ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ
МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ДЕМЕДЮК СЕРГІЙ ВАСИЛЬОВИЧ

УДК 343.9.01:004.056(477)

ОРГАНІЗАЦІЙНО-ПРАВОВІ ТА КРИМІНОЛОГІЧНІ ЗАСАДИ КІБЕРСТІЙКОСТІ В УКРАЇНІ

12.00.07 «Адміністративне право і процес; фінансове право;
інформаційне право»
12.00.08 «Кримінальне право та кримінологія; кримінально-виконавче право»

Реферат
дисертації на здобуття наукового ступеня
доктора юридичних наук

Одеса – 2026

Дисертацією є кваліфікаційна наукова праця на правах рукопису.

Робота підготовлена здобувачем самостійно.

Опоненти: доктор юридичних наук, професор,
заслужений юрист України
КАРЧЕВСЬКИЙ Микола Віталійович,
ЗВО «Університет Короля Данила»,
професор кафедри права імені академіка УАН
о. Івана Луцького;

доктор юридичних наук, професор
СОБКО Ганна Миколаївна,
Одеський державний університет внутрішніх справ,
професор кафедри кримінального права та кримінології;

доктор юридичних наук, професор
ВЕСЕЛОВ Микола Юрійович,
Державний університет економіки і технологій,
професор кафедри права Навчально-наукового юридичного інституту.

Захист відбудеться 07 травня 2026 р. о 10:00 годині на засіданні спеціалізованої вченої ради Д 41.884.04 в Одеському державному університеті внутрішніх справ за адресою: 65014, місто Одеса, вул. Успенська, 1.

З дисертацією можна ознайомитись на офіційному сайті https://oduvs.edu.ua/ та в науковій бібліотеці Одеського державного університету внутрішніх справ за адресою: 65014, місто Одеса, провулок Сабанський, 4.

Вчений секретар
спеціалізованої вченої ради **О.В. Ковальова**

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Обґрунтування вибору теми дослідження. На сучасному етапі розвитку інформаційного суспільства спостерігається фундаментальне зміщення акцентів у стратегіях забезпечення кіберзахисту. Традиційна модель «кібербезпеки», зосереджена переважно на створенні непроникних бар'єрів та запобіганні вторгненням, демонструє обмежену ефективність перед обличчям складних багатовекторних кібератак. Визнання концепції «неминучості компрометації» зумовило появу та розвиток парадигми кіберстійкості. На відміну від статичного захисту, кіберстійкість визначається як здатність соціотехнічних систем передбачати, протистояти, відновлюватися та адаптуватися до несприятливих умов, стресів або активних нападів на цифрові ресурси.

Актуальність дослідження на світовому рівні підтверджується прийняттям засадничих актів, що в одних випадках прямо вказують на кіберстійкість, зокрема в ЄС – Акт Європейського Союзу про кіберстійкість (*EU Cyber Resilience Act – 2024*), а в інших – містять окремі розділи цього спрямування, зокрема у Великій Британії – Національна кіберстратегія та розділ у ній «Кіберстійкість» (*National Cyber Strategy (Cyber Resilience) – 2023*) та США – Американська кіберстратегія Президента Трампа (*President Trump's Cyber Strategy for America – 2026*), з включенням змістовних складових кіберстійкості, а також правовим врегулюванням у цій сфері безпекових стандартів NIST, MITRE і NIS2, що також націлюють на застосування цієї концепції та спрямовують на забезпечення життєздатності систем навіть у стані часткового ураження.

Для України актуальність розбудови національної кіберстійкості набуває особливої гостроти, що детерміновано безпрецедентною інтенсивністю кібератак у межах гібридної агресії. Специфіка сучасного протистояння свідчить, що об'єктами атак стають не лише окремі бази даних, а цілісні екосистеми надання державних послуг, енергетичні мережі та транспортні комунікації. У цьому контексті кіберстійкість виступає критичним компонентом національної безпеки, оскільки вона гарантує безперервність функціонування органів державної влади та об'єктів критичної інфраструктури. Необхідність теоретичного осмислення та практичного впровадження засад кіберстійкості в Україні зумовлена потребою створення механізмів, які б дозволили мінімізувати час відновлення після інцидентів та забезпечили гнучкість управління ризиками в умовах високої невизначеності.

Водночас, інституціоналізація кіберстійкості вимагає перегляду наявних організаційно-правових засад, оскільки існуюче нормативне регулювання часто орієнтоване на реагування, а не на проактивне вибудовування стійких архітектур. Актуальність теми підсилюється необхідністю адаптації українського законодавства до вимог європейських стандартів, що передбачає запровадження жорстких вимог до кіберстійкості продуктів із цифровими елементами протягом усього їхнього життєвого циклу. Створення ефективної системи управління кіберстійкістю на державному рівні потребує чіткого нормативного визначення функцій суб'єктів кібербезпеки, розробки метрик оцінювання здатності до відновлення та формування культури розбудови стійкості.

Окремим аспектом актуальності є стрімка трансформація кіберзлочинності, яка дедалі частіше використовує вразливості людського фактора та складні схеми онлайн-шахрайства для підриву довіри до цифрових інституцій. Водночас, протидія кіберзлочинності є одним із ключових напрямів забезпечення кіберстійкості суспільства і з врахуванням вимоги щодо комплексності дослідження, потребує адекватного, саме на основі сучасних кримінологічних підходів, обґрунтування змісту та пріоритетів відповідної державної політики.

Кримінологічний аналіз сучасних загроз свідчить про глибоку інтеграцію зловмисних практик у соціальні мережі та хмарні сервіси. Забезпечення кіберстійкості за таких умов неможливе без розробки новітніх методологічних засад виявлення злочинної діяльності, зокрема через використання аналітичної розвідки (OSINT) та впровадження відповідних правоохоронних стратегій (Intelligence-Led Policing, IOCTA). Дослідження кримінологічних детермінант кіберзагроз дозволяє сформувати пріоритети стратегічної протидії злочинності, що є невід'ємною частиною загальної кіберстійкості держави та її громадян.

Водночас, динамічність кіберпростору робить традиційні статистичні методи малоефективними для довгострокового прогнозування. Потреба у використанні інтелектуальних методів аналізу, експертних оцінок для форсайту кіберзагроз та оцінювання ризиків, є нагальною науковою проблемою. Розробка прогнозних моделей стійкості дозволить здійснювати превентивні інвестиції в найбільш вразливі ділянки цифрового простору, забезпечуючи перехід від боротьби з наслідками інцидентів до управління потенціалом адаптації та сталого розвитку національної кіберсистеми.

Викладені вище обставини у своїй сукупності засвідчують актуальність теми дисертаційного дослідження.

Ступінь наукової розробленості проблеми. Низка проблемних питань такої широкої палітри наукового пізнання достатньо поглиблено досліджувалися у роботах вітчизняних і зарубіжних вчених. Зокрема, доктринальні положення та окремі аспекти адміністративно-правового й інформаційно-правового характеру щодо формування та реалізації державної політики були предметом вивчення таких вчених як: В. Авер'янов, О. Баранов, К. Бєляков, Ю. Битяк, Л. Веселова, В. Галунько, В. Грохольський, А. Денисова, І. Діордіца, Д. Дубов, Д. Калаянов, Р. Калюжний, В. Колпаков, М. Корнієнко, О. Коропатов, О. Крижановська, А. Марущак, В. Пилипчук, В. Пядишев, Н. Свиридюк, В. Стефанюк, С. Тімченко, Т. Тур, Т. Фулей, І. Цюприк, Ю. Шемшученко, Х. Ярмакі та ін. Водночас, кримінологічний ризик-орієнтований базис, а також сучасний кримінологічний інструментарій, зокрема і у сфері кібербезпеки із застосуванням інформаційних технологій, були предметом вивчення таких вчених як: А. Бабенко, Д. Балобанова, В. Бутузов, В. Дрьомін, С. Зибін, С. Казмірчук, М. Карчевський, О. Користін, В. Конопельський, М. Корнієнко, О. Корченко, О. Костенко, О. Литвак, В. Литвиненко, В. Меркулова, В. Підгородинський, Г. Собко, П. Фріс, О. Шкута та ін.

Серед зарубіжних вчених важливо виділити доктринальні дослідження саме на рівні пізнання суспільства ризику таких вчених як: У. Бек, Ф. Фукуяма, А. Гідденс,

а також щодо формування кіберстійкості у сучасному безпековому кіберпросторі: Г. Тіірмаа-Клаар, Д. Бодо, Н. Вайлдінг, Л. Геррінгтон, Б. Дюпон, С. Муйє, Р. Олдріч, М. Тонхаузер, Й. Ріствей, С. Хассілл, Р. Екмаєр, В. Фумі, Ж-П. Кемар, Н. Полемі, Р. Румпель Келлі, С. Леверетт, Е. Оутон, Дж. Копік, С. Такер, Р. Пант, Л. Прайор, Г. Кассара, Т. Еван, С. Дж. Раффл, М. Тувесон, А. Коберн, Д. Ральф та Дж. В. Голлта багато інших.

Попри численні дослідження, правове регулювання кіберстійкості стало ключовим чинником нацбезпеки України. В умовах гібридної війни, де кібератаки супроводжують воєнні дії, розбудова такої системи є стратегічним пріоритетом для стійкості суспільства. Саме тому, обране дослідження спрямоване на удосконалення національної доктрини кібербезпеки на основі розробки організаційно-правових та кримінологічних засад кіберстійкості, що є критично важливою науковою та практичною проблемою. Поєднання компаративістики з методологією стратегічного аналізу на основі оцінки ризиків дозволяє сформувати дієвий механізм протидії сучасним кіберзагрозам та забезпечити сталий розвиток цифрового суспільства в Україні.

Зв'язок роботи з науковими програмами, планами, темами. Тема дисертаційного дослідження узгоджується з положеннями: 1) п. 4 розділу 1 та 47 розділу 3 Стратегії національної безпеки України (Указ Президента України від 14.09.2020 р. № 392/2020); 2) п.п. 4 та 5 Стратегії кібербезпеки України (Указ Президента України від 26.08.2021 р. № 447/2021); 3) п. 1.2 розділу ІІ Комплексного стратегічного плану реформування органів правопорядку як частини сектору безпеки і оборони України на 2023-2027 роки (Указ Президента України від 11.05.2023 р. № 273/2023); 4) п. 16 Плану заходів на 2025 рік реалізації Стратегії кібербезпеки України (Розпорядження КМУ від 07.03.2025 р. № 204-р); 5) п.п. 3, 7, 11, 13 Тематики наукових досліджень та науково-технічних (експериментальних) розробок на 2025–2029 роки (наказ МВС від 21.05.2024 р. № 326); 6) темою науково-дослідних робіт Одеського державного університету внутрішніх справ «Пріоритетні напрямки розвитку реформування правоохоронних органів в умовах розгортання демократичних процесів у державі» (номер державної реєстрації 0123U103538).

Тему дисертації затверджено рішенням Вченої ради Одеського державного університету внутрішніх справ (протокол № 2 від 27.01.2026 року).

Мета і завдання дослідження. *Метою* дослідження є висвітлення організаційно-правових та кримінологічних засад кіберстійкості України та визначення пріоритетних напрямів розвитку вітчизняного законодавства.

