Г. Рувін (заст. голов. ред.) та ін. – Київ: Видавництво Ліра-К, 2022. Вип. 67. 704 с. https://jurkniga.ua/contents/kriminalistika-i-sudova-ekspertiza-izhvidomchiy-naukovo-metodichniy-zbirnik.pdf

55. Стратонов В.М. Стан наукового дослідження криміналістичної характеристики кіберзлочинів як елементу методики їх розслідування. Інновації в криміналістиці та судовій експертизі: матеріали міжвідом. наук.-практ. конф. (Київ, 25 листоп. 2021 р.) / [редкол.: В. В. Чернєй, С. С. Чернявський, А. А. Саковський та ін.]. Київ: Нац. акад. внутр. справ, 2021. 435 с. С. 55-59.

56. Стратонов В.М. «Комп'ютерні злочини»: окремі особливості та характеристики. Науковий вісник Дніпропетровського державного університету внутрішніх справ. 2020. № 2. С. 134-141. https://visnik.dduvs.in.ua/?page_id=48

57. Стратонов В.М. Інформація та інформаційні відносини як новий криміналістичний об'єкт. Південноукраїнський правничий часопис. № 4, 2019. С. 84–89.

58. Гавловська А.О. Превенція (запобігання) самовільного залишення частини або місця служби в умовах воєнного стану в України. Київський часопис

права. 2025. № 2. С. 338-343. https://kyivchasprava.kneu.in.ua/index.php/kyivchasprava/article/view/618/587 DOI https://doi.org/10.32782/klj/2025.2.45

59. Гавловська А.О. Кримінологічний портрет військовослужбовця-правопорушника, що скоює СЗЧ, в умовах російсько-української війни. Juris Europensis Scientia. Випуск 3, 2025. С. 142-147. http://jes.nuoua.od.ua/archive/3_2025/30.pdf DOI https://doi.org/10.32782/chern.v3.2025.28