Для досягнення цієї мети потрібно розв'язати наступні *завдання*:

- дослідити генезис та еволюцію концепції «стійкості» у міждисциплінарному розрізі для визначення теоретичного підґрунтя кіберстійкості;

- розмежувати поняття «кібербезпека» та «кіберстійкість», обґрунтувавши перехід до нової парадигми захисту в умовах високої невизначеності з визначенням ключових спроможностей системи кіберстійкості;

- проаналізувати міжнародний досвід та стратегічні моделі розбудови кіберстійкості (на прикладі НАТО, ЄС, США та Великобританії) для формування

концептуальних засад та практичних рекомендацій щодо створення національної системи кіберстійкості України;

- обґрунтувати інституціональну модель кіберстійкості як інтегровану систему взаємодії ринкових, стандартизаційних та регуляторних механізмів у забезпеченні стійкості національної кіберсистеми;

- здійснити функціональний аналіз суб'єктного складу національної системи кібербезпеки України, визначити роль державних органів у впровадженні інституційної моделі стійкості та оцінити рівень міжнародної інтеграції України у глобальний кібербезпековий простір;

- розробити та обґрунтувати концептуальні засади цивільно-військового співробітництва як системоутворюючого компонента національної кіберстійкості України;

- проаналізувати та визначити сучасний методологічний підхід щодо аналітичної розвідки стратегічних напрямів кіберстійкості через інтеграцію методів стратегічного форсайту, OSINT-моніторингу та ризик-орієнтованого аналізу;

- здійснити комплексний аналіз та ранжування ключових кіберзагроз за рівнем ризику їх поширення в Україні, для обґрунтування пріоритетних стратегічних напрямів розбудови національної кіберстійкості;

- обґрунтувати методологічні засади діагностики кіберстійкості національної інформаційної інфраструктури через розробку та апробацію інтегрованої матричної моделі, що поєднує цикли управління інцидентами (планування, поглинання, відновлення, адаптація) з операційними доменами системи (фізичним, інформаційним, когнітивним, соціальним);

- провести прикладний аналіз інституційної спроможності суб'єктів кібербезпеки України на основі ризик-орієнтованого підходу та розробити стратегічні правові орієнтири для подолання виявлених системних розривів;

- обґрунтувати методологічні засади кримінологічного аналізу кіберзлочинності в Україні, що базується на синергії ризик-орієнтованого підходу та інструментарію стратегічного аналізу;

- на основі емпіричного аналізу ідентифікувати ключові виклики кіберзлочинності та актуальний інструментарій вчинення злочинів;

- проаналізувати фінансову екосистему кіберзлочинності, інструменти анонімізації та комунікації зловмисників, а також роль міжсекторальних факторів (соціальна інженерія, IoT) у формуванні сучасного ландшафту кримінальних загроз в Україні.

Об'єктом дослідження є суспільні відносини у сфері забезпечення кібербезпеки в Україні.

Предметом дослідження є організаційно-правові та кримінологічні засади кіберстійкості України.

Методи дослідження. Багатоаспектність предмета гносеології обумовлює необхідність застосування цілісної системи методологічного інструментарію, що включає в себе:

- *генетико-морфологічний аналіз* використаний у підрозділі 1.1 для дослідження історичного походження терміна «стійкість»;

- *компаративний аналіз* застосований для розмежування понять «кібербезпека» та «кіберстійкість» та порівняння класичної парадигми «кібербезпеки» з новітньою концепцією «кіберстійкості» (2.1); зіставлення євроатлантичних стандартів (Директива NIS2, моделі CIMIC НАТО) із поточною нормативною базою та практичним досвідом України (2.2, 2.3); аналізу міжнародних інструментів співпраці (4.3) та розробки пропозицій щодо гармонізації українського законодавства;

- *системний підхід* застосований для дослідження національної системи кібербезпеки як складного соціотехнічного комплексу (2.1-2.3);

- *функціонально-структурний аналіз* використаний у підрозділі 1.2 для декомпозиції життєвого циклу стійкості на окремі фази (передбачення, витримування, відновлення, адаптація); для розмежування повноважень суб'єктів кібербезпеки України відповідно до їхніх ролей у забезпеченні стійкості (2.2) та визначення специфічних функцій «цивільних асистентів» та «кіберрезерву» у системі оборони держави;

- *контент-аналіз нормативно-правової бази* використаний у підрозділі 1.3 для вивчення стратегій кібербезпеки України та провідних держав світу, а також критичного аналізу Закону «Про основні засади забезпечення кібербезпеки України» та Директиви NIS2 (2.3);

- *метод термінологічного аналізу та дефініції* використаний для уточнення понятійно-категоріального апарату, виявлення «термінологічного розриву» у чинному законодавстві та формулювання авторського визначення понять «інституціоналізація кіберстійкості» (2.1) та «Cyber-CIMIC» (2.3);

- *метод моделювання* застосовано для розробки теоретичної моделі багаторівневої взаємодії суб'єктів, побудови моделі «координаційного хабу» на базі НКЦК та моделі цивільно-військового співробітництва, що охоплює стратегічний, тактичний та операційний рівні (2.2, 2.3);

- *метод екстраполяції та прогнозування* застосовано для визначення перспектив розвитку національної системи кіберстійкості (2.2, 2.3, 3.1);

- *соціологічний аналіз* використаний для переосмислення природи кіберзагроз не лише як технічних проблем, а як соціальних ризиків, що дозволило обґрунтувати необхідність залучення громадян як активних суб'єктів кіберстійкості (розділ 3);

- *ризик-орієнтований метод* застосований як наскрізний інструмент для обґрунтування пріоритетності інвестицій у кіберстійкість та протидії кіберзлочинності (розділи 3, 4);

- *метод стратегічного управління* застосований для визначення пріоритетів державної політики у сфері кібербезпеки, що дозволило сформувати ієрархію цілей: від захисту індивідуального користувача до гарантування безпеки критичної інфраструктури держави (розділи 3, 4).

Емпіричну основу дослідження складають: дані державної статистичної звітності – матеріали Офісу Генерального прокурора щодо зареєстрованих кримінальних правопорушень; статистичні відомості Державної судової адміністрації України; інформаційні та аналітичні матеріали Національного координаційного центру кібербезпеки РНБО України, Держспецзв'язку та

Національної поліції України; дані експертних та соціальних опитувань щодо кіберзагроз та кіберстійкості національної системи кібербезпеки (1013 осіб, які представляють фахове середовище в центральних та місцевих органах влади, на об'єктах критичної інформаційної інфраструктури та правоохоронних органах), а також щодо протидії кіберзлочинності (764 співробітників Департаменту кіберполіції НПУ).

Правову основу дослідження склали конституційні норми, міжнародно-правові акти (міжнародні конвенції, директиви ЄС тощо), нормативно-правові акти Верховної Ради України, Кабінету Міністрів України, Президента України, РНБО України, Держспецзв'язку України, Національної поліції України, Служби безпеки України, Офісу Генерального прокурора України тощо.

Наукова новизна отриманих результатів пояснюється тим, що дисертація є першим комплексним дослідженням, у якому системно висвітлюється концепт кіберстійкості як вищий рівень кібербезпеки України та сформульовано низку нових положень, зокрема:

вперше:

- сформульовано дефініцію національної кіберстійкості як динамічної емерджентної властивості соціо-кібернетичної системи, що інтегрує не лише технічні параметри захисту, а й когнітивні та організаційні аспекти адаптації до умов високої невизначеності;

- запропоновано концептуальну модель «спільної відповідальності» в межах національної екосистеми кіберстійкості, де держава виступає фасилітатором та ризик-менеджером, надаючи бізнесу інструменти самооцінки та розвідувальні дані в обмін на прозору звітність, а стійкість держави розглядається як похідна від здатності окремих суб'єктів критичної інфраструктури до самовідновлення;

- обґрунтовано трикомпонентну інституціональну модель кіберстійкості (маркетинг – стандартизація – регулювання) як цілісну систему формування та реалізації політики кіберстійкості, що дозволяє інтегрувати економічні, організаційні та правові механізми в єдину архітектуру кіберменеджменту;

- сформульовано концептуальну модель «Cyber-CIMIC» як специфічну форму цивільно-військового співробітництва в цифровому просторі, що, на відміну від класичної моделі CIMIC НАТО (орієнтованої на підтримку військових операцій у фізичних доменах), розглядається як безперервний процес соціотехнічної взаємодії державних, військових та приватних акторів для забезпечення національної кіберстійкості;

- обґрунтовано необхідність запровадження інституту «цивільного кіберрезерву» та правового режиму «регуляторних пісочниць» у сфері кібероборони, що дозволяє легітимізувати участь недержавних суб'єктів у відсічі збройній агресії в кіберпросторі без обов'язкової комбатантизації за класичними ознаками;

- сформульовано концептуальну модель «Стійкість через право», яка базується на переході від декларативного характеру норм кібербезпеки до жорсткої юридичної фіксації необхідних функціональних спроможностей суб'єктів (передбачення, витримування, відновлення, адаптація);

- обґрунтовано концептуальну модель «інтелектуальної стійкості», яка розглядає аналітичну розвідку як цілісний процес трансформації первинних даних у стратегічні рішення через синергію OSINT як джерела актуальної фактологічної бази, форсайту як інструменту предиктивного моделювання альтернативних сценаріїв і «слабких сигналів» та ризик-орієнтованого підходу як механізму пріоритезації ресурсів, що у сукупності забезпечує перехід від реактивного захисту до проактивного управління життєздатністю критичної інфраструктури в умовах гібридної агресії;

- сформовано ієрархічну модель кіберзагроз для України, яка інтегрує технічні вразливості з деструктивними наслідками гібридної агресії та кібертероризму в єдиному розрахунковому полі ризиків;

- експериментально встановлено та математично підтверджено залежність між профілем професійного досвіду експерта (стаж <3, 3–10, >10 років) та суб'єктивною оцінкою рівня ризику специфічних кіберзагроз;

- розроблено та апробовано комплексну діагностичну матрицю кіберстійкості національної інфраструктури, яка дозволяє вимірювати нелінійні зв'язки між технічною стабільністю фізичного домену та ефективністю ухвалення рішень у когнітивній і соціальній сферах;

- обґрунтовано та емпірично підтверджено існування «безпекового розриву» між центральним та регіональним рівнями управління кібербезпекою України, що потребує переходу від уніфікованого до диференційованого правового регулювання;

- здійснено комплексне зіставлення експертних оцінок на основі ризик-орієнтованого підходу з статистичними даними ЄРДР, що дозволило виявити розбіжності у обліку кіберзлочинів (зокрема за ст. 362 ККУ) та обґрунтувати необхідність вдосконалення системи кодування злочинів у цифровій сфері;

- обґрунтовано та реалізовано стратегічний аналіз кіберзлочинності в Україні, що базується на інтеграції ризик-орієнтованого підходу та методології Europol IOCTA, що передбачає не лише аналіз статистичних даних ЄРДР, а й обов'язкове залучення експертної думки;

- ідентифіковано та класифіковано специфічний інструментарій кіберзлочинців за рівнем поширеності в українському сегменті, зокрема встановлено домінування операційної системи Kali Linux та використання методів Брутфорс і DoS-атак як ключових засобів вчинення кіберзлочинів;

- на основі емпіричних даних обґрунтовано вплив анонімізації на ефективність правоохоронної діяльності через оцінку популярності VPN-сервісів та мережі Tor, а також прогнозування майбутніх ризиків їх використання як засобів приховування злочинної діяльності в умовах цифровізації.

удосконалено:

- теоретичне розмежування категорій «кібербезпека» та «кіберстійкість» у контексті державного управління, що полягає у трактуванні кіберстійкості не як технічного стану, а як динамічної інституційної спроможності системи до адаптації та самовідновлення, що потребує інтеграції в загальну стратегію корпоративного та державного управління;

- підхід до формування національної екосистеми кіберстійкості шляхом синтезу трьох складників: нормативної обов'язковості (досвід ЄС), технологічної адаптивності (досвід США) та соціотехнічної синергії (досвід Великобританії), що дозволяє перейти від фрагментарного захисту до створення «колективного імунітету» держави;

- механізм інтеграції метрик кіберстійкості, на основі ризик-орієнтованого підходу, у загальну систему управління державними ризиками, що забезпечує перехід від кількісного підрахунку інцидентів до оцінки реальної готовності інфраструктури до відновлення;

- підхід до інституційного забезпечення кіберстійкості на національному рівні шляхом визначення функціональної моделі розподілу повноважень між суб'єктами кібербезпеки, що забезпечує комплексність, уникнення дублювання функцій та підвищення ефективності управління кіберризиками

- функціональну схему розподілу повноважень суб'єктів національної системи кібербезпеки, де, на основі аналізу чинного законодавства, чітко розмежовано вектори впливу: регуляторний (Держспецзв'язку), стандартизуючий (НКЦК як методологічний хаб) та стимулюючий (Мінцифра), що усуває дублювання функцій та підвищує керованість системи;

- понятійно-категоріальний апарат щодо змісту терміна «цивільно-військове співробітництво у сфері кібербезпеки», який на відміну від існуючих підходів, трактується не як ситуативна взаємодія, а як сталий правовий та організаційний механізм інтеграції ресурсів волонтерських ІТ-спільнот та приватного сектору до загальнодержавної системи кібероборони;

- організаційно-функціональну структуру взаємодії суб'єктів кібербезпеки, де роль Національного координаційного центру кібербезпеки (НКЦК) трансформована із суто дорадчого органу в стратегічний «комунікаційний хаб», що забезпечує вертикальну та горизонтальну сумісність військових і цивільних стандартів обміну інформацією;

- методологію стратегічного аналізу кіберзагроз через інтеграцію інструментарію OSINT у структуру ризик-менеджменту, що перетворює відкриті дані на верифіковані індикатори для розрахунку ймовірності та впливу загроз;

- класифікацію кіберзагроз у контексті ІПСО та гібридної війни, де кібератака розглядається не лише як технічний акт, а як інструмент маніпуляції суспільною довірою та дискредитації військово-політичного керівництва;

- модель міждоменної комунікації в кіберсистемах, де когнітивний домен визначено як ключовий чинник «живучості» системи через його здатність перерозподіляти інформаційні потоки у разі руйнування фізичних вузлів;

- типологію on-line шахрайства через диференціацію загроз із використанням платіжних карток (фішинг, вішинг) та без них (торгівля віртуальними товарами, криптовалютні махінації), що дозволяє правоохоронним органам точніше фокусувати оперативні ресурси;

- типологію засобів анонімізації злочинців, де в системному аналізі розмежовано використання комерційних VPN, власноналаштованих серверів та децентралізованих мереж;

- типологію фінансової активності кіберзлочинців через розмежування платіжних інструментів за рівнем ризику: від традиційних банківських переказів до використання криптовалют (Bitcoin, USDT) та систем електронних грошей (EasyPay, PayPal), що сприяє розробці ефективніших механізмів фінансового моніторингу;

- систему джерел кримінологічної інформації про on-line шахрайства, де окрім матеріалів кримінальних проваджень, враховано значну питому вагу довідково-аналітичних матеріалів (близько 30%), що дозволяє нівелювати вплив високої латентності цього виду злочинів.

дістали подальшого розвитку:

- міждисциплінарна теорія стійкості через адаптацію екологічних та інженерних принципів стійкості до специфіки функціонування сучасних кіберфізичних систем та ІТ-мереж;

- теоретичні підходи до розуміння кіберстійкості як складної адаптивної системи, в якій ключову роль відіграє не сукупність заходів, а їх узгодженість, пріоритезація та здатність до динамічної трансформації в умовах невизначеності;

- концепція міжнародної суб'єктності України в глобальному кіберпросторі на основі подальшого розвитку та трансформації України з реципієнта міжнародної технічної допомоги у ключового донора унікального практичного досвіду для країн НАТО та ЄС, що легітимізує національні безпекові протоколи як основу для майбутніх міжнародних стандартів колективної стійкості;

- підходи до гармонізації національного законодавства із євроатлантичними вимогами, зокрема в частині адаптації стандартів ISO/IEC 27000 та положень Директиви NIS2, що забезпечує інституційну сумісність України з міжнародними мережами реагування на інциденти;

- наукові підходи до формування мережевої моделі кібероборони, що базується на принципах функціональної комплементарності та розподіленої відповідальності, що дозволяє ефективно масштабувати спроможності держави за рахунок гнучкого залучення цивільного інтелектуального капіталу в умовах гібридної війни;

- методика багаторівневої фільтрації експертних даних у сфері кібербезпеки на основі «тесту на логічну узгодженість», що дозволило статистично значущо підвищити надійність прогнозних моделей розвитку кіберзагроз;

- використання методів інтелектуального аналізу даних для моніторингу регіональних та галузевих особливостей поширення кіберризиків в Україні;

- кримінологічна теорія мотивації кіберзлочинців, доповнена факторами «гібридної війни» та «колабораційної співпраці», що виходить за межі класичного корисливого мотиву;

- кримінологічна характеристика способів комунікації в кіберпросторі, яку доповнено порівняльним аналізом використання месенджерів (Telegram – 66%, WhatsApp – 56,3%, Viber – 52,3%) як основних каналів взаємодії між злочинцями та жертвами, а також прогнозуванням ризиків їх використання у післявоєнний період;

- розуміння впливу технологічних чинників на ландшафт кіберзлочинності, зокрема щодо експлуатації вразливостей Інтернету речей (IoT) для створення ботнетів та проведення DDoS-атак, що розглядається як критична загроза для стабільності цифрової інфраструктури в умовах масової цифровізації;

- теоретичні засади протидії соціальній інженерії, які розширено через аналіз динаміки поширення методів фішингу, вішингу та смішингу, а також обґрунтування того, що людський фактор залишається найбільш критичною ланкою в системі забезпечення кіберстійкості держави.

Практичне значення отриманих результатів. Загальні положення дослідження, отримані висновки та обґрунтовані пропозиції використані та можуть у подальшому бути використані за такими напрямами:

– *науково-дослідна робота* – для наукових розробок проблемних аспектів окремих напрямів удосконалення кібербезпеки та формування національної системи кіберстійкості в Україні (акт впровадження в наукову діяльність Одеського державного університету внутрішніх справ від 15.01.2026 року);

– *правотворча діяльність* – для удосконалення законодавства, що регулює відносини у сфері кібербезпеки (довідка №89д9/10-2025/251968 від 03.11.2025 про впровадження у діяльності ВРУ при розроблені законопроекту № 12207 «Проект Закону про внесення змін до деяких законів України щодо удосконалення процедур нагляду за кібербезпекою та запровадженням європейських схем сертифікації кібербезпеки»);

– *правозастосовна діяльність* – для впровадження моделі стійкого правопорядку, що забезпечує перехід від констатації вчинених злочинів до проактивного виявлення латентних загроз та ідентифікації складних кримінальних схем, та передбачає вдосконалення координації суб'єктів національної системи кібербезпеки через автоматизований обмін даними про аномальну активність у реальному часі; методологія аналітичної розвідки має базуватися на інтеграції алгоритмів машинного навчання та предиктивного аналізу великих даних для виявлення транскордонних злочинних мереж, задіяних у гібридній війні, що посилює кіберстійкість суспільства шляхом підвищення інституційної спроможності органів правопорядку, впровадження стандартів безпеки на етапі проектування систем та мінімізації економічної привабливості кіберзлочинності;

– *освітній процес* – при викладанні навчальних дисциплін «Кримінально-правова та кримінологічна характеристика кіберзлочинності», «Інформаційна та кібернетична безпека», «Кримінальний аналіз», «Пошук інформації з відкритих джерел (OSINT) працівниками кримінальної поліції», «Протидія кіберзлочинності», при підготовці відповідних розділів підручників, навчальних посібників, програм, проведенні занять з професійної підготовки працівників оперативних підрозділів Національної поліції України (акт впровадження в освітній процес Одеського державного університету внутрішніх справ від 15.01.2026 року).

Апробація матеріалів дисертації. Основні положення дисертації апробовано на: XIV Міжнародній науково-практичній конференції «Безпекотворення: питання теорії, практики та правові аспекти» (м. Київ, 06 квітня 2023 р.), XV міжнародній науково-практичній конференції «Закарпатські правові читання» (м. Ужгород, 27 квітня 2023 р.), III Міжнародній науково-практичній інтернет-конференції з нагоди відзначення Дня науки – 2023 в Україні «Актуальність та особливості наукових досліджень в умовах воєнного стану» (м. Київ, 23 травня 2023 р.), науково-практичному круглому столі «Безпекова ситуація в Україні в умовах війни: стан,

загрози, напрями забезпечення» (м. Київ, 26 вересня 2023 р.), X Міжнародній науково-практичній інтернет-конференції «Стан та перспективи розвитку адміністративного права України» (м. Одеса, 20 жовтня 2023 р.), міжвідомчій науково-практичній конференції «Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України» (м. Київ, 17 листопада 2023 р.), Міжнародній науково-практичній конференції «Кібербезпека в Україні: правові та організаційні питання» (м. Одеса, 17 листопада 2023 р.), Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks «Management in Global Information Networks» (м. Велятино, 25 січня 2024 р.), Всеукраїнській науково-практичній конференції «Актуальні питання забезпечення безпекового середовища в Україні» (м. Київ, 19 квітня 2024 р.), IV Міжнародній науково-практичній інтернет-конференції з нагоди відзначення Дня науки-2024 в Україні «Актуальність та особливості наукових досліджень в умовах воєнного стану» (м. Київ, 22 травня 2024 р.), Всеукраїнській науково-практичній конференції «Безпекова ситуація в Україні в умовах війни: стан, загрози, напрями забезпечення безпеки» (м. Київ, 27 вересня 2024 р.), Міжнародній науково-практичній конференції «Протидія організованій злочинності і корупції в умовах збройного конфлікту: досвід та перспективи з нагоди 5-річчя створення Департаменту стратегічних розслідувань НПУ» (м. Кропивницький, 04 жовтня 2024 р.), Міжвідомчій науково-практичній конференції «Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України» (м. Київ, 01 листопада 2024 р.), круглому столі «Роль OSINT-досліджень у підвищенні рівня національної безпеки України» (м. Львів, 07 травня 2025 р.), Міжнародній науково-практичній конференції «Кримінальний аналіз і кібербезпека: об’єднання зусиль для нових викликів» (м. Одеса, 23 травня 2025 р.), Київському міжнародному форумі кіберстійкості (м. Київ, 19-20 лютого 2026 р.).

Публікації. Основні положення дисертації опубліковані в 33 наукових працях, з яких: 2 – одноосібні розділи колективних монографій, 18 – наукові статті в фахових виданнях (з яких 5 – у періодичних виданнях іноземних держав (фахові видання, включені до наукометричних баз Scopus, зокрема 2 – Q3 і 1 – Q1) та Web of Science), 13 – тези доповідей.

Особистий внесок. Дисертаційна робота виконана здобувачем самостійно. Викладені у дисертації положення, що виносяться на захист, розроблені ним особисто. У наукових працях, опублікованих у співавторстві, особистий внесок полягає у наступному:

- Demedyuk S.V., Demedyuk T.S. Dangerous pornographic content on the internet as a projection of a personality deviation of the child pornography distributor. *Information technologies and learning tools*. 2018. Vol. 68 № 6. P. 278-290 (досліджено кримінально-правовий контент насильства над дітьми в інтернеті);

- Korystin O., Korchenko O., Kazmirchuk S., Demediuk S., Korystin O. Comparative Risk Assessment of Cyber Threats Based on Average and Fuzzy Set Theory. *International Journal of Computer Network and Information Security*. 2024. Vol. 16. №. 1. P. 24-34 (сформовано та проаналізовано емпіричний матеріал дослідження, розкрито методологічні засади дослідження);

- Korystin O., Demediuk S., Sviridyuk N., Mitina O., Aleksander M., Yuriy Kardashevskyy. Risk Forecasting of Information-content-security. *Cyber Hygiene & Conflict Management in Global Information Networks*: Proceedings of the Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks. 2025. Vol. 3925. P. 273–280 (сформовано емпіричний матеріал дослідження, проаналізовано ризики поширення кіберзагроз та визначено пріоритетними ризики, пов'язані з інформаційною безпекою);

- Korystin O., Demediuk S., Likhovitskyy Y., Kardashevskyy Y., Mitina O. Priorities for the Strategic Development of Ukraine's Cybersecurity Based on the Analysis of Expert Sampling Patterns, *International Journal of Information Technology and Computer Science.* 2025. Vol. 17. No. 2. P. 24-35 (розкрито сутність окремих кіберзагроз, на основі інтерпретації статистичних та аналітичних даних обґрунтовано пріоритети стратегічного розвитку системи кібербезпеки в Україні);

- Korchenko O., Korystin O., Shulha V., Kazmirchuk S., Demediuk S., Zybin S. Sustainable Development of Smart Regions via Cybersecurity of National Infrastructure: A Fuzzy Risk Assessment Approach. *Sustainability*. (2025). Vol. 17. Is. 19. P. 8757 (сформовано емпіричний матеріал дослідження кібербезпеки критичної інформаційної інфраструктури, проаналізовано ризики та виділено пріоритетні кіберзагрози);

- Демедюк С.В., Користін О.Є. Стійкість системи кібербезпеки та її забезпечення в НАТО. *Наука і правоохорона.* 2023. № 1(59). С.77-85 (досліджено методологічні засади та досвід і стандарти НАТО у сфері забезпечення кіберстійкості);

- Користін О.Є., Демедюк С.В., Панченко Є.В., Користін О.О. Національні реалії аналізу кіберзлочинності за методологією Європолу ІОСТА. *Південноукраїнський правничий часопис*. 2023. № 3. С.53-59 (досліджено методологічні засади ІОСТА за матеріалами Європолу та інтерпретовано аналітичні висновки за окремими особливостями в описових статистиках);

- Користін О.Є., Демедюк С.В. Актуалізація кіберстійкості та історичні витоки концепції «стійкість». *Аналітично-порівняльне правознавство: електронне наукове фахове видання юридичного факультету ДВНЗ «Ужгородський національний університет»*. 2023. №06. С. 708-713 (проаналізовано окремі аспекти дослідженості концепції «стійкість» та щодо обґрунтування актуальності її розбудови в Україні);

- Демедюк С.В., Користін О.Є. Тенденції та характерні особливості on-line шахрайства в Україні. *Наука і правоохорона*. 2024. Том 3-4. № 65-66. С. 142-154 (проаналізовано ризики та інтерпретовано отримані статистичні результати й аналітичні висновки, що характеризують сучасні тенденції поширення on-line шахрайства в Україні).

Структура та обсяг дисертації визначені її метою і завданнями. Робота складається зі списку умовних позначень, анотації, вступу, чотирьох розділів, які об'єднують тринадцять підрозділів, висновків, списку використаних джерел (424 найменування на 49 сторінках), 4 додатків на 42 сторінках. Повний обсяг дисертації складає 525 сторінок, з яких основний текст – 412 сторінок.

ОСНОВНИЙ ЗМІСТ РОБОТИ

Вступна частина містить обґрунтування важливості обраної тематики, демонструє зв'язок дослідження з відповідними науковими програмами, планами та темами. У вступі сформульовано мету та завдання роботи, визначено об'єкт і предмет дослідження, описано застосовані методи дослідження. Розкрито наукову новизну отриманих результатів та їхнє практичне застосування, подано відомості про апробацію результатів дослідження, а також про висвітлення ключових положень і висновків дисертаційного дослідження у наукових публікаціях. Надано характеристику структури дисертаційної роботи.

У **Розділі 1. «Теоретико-методологічні засади розбудови національної кіберстійкості»** здійснено системний аналіз генезису та еволюції концепції «стійкість», обґрунтовано необхідність зміни парадигми від класичного захисту периметра до забезпечення життєздатності складних кіберфізичних систем, а також досліджено міжнародний досвід і нормативно-правову базу розбудови національних систем кіберстійкості.

У підрозділі 1.1 «Актуалізація кіберстійкості та історичні витоки концепції «стійкість» проведено генетико-морфологічний аналіз категорії «стійкість». Встановлено її міждисциплінарну природу, де сучасне розуміння кіберстійкості еволюціонувало від інженерної стійкості (здатність повертатися до вихідного стану) до екологічної та адаптивної стійкості (здатність трансформуватися під впливом шоків). Доведено, що актуалізація кіберстійкості у сучасному безпековому дискурсі зумовлена неспроможністю традиційних методів кібербезпеки гарантувати повну цілісність систем в умовах складних цілеспрямованих атак. Автор визначає кіберстійкість як емерджентну властивість системи, що дозволяє їй не лише витримувати деструктивні впливи, а й забезпечувати виконання критичних функцій під час та після інциденту.

У підрозділі 1.2 «Концептуальні основи та функціональні компоненти кіберстійкості» детерміновано архітектурні складники стійкості та механізми їх реалізації. Науково обґрунтовано чотирьохкомпонентну функціональну модель, що включає здатності системи: передбачати загрози; витримувати активний вплив; відновлюватися до стабільного стану; адаптуватися через інтеграцію отриманого досвіду в оновлені захисні механізми. Особливу увагу приділено розмежуванню понять «кібербезпека» та «кіберстійкість». Аргументовано, що стійкість визнає неминучість компрометації систем і акцентує увагу на мінімізації каскадних ефектів та швидкості відновлення. Обґрунтовано роль адаптивних технік (диверсифікація, сегментація, обманні технології) як інструментів підвищення «вартості атаки» для зловмисника.

У підрозділі 1.3 «Нормативно-правове та стратегічне забезпечення національної кіберстійкості» проаналізовано світові стандарти (зокрема фреймворки NIST, MITRE, ISO та Директиви ЄС) і вітчизняне законодавство у сфері захисту критичної інфраструктури. Виявлено, що розбудова національної системи кіберстійкості потребує переходу до моделі «спільної відповідальності». Доведено необхідність впровадження ризик-орієнтованого підходу на державному рівні, де

пріоритетність захисту визначається соціально-економічною значущістю цифрових сервісів. За результатами аналізу встановлено, що ключовим викликом залишається відсутність єдиної системи метрик для кількісного оцінювання стану стійкості на різних рівнях управління, що визначає подальший вектор дослідження.

Розділ 2. «Організаційно-правові напрями та зміст інституалізації кіберстійкості» охоплює три підрозділи.

У підрозділі 2.1 «Інституціоналізація кіберстійкості» розкрито теоретико-методологічні засади переходу від класичної парадигми кібербезпеки до концепції кіберстійкості як здатності системи до адаптації та швидкого відновлення. Обґрунтовано, що інституціоналізація кіберстійкості розглядається як багатовимірний процес формування стійких спроможностей держави, бізнесу та суспільства до протидії, відновлення та адаптації до кіберзагроз. Встановлено, що сучасні підходи до кіберстійкості реалізуються через поєднання трьох ключових інституційних механізмів: маркетингового, який формує економічні стимули та попит на безпеку; стандартизаційного, що забезпечує уніфікацію підходів і практик; та регуляторного, який встановлює обов'язкові вимоги і контроль. Доведено, що ефективність кіберстійкості визначається не окремими заходами, а узгодженістю цих механізмів у межах єдиної системи кіберуправління.

Особливу увагу приділено аналізу Директиви ЄС NIS2 як каталізатора нормативних змін, що запроваджує інститут персональної відповідальності керівництва та суворі регламенти звітування про інциденти. Доведено, що поєднання ринкових стимулів (зокрема кіберстрахування) із жорстким державним регулюванням створює самоадаптивне середовище, здатне мінімізувати наслідки критичних деструктивних впливів у цифровій сфері.

На прикладі України обґрунтовано функціональну модель розподілу повноважень між ключовими суб'єктами, що забезпечує комплексне охоплення процесів кіберстійкості, з урахуванням європейських підходів до регулювання та захисту критичної інфраструктури.

У підрозділі 2.2 «Суб'єктний склад та міжнародний контекст формування системи кіберстійкості» здійснено комплексний аналіз організаційної структури національної системи кібербезпеки України. Автором проведено функціональне розмежування повноважень ключових суб'єктів відповідно до визначених інституційних підходів: регулювання (Держспецзв'язку), стандартизація (НКЦК при РНБО) та маркетингове стимулювання (Мінцифра). Встановлено, що НКЦК трансформується у стратегічний методологічний хаб, що забезпечує єдність підходів до оцінки ризиків на загальнодержавному рівні. У роботі доведено високу ступінь міжнародної суб'єктності України, яка в умовах відсічі повномасштабній збройній агресії перетворилася на ключового контрибутора глобальної безпеки. Обґрунтовано значущість інтеграції до Об'єднаного центру передових технологій з кібероборони НАТО (CCDCOE) та мережі CSIRTs, що дозволяє легітимізувати унікальний український досвід як основу для розробки новітніх євроатлантичних стандартів стійкості.

У підрозділі 2.3 «Організаційно-правові механізми цивільно-військового співробітництва у формуванні національної системи кіберстійкості»

аргументовано, що в умовах гібридної війни цивільно-військове співробітництво (Cyber-CIMIC) стає системоутворюючим чинником національної оборони. Визначено дефініцію «Cyber-CIMIC» як багаторівневу систему інтеграції спроможностей сектору безпеки і оборони, приватних технологічних компаній та волонтерських кіберспільнот. Доведено, що існуюча нормативна база України містить «термінологічний розрив», оскільки фактичні механізми залучення цивільних фахівців до кібероборони не мають належної юридичної легітимізації.

Здійснено порівняльний аналіз моделі CIMIC НАТО та українського досвіду, на основі чого запропоновано перехід від лінійної моделі взаємодії до мережевої екосистеми, що об'єднує ресурси сектору безпеки, приватного бізнесу та волонтерських спільнот. Встановлено, що оптимальна модель «Cyber-CIMIC» передбачає дворівневу інтеграцію: нормативну – через законодавче закріплення інтегрованого принципу взаємодії у профільному законі, та організаційну – шляхом створення постійних координаційних механізмів при НКЦК. Розроблено пакет концептуальних змін до Закону України «Про основні засади забезпечення кібербезпеки України», які передбачають: законодавче закріплення поняття «Cyber-CIMIC»; інституціоналізацію ролі НКЦК як стратегічного хабу; впровадження інституту «цивільного кіберрезерву» як механізму гнучкої мобілізації фахівців; створення правових «регуляторних пісочниць» для реалізації спеціальних правових режимів, що стимулюють обмін даними про кіберзагрози на юридичні преференції. Сформульовано конкретні правки до профільного законодавства, які дозволяють легітимізувати участь цивільних експертів у кібероборoні держави («цивільні асистенти»), забезпечуючи при цьому сумісність із доктринами НАТО та дотримання норм міжнародного гуманітарного права в цифровому просторі.

У третьому розділі «Аналітична розвідка стратегічних напрямів кіберстійкості в Україні» здійснено комплексний аналіз перспективних векторів розвитку національної системи кібербезпеки, обґрунтовано методологічні засади стратегічного планування та розроблено концептуальні засади нормативно-правового зміцнення стійкості держави.

У *підрозділі 3.1 «Методологія та процес аналітичної розвідки стратегічних напрямів кіберстійкості в Україні»* обґрунтовано концепцію аналітичної розвідки як цілісного інтелектуального циклу трансформації розрізнених первинних даних у верифіковані стратегічні знання для прийняття обґрунтованих управлінських рішень. Автор доводить, що в умовах динамічних загроз сучасна методологія забезпечення кіберстійкості України має базуватися на стійкій синергії трьох взаємодоповнюючих компонентів: OSINT, форсайту та ризик-орієнтованого підходу.

Використання OSINT (Open Source Intelligence) виступає джерелом фактологічної точності в режимі реального часу, забезпечуючи глибинний моніторинг цифрового простору, ідентифікацію тактик супротивника та верифікацію гіпотез на ранніх стадіях інцидентів. Впровадження методів стратегічного форсайту розширює горизонт планування через предиктивне моделювання альтернативних сценаріїв майбутнього та виявлення «слабких сигналів» нових технологічних викликів, що дозволяє перейти від реактивного

захисту до проактивної розбудови архітектури безпеки. Ключовим інтегратором цієї системи стає ризик-орієнтований підхід (згідно зі стандартом ISO 31000), який на основі оцінювання ймовірності та потенційного впливу загроз забезпечує чітку ієрархію пріоритетів і раціональний розподіл державних ресурсів.

Така методологічна синергія формує модель інтелектуальної стійкості, де поєднання інформаційної повноти розвідки, стратегічного прогнозування та прагматичного управління ризиками гарантує високу адаптивність національної системи кібербезпеки до каскадних ефектів у критичній інфраструктурі.

Особливу увагу приділено результатам дослідницького проєкту 2024 року, у межах якого проведено комплексне оцінювання 1025 індикаторів кіберзагроз. Через застосування аналітичного інструментарію та впровадження авторських фільтрів логічної надійності, було верифіковано експертну думку та виявлено статистично значущу варіативність у сприйнятті ризиків залежно від фахового досвіду та галузевої приналежності респондентів.

Дослідження підтверджує, що в умовах гібридної агресії ефективність кіберзахисту залежить від здатності системи виявляти «слабкі сигнали» та адаптувати архітектуру безпеки до каскадних ефектів у критичній інфраструктурі.

Підрозділ 3.2 «Обґрунтування стратегічних напрямів кіберстійкості на основі аналізу кіберзагроз» присвячено емпіричному обґрунтуванню стратегічних векторів кіберстійкості України на основі ризик-орієнтованого аналізу. Автор класифікує та детально досліджує шість доменів кіберзагроз: від порушення базових характеристик безпеки до використання кібератак як інструментів гібридної війни та кібертероризму.

На основі статистичних даних виявлено, що найвищий рівень ризику зафіксовано в енергетичному (73,5%) та оборонно-промисловому (70,6%) комплексах. Особливу увагу приділено психологічному аспекту сприйняття загроз: встановлено, що досвідчені фахівці дають більш зважені прогнози щодо деструктивних ІПСО, покладаючись на інституційну стійкість Сил оборони, тоді як менш досвідчені кадри гостріше реагують на загрози дискредитації влади. Сформовано цілісну систему стратегічних пріоритетів, яка включає посилення захисту КІ, впровадження технологій раннього попередження (ШІ, Big Data), адаптацію політик до умов цифрової трансформації та розвиток національної кіберрозвідки.

Успішна реалізація цих напрямів неможлива без конвергенції досвіду та розвитку людського капіталу, що передбачає синергію між «техноцентричним» баченням молодих фахівців та стратегічною глибиною експертів зі стажем понад 10 років. Кінцевим етапом розбудови стійкості є нормативно-правова інтеграція ризик-орієнтованого підходу у державну політику, що забезпечить раціональний розподіл ресурсів та зміцнить міжнародну суб’єктність України як лідера у сфері відбиття гібридних загроз.

Підрозділ 3.3 «Методологічні засади та діагностика кіберстійкості національної інформаційної інфраструктури» присвячено розробці та впровадженню методологічного інструментарію діагностики кіберстійкості як емерджентної властивості гетерогенних мереж. Автор здійснює чітке термінологічне

розмежування понять «надійність», «вразливість» та «стійкість», доводячи, що стратегія кіберстійкості спрямована на забезпечення безперервності критичних процесів навіть за умови успішної експлуатації вразливостей.

Центральне місце в роботі посідає Матриця кіберстійкості, побудована на синергії функцій: планування, поглинання, відновлення, адаптація, - та доменів: фізичний, інформаційний, когнітивний, соціальний. Емпіричне наповнення матриці дозволило виявити динамічний профіль стійкості національної інфраструктури, де середні значення показників коливаються в межах 51,7–55,1%. Аналіз підтвердив тезу про «інформаційну домінантність» системи (пріоритет рекуперації даних) та виявив «соціальну інерцію» – сповільнене відновлення організаційних зв'язків порівняно з технічними компонентами. Запропонований підхід перетворює розрізнені технічні метрики у цілісну модель підтримки державних рішень у сфері захисту критичної інфраструктури.

Підрозділ 3.4 «Прикладний аналіз системних спроможностей та правові орієнтири забезпечення кіберстійкості інформаційної інфраструктури» присвячено прикладному дослідженню інституційної спроможності як динамічної характеристики системи протидії кіберзагрозам. Автор аналізує неоднорідний ландшафт спроможностей України, де середні значення варіюються від 44,5% до 66,3%, ідентифікуючи зони системної вразливості, зокрема на муніципальному та індивідуальному рівнях.

Особливу увагу приділено суб'єктно-рівневому дисонансу: виявлено розрив між експертним оптимізмом представників керівних ланок та певним скептицизмом науковців щодо реального стану захищеності периферійних вузлів. У роботі запропоновано перехід до нормотворення на основі фактичних даних, що передбачає юридичну трансформацію виявлених вразливостей у нормативно закріплені спроможності. Сформульовано пропозиції щодо впровадження інституту «муніципального офіцера з кібербезпеки» та легалізації етичних досліджень вразливостей як інструментів зміцнення національної екосистеми кіберстійкості.

У четвертому розділі «Пріоритети стратегічного забезпечення протидії кіберзлочинності» досліджено сучасний стан та тенденції розвитку злочинності у цифровому середовищі, визначено методологічні підходи до її аналізу та обґрунтовано стратегічні вектори мінімізації кримінальних загроз у кіберпросторі.

Підрозділ 4.1 «Сучасні методологічні засади виявлення та аналізу кіберзлочинності» присвячено розробці та апробації методологічного каркаса розслідування кіберзлочинів, який інтегрує обчислювальні методи (текст-майнінг, машинне навчання, аналіз вузлів) із традиційними кримінологічними підходами. Автор класифікує методи розслідування на три ключові рівні: аналіз соціальних мереж (для виявлення сучасних трендів та наслідків неправомірної поведінки), Data Mining (для пошуку шаблонів та типології злочинної діяльності у великих масивах даних) та статистичний аналіз.

Особливий акцент зроблено на адаптації методології IOCTA (Internet Organised Crime Threat Assessment) до українських реалій. Емпіричну базу дослідження склало суцільне опитування фахівців Кіберполіції України з використанням верифікаційних фільтрів надійності. Результати аналізу демонструють перевагу юридичної освіти

серед кадрів (69%) при поступовому нарощуванні технічної експертизи (22%). Дослідження підтверджує, що ефективна протидія «справжній» кіберзлочинності (хакерство, DDoS) та «електронним» злочинам (шахрайство) потребує переходу до предиктивних моделей, де ризик розглядається як набір способів прийняття рішень у правоохоронній діяльності.

Підрозділ 4.2 «Виклики та пріоритетні напрями стратегічного забезпечення протидії кіберзлочинності в Україні» присвячено емпіричному аналізу ландшафту кіберзлочинності в Україні, класифікованому за чотирма напрямами: втручання в комп'ютерні мережі, протиправний контент, банківські злочини та платіжне шахрайство. Автор порівнює дані експертного опитування з офіційною статистикою ЄРДР, виявляючи зони високої латентності та специфіку суб'єктів посягання, де найбільших збитків (у окремих випадках понад 1 млрд грн) зазнають фізичні особи та державний сектор.

Досліджено інструментарій кіберзлочинців, де ключовими джерелами шкідливого ПЗ визначено соціальні мережі та форуми Даркнету, а основними векторами атак – фішинг (52,3%) та несанкціоноване зняття готівки (63,7%). Особлива увага приділена мотиваційному аспекту: поряд із домінуючим прагненням до наживи (понад 60%), зафіксовано стійкий тренд використання кіберзлочинності як інструменту гібридної агресії рф. Сформовано прогнозні оцінки ризиків на післявоєнний період, де пріоритетними загрозами визначено шахрайство з конвертацією криптовалют та фішингові кампанії з використанням скомпрометованих платіжних інструментів.

У підрозділі 4.3 «Ризики поширення кримінальних загроз у кіберпросторі». Оцінено ризики використання технологій анонімізації та криптоактивів для легалізації доходів, отриманих злочинним шляхом. Доведено, що поширення кримінальних загроз безпосередньо корелює із системними прогалинами у міжнародному співробітництві, що потребує розробки нових правових механізмів для оперативного подолання юрисдикційних бар'єрів у транскордонних розслідуваннях.

Розділ присвячено дослідженню інфраструктурних та операційних аспектів сучасної кіберзлочинності та здійснено комплексний аналіз загрозового ландшафту, акцентуючи увагу на експансії Інтернету речей (IoT) та соціальної інженерії.

Розкрито механізми функціонування кримінальних онлайн-ринків, де Darknet виступає платформою для торгівлі не лише наркотиками (ризик 40,3%) та зброєю, а й шкідливим ПЗ та скомпрометованими персональними даними. Особливу увагу приділено методам анонімізації, де VPN-сервіси (53,4%) та мережа Tor визначені як базові інструменти приховування злочинної діяльності.

Досліджено роль соціальної інженерії (фішинг, вішинг, смішинг) як основного методу обходу технічних систем захисту, що використовується у 60% атак. Виявлено нові вектори загроз, пов'язані з Інтернетом речей (IoT), де вразливі смарт-пристрої інтегруються у ботнети для проведення масштабних DDoS-атак. Сформовано прогнозний профіль фінансової активності на післявоєнний період, що вказує на збереження високих ризиків відмивання коштів через децентралізовані платформи та електронні гроші (EasyPay, PayPal).

ВИСНОВКИ

За результатами дослідження вирішено наукову проблему щодо розбудови національної системи кіберстійкості в Україні та зроблено такі висновки:

1. Дослідження генезису концепції «стійкості» підтверджує її міждисциплінарну природу та визначає еволюційний перехід від статичних інженерних моделей (повернення до вихідного стану) до динамічних екологічних та адаптивних систем (здатність до трансформації).

Теоретичним підґрунтям сучасної кіберстійкості визначено зміну парадигми: від спроб побудови «непроникного захисту» до створення емерджентних властивостей системи, що забезпечують її функціонування в умовах неминучих інцидентів. Ключовим результатом еволюції є перехід до «динамічної адаптивності» та принципу «граціозної деградації», де стійкість розглядається не як стабільний стан, а як безперервний процес навчання, самоорганізації та підтримки критичних функцій під час складних кібератак. Таким чином, кіберстійкість обґрунтовано як якісно новий етап системної інженерії, що базується на управлінні ризиками в умовах високої невизначеності.

2. Розмежування понять дозволило встановити їхню комплементарну природу: якщо «кібербезпека» зосереджена на мінімізації ймовірності реалізації загрози, то «кіберстійкість» визнає неминучість компрометації та фокусується на підтримці життєздатності системи й мінімізації наслідків інцидентів.

В основі цієї нової парадигми лежить інтегрована чотирьохкомпонентна модель, яка включає спроможності передбачати загрози через проактивний аналіз, витримувати деструктивні впливи без втрати критичних функцій, оперативно відновлюватися до стабільного стану та адаптуватися шляхом трансформації архітектури на основі отриманого досвіду. Функціональний взаємозв’язок цих компонентів формує безперервний цикл самоорганізації, де фаза адаптації стає підґрунтям для нового етапу передбачення. Ключовим елементом цієї парадигми є зміщення акценту з «непроникності» на життєздатність системи, де через механізми адаптивної диверсифікації, сегментації та обманних технологій досягається критичне підвищення «вартості атаки» для зловмисника. Таким чином, кіберстійкість визначено як стратегічну характеристику, що забезпечує виконання критичних функцій навіть за умов часткового успіху атаки, перетворюючи досвід інцидентів на оновлені механізми самоорганізації та захисту.

3. Аналіз світового досвіду свідчить про глобальну трансформацію парадигми захисту: від пасивної «кібербезпеки» до активної «кіберстійкості», що базується на визнанні неминучості інцидентів та здатності системи зберігати життєздатність під час атак.

Дослідження підтверджує, що успішні національні моделі розбудови кіберстійкості базуються на трьох фундаментальних принципах, які утворюють цілісну систему захисту. Першим складником є нормативна обов’язковість, що на прикладі досвіду ЄС демонструє перехід від добровільних рекомендацій до жорсткого регулювання відповідальності виробників цифрових продуктів та безпеки ланцюгів постачання. Другим принципом виступає технологічна адаптивність, реалізована в моделі США через впровадження інженерних стандартів NIST та

архітектури «нульової довіри», які забезпечують швидке відновлення їхніх критичних функцій. Третім ключовим елементом є соціотехнічна синергія, притаманна досвіду Великої Британії, що передбачає розбудову «колективної стійкості» через розвинене публічно-приватне партнерство та активне залучення людського капіталу на всіх рівнях – від загальнодержавного до регіонального.

Для України пріоритетним визначено шлях творчого синтезу: адаптація європейського права для сертифікації продуктів, імплементація американських технічних стандартів для захисту промислових систем та впровадження британських моделей регіональної стійкості. Такий інтегрований підхід дозволить Україні трансформувати досвід відсічі збройній агресії у стійку цифрову екосистему, здатну не лише витримувати сучасні кібершоки, а й виступати гарантом безпеки в європейському цифровому просторі.

4. Доведено, що інституціоналізація кіберстійкості є не лінійним впровадженням окремих технічних або організаційних заходів, а системним процесом інтеграції різнорідних інструментів управління кіберризиками, а також є процесом переходу від статичного захисту до динамічної моделі адаптації та відновлення систем. Обґрунтовано, що домінуючі міжнародні підходи (зокрема стандарти та галузеві практики) мають обмеження, пов’язані з відсутністю пріоритезації заходів і надмірною технократичністю, що знижує їх адаптивність до кризових умов. Доведено, що найбільш ефективною є модель, яка поєднує нормативний вплив держави, економічні стимули ринку та методологічну підтримку стандартів, забезпечуючи баланс між примусом і саморегуляцією.

Встановлено, що ключовим елементом сучасної інституціоналізації є імплементація стандартів Директиви NIS2, яка впроваджує жорстку відповідальність керівництва та обов’язковість звітування про інциденти. Це дозволяє трансформувати кіберстійкість із вузькотехнічного завдання на стратегічний компонент державного управління. Такий підхід створює умови для формування «культури стійкості», де кожен суб’єкт господарювання стає активним учасником системи національної безпеки, що підвищує загальну адаптивність критичної інфраструктури до гібридних загроз.

5. Дослідження суб’єктного складу підтвердило формування в Україні багаторівневої ієрархічної системи, де НКЦК при РНБО виконує роль стратегічного координатора та методологічного хабу. Встановлено чіткий розподіл функцій: Адміністрація Держспецзв’язку реалізує регуляторні завдання, НКЦК забезпечує стандартизацію, а Мінцифра стимулює ринкові механізми розвитку галузі. Особливу увагу приділено міжнародній суб’єктності України, яка в умовах повномасштабної війни трансформувалася з реципієнта технологій на ключового донора практичного досвіду. Участь у CCDCOE НАТО та мережі CSIRT легітимізує українські протоколи відсічі агресії як основу для майбутніх міжнародних стандартів колективної стійкості. Зроблено висновок, що сучасна архітектура суб’єктів забезпечує інституційну цілісність системи, дозволяючи ефективно поєднувати національні оборонні спроможності з міжнародними механізмами взаємодії у кіберпросторі.

6. У ході дослідження доведено, що цивільно-військове співробітництво є

фундаментом національної кіберстійкості, що трансформує класичну модель CIMIC у гнучку мережеву екосистему. Виявлено термінологічну прогалину в українському правовому полі, де фактична взаємодія суб'єктів у кіберпросторі випереджає її законодавче закріплення. Сформовано авторське визначення дефініції «Cyber-CIMIC» та розроблено стратегічні правки до Закону України «Про основні засади забезпечення кібербезпеки України». Запропоновані зміни дозволяють інституціоналізувати роль НКЦК як стратегічного хабу, легалізувати статус волонтерських ІТ-спільнот та впровадити економічні стимули, такі як «регуляторні пісочниці», для приватних операторів критичної інфраструктури. Ефективність моделі «Cyber-CIMIC» забезпечується синергією між військовою спроможністю, державним регулюванням та інноваційним потенціалом приватного сектору. Реалізація цих підходів забезпечить перехід від ситуативної координації до системної інтеграції ресурсів, що підвищить адаптивність держави до гібридних загроз, дозволить трансформувати практичний досвід у глобальні стандарти безпеки нового покоління та забезпечить сумісність із євроатлантичними стандартами безпеки.

7. Сучасне методологічне забезпечення кіберстійкості України ґрунтується на синергії OSINT, форсайту та ризик-орієнтованого підходу, що дозволяє трансформувати систему захисту з реактивної у проактивну та адаптивну. Використання OSINT виступає фундаментом інформаційної актуальності, забезпечуючи аналітичну розвідку верифікованими даними з відкритих джерел для миттєвого реагування на поточні загрози та розуміння тактик супротивника. Впровадження методів форсайту розширює горизонт планування, дозволяючи через сценарне моделювання та аналіз «слабких сигналів» конструювати альтернативні варіанти майбутнього та випереджати технологічні виклики. Ключовим інтегратором цієї системи стає ризик-орієнтований підхід (згідно зі стандартом ISO 31000), який на основі математико-статистичного аналізу експертних оцінок забезпечує об'єктивну пріоритезацію ресурсів та мінімізацію потенційних наслідків. Таким чином, поєднання фактологічної точності розвідки, стратегічного прогнозування та прагматичного управління ризиками формує цілісну модель інтелектуальної стійкості держави, здатну до еволюційного самовідновлення в умовах постійної гібридної агресії.

8. На основі проведеного ризик-орієнтованого аналізу та верифікації експертних оцінок, стратегія кіберстійкості України має трансформуватися з моделі фрагментарного технічного захисту в цілісну систему національної відмовостійкості. Ключовим стратегічним пріоритетом визначено гібридизацію та ешелонований захист критичної інфраструктури, що передбачає впровадження моделі «системної різноманітності», де цифровізація енергетичного та оборонного комплексів обов'язково поєднується з модернізацією аналогових систем як останньої лінії оборони від кібертерористичних атак.

Паралельно з цим, стратегія фокусується на впровадженні інтелектуального моніторингу та предиктивної аналітики, де використання технологій штучного інтелекту та аналізу великих даних дозволяє перейти від реактивного реагування на інциденти до завчасного виявлення «слабких сигналів» кібершпигунства. Важливою

складовою цієї моделі є протидія когнітивним загрозам та деструктивним ІПСО, оскільки високий ризик використання кібератак для дискредитації влади та розколу суспільства вимагає створення єдиної екосистеми контрпропаганди та захисту інформаційного простору Сил оборони України.

9. Розроблено та практично застосовано матрицю показників кіберстійкості, яка дозволила кількісно оцінити стан вітчизняної кіберінфраструктури. Діагностика виявила формування «техноцентричної моделі стійкості», де технічні та інформаційні домени (середній показник ~55%) випереджають управлінські та соціальні механізми (51–52%). Встановлено, що найбільш критичною ланкою є етап планування в соціальному домені (51,75%), що вказує на дефіцит міжвідомчої координації. Водночас найвищу ефективність система демонструє на стадії відновлення інформаційного домену (55,14%) та в процесах адаптації, що підтверджує здатність національної інфраструктури ефективно навчатися на реальних інцидентах і трансформувати досвід атак у стратегічний актив.

10. Доведено концептуальну перевагу моделі «нарощування спроможностей» над пасивною моделлю «фіксації вразливостей». Емпіричний аналіз зафіксував диспропорцію між високим рівнем захищеності центральних вузлів інформаційної інфраструктури (спроможність > 59%) та низькою витривалістю регіональних систем і приватного сектору (ризик на місцевому та індивідуальному рівнях < 50%), що свідчить про глибокий безпековий розрив. Виявлено «страх інновацій» у регуляторних органах (низька мотивація до нетрадиційного оповіщення - 34–46%) та критичний стан наукового забезпечення (ризик < 46%). Обґрунтовано пакет правових реформ, що включає дефініцію «кіберстійкості» у базовому законі, створення регіональних центрів стійкості при ОВА, декриміналізацію етичного хакінгу та запровадження Державного фонду кіберінновацій для реанімації наукового циклу.

Розроблено та представлено авторську концепцію «стійкість через право», яка передбачає перехід від декларативного регулювання до юридичної фіксації чотирьох функціональних спроможностей суб’єктів: *передбачення, витримування, відновлення та адаптація*. Запропоновано конкретні кроки щодо гармонізації українського законодавства із Директивою ЄС NIS2, зокрема в частині легалізації адаптивного управління ризиками та залучення спільноти етичних дослідників до зміцнення критичної інфраструктури.

11. Аналіз сучасних методологічних засад виявлення та аналізу кіберзлочинності дозволяє стверджувати, що трансформація злочинної діяльності у цифровому просторі вимагає радикального перегляду традиційних підходів до кримінологічного моніторингу. Сучасна методологія повинна базуватися на комплексному поєднанні технічного аналізу (цифрова криміналістика) та соціально-поведінкових досліджень та забезпечувати перехід від пасивної фіксації кіберзлочинів до динамічного управління ризиками.

Важливим аспектом є визнання того, що цифрові докази є надзвичайно волатильними, що потребує впровадження інструментів динамічного аналізу в режимі реального часу. Методологічний апарат має включати моделі предиктивного аналізу, які дозволяють ідентифікувати аномальну активність ще до моменту

настання тяжких наслідків. Таким чином, методологічне оновлення стає фундаментом для побудови дієвої системи стратегічного прогнозування ландшафту загроз, де першочерговим завданням є перехід від реактивної фіксації подій до проактивного виявлення латентних загроз та ідентифікації складних злочинних схем.

Застосування багаторівневої системи фільтрації експертних даних дозволило шляхом відсіювання логічних помилок підвищити якість вибірки та виявити реальні статистичні розбіжності у сприйнятті загроз (наприклад, щодо активності в Darknet та відмивання коштів). Доведено, що використання методів Data Mining, аналізу соціальних мереж та регресійного моделювання в поєднанні з експертною думкою забезпечує репрезентативність аналізу навіть в умовах високої анонімності та транскордонності кіберзлочинного середовища.

12. У ході дослідження ідентифіковано on-line шахрайство як найбільш масовий вид кіберзлочину (36% від загальної сукупності), причому 84% таких діянь кваліфікуються за частинами 3 та 4 ст. 190 ККУ. Виявлено домінування операційної системи Kali Linux (41% при втручаннях у системи) та програмного забезпечення для Brute-force і DoS-атак. Встановлено критично високий рівень організованості злочинності: понад 70% випадків розповсюдження дитячої порнографії та 50% несанкціонованих втручань вчиняються у складі ОЗУ. Аналіз підтвердив кореляцію між досвідом експертів та оцінкою ризиків, а також зафіксував значну частку злочинів (до 17%), що мають ознаки співпраці з агресором у межах гібридної війни.

Логіка розвитку протидії кіберзлочинності вимагає переходу до моделі «стійкого правопорядку», де юридичні норми є гнучкими та адаптивними до технологічних змін, а правоохоронна діяльність інтегрована в загальну архітектуру національної безпеки. Тільки такий інтегрований підхід дозволить Україні не лише ефективно розслідувати злочини, а й формувати безпечне цифрове середовище, здатне витримувати цілеспрямований тиск з боку як організованої злочинності, так і ворожих державних акторів.

13. Встановлено, що фінансова мотивація є ключовим драйвером кіберзлочинності (50-60%), де домінують шахрайства з платежами (67,1%). Виявлено стійку ієрархію криптоінструментів, де Bitcoin залишається лідером для розрахунків (54,9%) та вимагання викупу, тоді як Monero та Zcash набирають популярності через підвищену анонімність. Доведено, що грошові мули (дропи) є критичною ланкою у процесі переведення активів у фіат (60,9%). Аналіз активності в Darknet підтвердив високу затребуваність криптопрограм (44,3%) та банківських даних (50%), а вивчення каналів комунікації показало домінування Telegram (66%) у взаємодії «злочинець-жертва» та форумів Deep Web (46%) у розрахунках між зловмисниками. Аналіз показує, що кіберзлочинці все частіше поєднують технічні вразливості з методами соціальної інженерії, що робить людський фактор найбільш критичною ланкою в системі захисту.

Подальше стратегічне планування повинно враховувати адаптивність злочинних угруповань, які швидко опановують новітні технології (штучний інтелект, дипфейки) для автоматизації фішингу та створення шкідливого ПЗ. У цьому контексті важливою є розбудова національної системи кібергігієни та

підвищення обізнаності громадян, оскільки індивідуальна вразливість трансформується у колективний ризик для всієї держави. Водночас, через посилення інституційної спроможності правоохоронних органів у поєднанні з жорстким контролем за обігом криптовалют та інших засобів анонімізації доходів можна досягти суттєвого зниження економічної привабливості кіберзлочинності.

14. Проведено критичний огляд законодавчого поля України, за результатами якого сформовано пропозиції щодо удосконалення нормативно-правового регулювання із врахуванням сучасних глобальних викликів та, пов'язаних із воєнною агресією та кібервійною проти України, а також спрямованих на гармонізацію вітчизняних стандартів із Директивою ЄС про мережеву та інформаційну безпеку (NIS2), зокрема:

1) до Закону України «Про основні засади забезпечення кібербезпеки України»:

додати статтю 1 пунктом такого змісту: «*цивільно-військове співробітництво у сфері кібербезпеки (Cyber-CIMIC) – система заходів з організації взаємодії між суб'єктами сектору безпеки і оборони, державними органами, приватним сектором та громадянським суспільством задля підвищення національної кіберстійкості, захисту критичної інформаційної інфраструктури та спільної відсічі кібератрегресії*»;

частину другу статті 5 доповнити словами: *«…здійснює координацію цивільно-військового співробітництва у сфері кібербезпеки на стратегічному рівні, забезпечуючи інтеграцію спроможностей волонтерських кіберспільнот та приватних технологічних компаній до загальної системи спротиву;…*»;

доповнити статтю 8:

частиною восьмою: «*Суб'єкти приватного сектору, що залучаються до заходів цивільно-військового співробітництва, отримують право на використання спеціальних правових режимів («регуляторних пісочниць») за умови забезпечення автоматизованого обміну даними про кіберінциденти з державними центрами реагування (CERT-UA) та дотримання стандартів сумісності НАТО»*;

а також частиною девятою: «*Запровадити інститут добровільного кіберрезерву як форми реалізації цивільно-військового співробітництва, що передбачає залучення цивільних фахівців на договірній основі до виконання завдань з кібероборони без обов'язкового набуття статусу військовослужбовця, із визначенням меж їхньої юридичної відповідальності та соціального захисту*»;

2) внести зміни до Закону України «Про захист прав споживачів»: *закріпити «Права на кіберзахист» як базового цифрового права* та *запровадити концепцію «мінімального гарантованого рівня цифрової безпеки»* для забезпечення обов'язкової відповідності цифрових продуктів і послуг стандартам кіберстійкості;

3) внести зміни до КПК України та законів про ОРД, контррозвідувальну та розвідувальну діяльність, які б дозволили *залучати наукові установи як офіційних експертних контріб'юторів до аналізу складних кіберінцидентів*;

4) прийняти Закон України «Про стимулювання інновацій у сфері кібербезпеки та кіберстійкості». Юридичний механізм має передбачати створення Державного фонду кіберінновацій, наповнення якого здійснюватиметься шляхом фіксованих відрахувань від ліцензійних зборів у сфері телекомунікацій та штрафів за порушення

законодавства про захист персональних даних. Крім того, доцільним є законодавче закріплення частки (не менше 1%) бюджетних призначень сектору безпеки та оборони на проведення НДДКР (науково-дослідних та дослідно-конструкторських робіт) виключно за напрямом кіберстійкості. Це дозволить перетворити фінансування з «залишкового» на «пріоритетне».

4) розробити та затвердити на рівні Кабінету Міністрів України

Типове положення про цифрову безпеку територіальної громади, яке б визначало обов'язковий перелік заходів із захисту реєстрів та комунальних сервісів;

Порядок функціонування національних наукових кібер-полігонів, що забезпечить науковцям правовий доступ до знеособлених масивів даних про реальні атаки для розробки прогнозних моделей, що є відповідю на потребу в когнітивній адаптації;

правовий інститут «муніципального офіцера з кібербезпеки» або делегування цих функцій спеціалізованим сервісним центрам на умовах аутсорсингу, що дозволить вирішити проблему кадрового дефіциту в регіонах;

механізм «субвенцій на кіберстійкість» – цільового фінансування з державного бюджету для технічного переоснащення найбільш вразливих громад;

механізм «Кібер-ваучерів» – державної субсидії для малих підприємств на отримання базових консультацій або аудитів від акредитованих приватних компаній;

внести зміни до освітніх стандартів та трудового законодавства щодо обов'язкового періодичного тестування працівників державного сектору та критичної інфраструктури закріпити, статус «цифрової грамотності» як компонента цивільного захисту;

юридичного статусу «міждисциплінарних освітньо-наукових центрів кіберстійкості» (Cyber Resilience Hubs) на базі провідних ЗВО.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, у яких опубліковано основні наукові результати дисертації

Монографії

1. Демедюк С.В. Розділ 26. Кібервійна та форсайт кіберстійкості. Реалізація філософії ILP в системі кримінального аналізу Національної поліції України: монографія / О.Є. Користін, Б.А. Денисенко, С.В. Демедюк та ін. ; за заг. ред. д-ра юрид. наук, проф. О.Є. Користіна. Київ: ВАЙТЕ, 2024. С. 343-357. DOI: https://doi.org/10.36486/978-966-2310-66-5-26

2. Демедюк С.В. Розділ 1. Стратегічний ландшафт застосування OSINT в секторі національної безпеки. OSINT Open Source Intelligence. Теорія та методологія. Монографія. за заг. ред. Користіна О.Є., Демедюка С.В. Київ: 7БЦ, 2025. С. 21-36.

Статті у наукових періодичних виданнях інших держав, у тому числі проіндексованих у базах даних Web of Science Core Collection, Scopus

1. Demedyuk S.V., Demedyuk T.S. Dangerous pornographic content on the internet as a projection of a personality deviation of the child pornography distributor. *Information technologies and learning tools*. 2018. Vol. 68 № 6. P. 278-290. DOI: 10.33407/itlt.v68i6.2582 (WoS)

2. Korystin O., Korchenko O., Kazmirchuk S., Demediuk S., Korystin O. Comparative Risk Assessment of Cyber Threats Based on Average and Fuzzy Sets Theory. *International Journal of Computer Network and Information Security*. 2024. Vol. 16. №. 1. P. 24-34. DOI: https://doi.org/10.5815/ijcnis.2024.01.02 (Scopus Q3)

3. Korystin O., Demediuk S., Sviridyuk N., Mitina O., Aleksander M., Yuriy Kardashevskyy. Risk Forecasting of Information-content-security. *Cyber Hygiene & Conflict Management in Global Information Networks*: Proceedings of the Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks. 2025. Vol. 3925. P. 273–280. (Scopus Q4)

4. Korystin O., Demediuk S., Likhovitskyy Y., Kardashevskyy Y., Mitina O. Priorities for the Strategic Development of Ukraine's Cybersecurity Based on the Analysis of Expert Sampling Patterns. *International Journal of Information Technology and Computer Science.* 2025. Vol. 17. No. 2. P. 24-35. DOI: https://doi.org/10.5815/ijitcs.2025.02.03 (Scopus Q3)

5. Korchenko O., Korystin O., Shulha V., Kazmirchuk S., Demediuk S., Zybin S. Sustainable Development of Smart Regions via Cybersecurity of National Infrastructure: A Fuzzy Risk Assessment Approach. *Sustainability.* (2025). Vol. 17. Is. 19. P. 8757. https://doi.org/10.3390/su17198757 (Scopus Q1)

Статті у наукових виданнях, включених до Переліку наукових фахових видань України

6. Демедюк С.В., Користін О.Є. Стійкість системи кібербезпеки та її забезпечення в НАТО. *Наука і правоохорона*. 2023. № 1(59). С.77-85. DOI: https: //doi.org/10.36486/np.2023.1(59).8

7. Демедюк С.В. Розбудова національної кіберстійкості та захист критично важливої інформаційної інфраструктури. *Наука і правоохорона*. 2023. № 2(60). С.78-85. DOI: https: //doi.org/10.36486/np.2023.2(60).8

8. Користін О.Є., Демедюк С.В., Панченко Є.В., Користін О.О. Національні реалії аналізу кіберзлочинності за методологією Європолу ІОСТА. *Південноукраїнський правничий часопис*. 2023. № 3. С.53-59. DOI https://doi.org/10.32850/sulj.2023.3.10

9. Демедюк С.В. Захист критично важливих послуг у цифрову епоху. *Наука і правоохорона*. 2023. № 3(61). С.26-34 DOI (Issue): https://doi.org/10.36486/np.2023.3(61).3

10. Користін О.Є., Демедюк С.В. Актуалізація кіберстійкості та історичні витоки концепції «стійкість». *Аналітично-порівняльне правознавство: електронне наукове фахове видання юридичного факультету ДВНЗ «Ужгородський національний університет».* 2023. №06. С. 708-713. DOI: https://doi.org/10.24144/2788-6018.2023.06.122

11. Демедюк С.В. Інституціоналізація кіберстійкості. *Наука і правоохорона.* 2023. № 4(62). С.31-41. DOI: https://doi.org/10.36486/np.2023.4(62).4

12. Демедюк С.В. Реалізація спроможності суб'єктів системи протидії кіберзлочинності. *Наука і правоохорона*. 2024. № 1(63). С.133-141. DOI: https://doi.org/10.36486/np.2024.1(63).13

13. Демедюк С.В. OSINT в контексті кібербезпеки. *Юридичний бюлетень*. 2024. № 34. С.200-207. DOI:10.32850/LB2414-4207.2024.34.26

14. Демедюк С.В. OSINT в контексті виявлення та запобігання кіберзлочинам. *Південноукраїнський правничий часопис.* 2024. № 4. С. 38-41. DOI: https://doi.org/10.32850/sulj.2024.4.7

15. Демедюк С.В., Користін О.Є. Тенденції та характерні особливості on-line шахрайства в Україні. *Наука і правоохорона*. 2024. Том 3-4. № 65-66. С. 142-154. DOI: https://doi.org/10.36486/np.2024.3(65).12

16. Демедюк С.В. Зміст та особливості експертної вибірки в оцінюванні кіберризиків. *Морська безпека та оборона*. 2025. №1. С.17-24. DOI: https://doi.org/10.32782/msd/2025.1/03

17. Демедюк С.В. Сучасні тенденції on-line шахрайства в Україні. *Право і суспільство*. 2025. №4. Т. 2. С. 186-194. DOI: https://doi.org/10.32842/2078-3736/2025.4.2.28

18. Демедюк С.В. Темна сторона комп'ютерних мереж: злочини та незаконна діяльність он-лайн. *Правові новели.* 2025. № 26. 157-166. DOI: https://doi.org/10.32782/ln.2025.26.18

Наукові праці, які засвідчують апробацію матеріалів дисертації

1. Демедюк С.В. Стійкість системи кібербезпеки та її правове забезпечення в Україні. *Закарпатські правові читання*: збірник тез за матеріалами XV міжнародної науково-практичної конференції (Ужгород, 27 квітня 2023 р.). Ужгород: УжНУ, 2023. С. 5-7.

2. Демедюк С.В. Захист критично важливої інформаційної інфраструктури в системі кібербезпеки. *Стратегії безпеки підприємництва в умовах воєнного стану*: Збірник тез за матеріалами XIV міжнародної науково-практичної конференції «Безпекотворення: питання теорії, практики та правові аспекти» (Київ, 06 квітня 2023 р.) / за ред. Тимошенко О.І., Київ: Видавництво Європейського університету», 2023. С. 26-27.

3. Демедюк С.В. Розбудова кіберстійкості на національному рівні. *Актуальність та особливості наукових досліджень в умовах воєнного стану*: збірник матеріалів III Міжнародної науково-практичної інтернет-конференції з нагоди відзначення Дня науки – 2023 в Україні (Київ, 23 травня 2023 р.). Київ: ДНДІ МВС України, 2023. С. 133-134.

4. Демедюк С.В. Актуалізація сучасних методологій аналізу кіберзлочинності. *Стан та перспективи розвитку адміністративного права України*: матеріали X міжнародної науково-практичної інтернет-конференції (Одеса, 20 жовтня 2023 р.). Одеса: ОДУВС. С. 63-66.

5. Демедюк С.В. Захист критично важливої інформаційної інфраструктури. *Безпекова ситуація в Україні в умовах війни: стан, загрози, напрями забезпечення*: матеріали науково-практичного круглого столу (Київ, 26 вересня 2023 р.) / [Редкол.: Вербенський М. Г., Опришко І. В., Кулик О. Г. та ін.]. Київ : ДНДІ МВС України, 2023. С. 168-170.

6. Демедюк С.В. Захист критично важливої інформаційної інфраструктури. *Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України*: матеріали міжвідомчої науково-практичної конференції. (Київ, 17 листопада 2023 р.). Київ: НАВС. С.40-44.

7. Демедюк С.В. Захист критично важливих кібер-активів. *Кібербезпека в Україні: правові та організаційні питання*: збірник матеріалів міжнародної науково-практичної конференції (Одеса, 17 листопада 2023 р.). Одеса: ОДУВС. С.55-57.

8. Демедюк С.В. Показники кіберстійкості. *Актуальні питання забезпечення безпекового середовища в Україні*: збірник тез наукових доповідей Всеукраїнської науково-практичної конференції (Київ, 19 квітня 2024 р.). Київ: ДНДІ МВС України, 2024. С.38-41.

9. Демедюк С.В. Щодо питань розвитку кіберстійкості. *Актуальність та особливості наукових досліджень в умовах воєнного стану*: збірник матеріалів IV Міжнародної науково-практичної інтернет-конференції з нагоди відзначення Дня науки-2024 в Україні (Київ, 22 травня 2024 р.). Київ: ДНДІ МВС України, 2024. С.19-21.

10. Демедюк С.В. Використання злочинцями комп'ютерних систем та мереж. *Безпекова ситуація в Україні в умовах війни: стан, загрози, напрями забезпечення безпеки*: збірник матеріалів всеукраїнської науково-практичної конференції (Київ, 27 вересня 2024 р.). Київ: ДНДІ. С. 203-207.

11. Демедюк С.В. Особливості онлайн шахрайства в Україні. *Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України*: матеріали міжвідомчої науково-практичної конференції (Київ, 01 листопада 2024 р.). Київ: НАВС, 2024. С. 35-38.

12. Демедюк С.В. Поширення та характерні складові кіберзалежних злочинів. *Протидія організованій злочинності і корупції в умовах збройного конфлікту: досвід та перспективи з нагоди 5-річчя створення Департаменту стратегічних розслідувань НПУ*: збірник матеріалів Міжнародної науково-практичної конференції (Кропивницький, 04 жовтня 2024 року). Кропивницький: ДонДУВС, 2024. С. 268-273.

13. Демедюк С.В. Інтеграція OSINT в систему кібербезпеки держави: стратегічні та прикладні аспекти. *Роль OSINT-досліджень у підвищенні рівня національної безпеки України*: матеріали круглого столу (Львів, 07 травня 2025 р.). Львів: ЛьвДУВС, 2025. С. 58-61.

АНОТАЦІЯ

Демедюк С.В. Організаційно-правові та кримінологічні засади кіберстійкості в Україні. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора юридичних наук за спеціальністю 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право»; 12.00.08 «Кримінальне право та кримінологія; кримінально-виконавче право». – Одеський державний університет внутрішніх справ, Одеса, 2026.

У дисертації здійснено комплексне теоретико-правове та кримінологічне дослідження кіберстійкості як новітньої парадигми забезпечення національної безпеки України в умовах цифрової трансформації та гібридної агресії. Обґрунтовано, що традиційна модель кібербезпеки, орієнтована на запобігання інцидентам, виявляється недостатньо ефективною в умовах зростання складності та багатовекторності кіберзагроз, що зумовлює необхідність переходу до концепції кіберстійкості як здатності системи передбачати, протидіяти, відновлюватися та адаптуватися до деструктивних впливів.

У роботі розкрито генезис і еволюцію поняття «стійкість» у міждисциплінарному вимірі, що дозволило сформувати сучасне розуміння кіберстійкості як емерджентної властивості соціотехнічних систем. Запропоновано авторське визначення кіберстійкості та здійснено теоретичне розмежування категорій «кібербезпека» і «кіберстійкість», доведено доцільність зміщення акцентів із захисту периметра на забезпечення безперервності функціонування критичних процесів.

Значну увагу приділено аналізу міжнародного досвіду формування кіберстійкості, зокрема підходів Європейського Союзу, США, Великої Британії та НАТО, що дозволило обґрунтувати напрями гармонізації національного законодавства із євроатлантичними стандартами. Встановлено, що ефективна система кіберстійкості має базуватися на поєднанні регуляторних, стандартизаційних і ринкових механізмів, які формують цілісну інституціональну архітектуру кіберуправління.

У дисертації розроблено концептуальну модель інституціоналізації кіберстійкості, що передбачає інтеграцію державного, приватного та громадянського секторів на засадах спільної відповідальності. Обґрунтовано необхідність розвитку цивільно-військового співробітництва у кіберпросторі, зокрема через впровадження моделі «Cyber-CIMIC», створення інституту цивільного кіберрезерву та запровадження спеціальних правових режимів для залучення недержавних суб’єктів до кібероборони.

Окремий блок дослідження присвячено методології аналітичної розвідки у сфері кіберстійкості. Доведено, що ефективне стратегічне управління кіберзагрозами можливе лише за умов синергії методів OSINT, стратегічного форсайту та ризик-орієнтованого підходу. Запропоновано модель інтелектуальної стійкості, яка забезпечує трансформацію даних у стратегічні рішення та підвищує адаптивність національної системи кібербезпеки.

На основі емпіричного аналізу здійснено ранжування кіберзагроз за рівнем ризику та визначено пріоритетні напрями зміцнення кіберстійкості України, зокрема у сферах критичної інфраструктури. Розроблено комплексну матричну модель діагностики кіберстійкості, що поєднує функціональні етапи управління інцидентами з операційними доменами системи та дозволяє оцінювати її здатність до відновлення і адаптації.

У роботі також досліджено сучасний стан кіберзлочинності, визначено її ключові тенденції, інструменти та кримінологічні детермінанти. Обґрунтовано

необхідність переходу до предиктивних моделей протидії кіберзлочинності на основі стратегічного аналізу та ризик-менеджменту.

Сформовано наукове бачення щодо формування цілісної теоретико-методологічної концепції кіберстійкості як вищого рівня кібербезпеки, розробки інституціональних, організаційно-правових і кримінологічних засад її забезпечення, а також створення інноваційних моделей оцінювання та управління кіберризиками.

Ключові слова: кіберстійкість, кібербезпека, кіберзагрози, кіберзлочинність, ризик-орієнтований підхід, OSINT, форсайт, критична інфраструктура, національна безпека, правове регулювання.

SUMMARY

Demediuk S.V. Organisational, legal and criminological foundations of cyber resilience in Ukraine. – Qualification scientific work on the rights of the manuscript.

Thesis for the degree of Doctor of Law in the following specialities: 12.00.07 «Administrative law and process; financial law; information law»; 12.00.08 «Criminal law and criminology; criminal enforcement law». – Odessa State University of Internal Affairs, Odessa, 2026.

The dissertation presents a comprehensive theoretical-legal and criminological study of cyber resilience as a modern paradigm for ensuring the national security of Ukraine in the context of digital transformation and hybrid aggression. It substantiates that the traditional cybersecurity model, focused primarily on incident prevention, proves insufficient under conditions of increasing complexity and multi-vector cyber threats, which necessitates a shift toward the concept of cyber resilience as the ability of a system to anticipate, withstand, recover, and adapt to disruptive impacts.

The study explores the genesis and evolution of the concept of “resilience” in an interdisciplinary dimension, which made it possible to formulate a modern understanding of cyber resilience as an emergent property of socio-technical systems. An author’s definition of cyber resilience is proposed, and a theoretical distinction between the categories of “cybersecurity” and “cyber resilience” is made, demonstrating the expediency of shifting the focus from perimeter protection to ensuring the continuity of critical processes.

Considerable attention is paid to the analysis of international experience in developing cyber resilience, particularly the approaches of the European Union, the United States, the United Kingdom, and NATO, which allowed for the substantiation of directions for harmonizing national legislation with Euro-Atlantic standards. It is established that an effective cyber resilience system should be based on a combination of regulatory, standardization, and market mechanisms that together form a coherent institutional architecture of cyber governance.

The dissertation develops a conceptual model for the institutionalization of cyber resilience, which предусматриває integration of the public, private, and civil sectors based on the principle of shared responsibility. The necessity of developing civil-military cooperation in cyberspace is substantiated, in particular through the implementation of the “Cyber-CIMIC” model, the creation of a civil cyber reserve institution, and the introduction of special legal regimes for engaging non-state actors in cyber defense.

A separate part of the research is devoted to the methodology of analytical intelligence in the field of cyber resilience. It is proven that effective strategic management of cyber threats is possible only through the synergy of OSINT methods, strategic foresight, and a risk-oriented approach. A model of intellectual resilience is proposed, which ensures the transformation of data into strategic decisions and enhances the adaptability of the national cybersecurity system.

Based on empirical analysis, cyber threats are ranked according to their level of risk, and priority directions for strengthening cyber resilience in Ukraine are identified, particularly in the field of critical infrastructure. A comprehensive matrix model for diagnosing cyber resilience is developed, combining functional stages of incident management with operational domains of the system, enabling the assessment of its capacity for recovery and adaptation.

The study also examines the current state of cybercrime, identifying its key trends, tools, and criminological determinants. The necessity of transitioning to predictive models of countering cybercrime based on strategic analysis and risk management is substantiated.

A scientific vision is formed regarding the development of a holistic theoretical and methodological concept of cyber resilience as a higher level of cybersecurity, the elaboration of institutional, organizational-legal, and criminological foundations for its provision, as well as the creation of innovative models for assessing and managing cyber risks.

Keywords: cyber resilience, cybersecurity, cyber threats, cybercrime, risk-oriented approach, OSINT, foresight, critical infrastructure, national security, legal regulation.