МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Харківський національний університет імені В.Н. Каразіна

Навчально-науковий інститут «Інститут державного управління»
Кафедра права, національної безпеки та європейської інтеграції

Кваліфікаційна робота магістра
на тему

ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ: ПУБЛІЧНО-ПРИВАТНА ВЗАЄМОДІЯ

Виконав студент 2 курсу,
групи ППГЗ-3-24
Спеціальності 281 «Публічне
управління та адміністрування»
Освітньо-професійної програми
«Публічна політика та управління в
умовах гібридних загроз»
_____ Олександр ЩЕРБАТЮК

Науковий керівник роботи:
доктор юридичних наук, професор
_____ Лариса ВЕЛИЧКО

Харків – 2025

ЗМІСТ

ВСТУП

Актуальність теми. У сучасному світі критична інфраструктура стала пріоритетною мішенню кібератак, здатних паралізувати функціонування цілих держав, порушити енергопостачання, транспортну систему, фінансовий сектор та інші життєво важливі галузі. Кіберінциденти проти критичної інфраструктури можуть спричинити не лише економічні збитки, але й загрозу життю громадян, національній безпеці та суверенітету держав.

Україна з 2014 року перебуває під систематичним кібератаками Російської Федерації, включаючи масштабні напади на енергосистему 2015-2016 років, які стали першими у світі прикладами реалізованого кібервимкнення електропостачання. В подальшому, повномасштабне вторгнення 24 лютого 2022 року супроводжувалося безпрецедентною інтенсивністю кібератак на критичну інфраструктуру, спрямованих на підрив державного управління, енергетичної безпеки та комунікацій. Критична інфраструктура України опинилася на передовій гібридної війни, де кіберзагрози інтегровані з фізичними військовими діями.

Слід зазначити, що національна система захисту критичної інфраструктури формувалася фрагментарно, без достатньої координації між державним та приватним секторами. Відсутність чіткого розподілу повноважень між органами влади, обмежена публічно-приватна взаємодія, недостатня міжвідомча координація та дефіцит кваліфікованих кадрів створюють серйозні виклики для забезпечення кіберстійкості критичної інфраструктури.

Актуальність даного дослідження обумовлена нагальною потребою розробки ефективної моделі публічно-приватної взаємодії у сфері кіберзахисту критичної інфраструктури України на основі узагальнення міжнародного досвіду та специфіки національного контексту. Ефективна система кіберзахисту критичної інфраструктури є необхідною умовою не лише для стійкості держави під час війни, але й для довгострокового забезпечення національної безпеки,

економічної стабільності, захисту прав громадян та успішної євроінтеграції України в повоєнний період.

Стан наукової розробки проблеми. Проблематика кіберстійкості критичної інфраструктури та механізмів публічно-приватної взаємодії в цій сфері перебуває у фокусі наукової уваги українських та зарубіжних дослідників, однак комплексні дослідження інтеграційних моделей публічно-приватної взаємодії в українському контексті залишаються обмеженими.

Серед українських науковців, які досліджують питання кібербезпеки критичної інфраструктури, слід відзначити внесок В.Г. Пилипчука, який аналізує правові засади захисту критичної інфраструктури та механізми державного регулювання у цій сфері, П.В. Вишневської, яка досліджує міжнародний досвід кібербезпеки, зокрема ізраїльську модель військово-цивільної синергії.

І.С. Кузьменко вивчає можливості інтеграції ізраїльських практик кібербезпеки в українські реалії, а Н.В. Гончарук аналізує адаптацію директиви NIS2 у державах Балтії та Польщі з акцентом на досвід для України. Зокрема, С.І. Андрієвський досліджує регіональну співпрацю в кібербезпеці на прикладі польського та балтійського досвіду, а Ю.А. Гульванська приділяє увагу правовому регулюванню кібербезпеки в Україні, проблемам міжвідомчої координації та шляхам удосконалення інституційної системи. В свою чергу, І. Коваленко аналізує кадрові виклики в кібербезпеці України, включаючи проблеми втрати фахівців через мобілізацію та міграцію до приватного сектору.

Зарубіжні дослідження представлені роботами, що стосуються інституційних моделей та технічних стандартів. Документи ENISA висвітлюють практичний досвід функціонування Information Sharing and Analysis Centers (ISACs) в Європейському Союзі як платформ обміну інформацією про кіберзагрози між державою та бізнесом. Публікації NIST (National Institute of Standards and Technology) обґрунтовують добровільну структуру управління кіберризиками через п’ять ключових функцій кібербезпеки. Офіційні матеріали UK National Cyber Security Centre демонструють британську модель публічно-приватної взаємодії через платформу CiSP. Дослідження NATO Cooperative

Cyber Defence Centre of Excellence аналізують міжнародну підтримку України у розбудові національної системи кіберзахисту. Аналітичні матеріали міжнародних організацій (Європейська Комісія, Світовий банк, USAID, GIZ, Microsoft) висвітлюють програми технічної та фінансової допомоги Україні у сфері кібербезпеки критичної інфраструктури.

Незважаючи на значну кількість досліджень окремих аспектів проблематики, відсутні комплексні роботи, які б системно аналізували моделі інтеграційної публічно-приватної взаємодії у сфері кіберстійкості критичної інфраструктури з урахуванням українського контексту воєнного стану та євроінтеграційних процесів. Практично відсутні дослідження, які узагальнюють міжнародний досвід та пропонують науково обґрунтовані рекомендації щодо адаптації успішних практик до українських реалій. Саме заповнення цієї прогалини визначає актуальність і практичну значущість даного дослідження.

Метою роботи є комплексний аналіз міжнародного досвіду публічно-приватної взаємодії у сфері кіберзахисту критичної інфраструктури та розробка науково обґрунтованої моделі інтеграційної публічно-приватної взаємодії для України з урахуванням специфіки воєнного стану та євроінтеграційних процесів.

Для досягнення поставленої мети визначено наступні *завдання:*

– узагальнити теоретико-концептуальні засади кіберстійкості критичної інфраструктури та розкрити роль публічно-приватної взаємодії у забезпеченні кіберзахисту;

– дослідити міжнародний досвід організації публічно-приватної взаємодії у сфері кіберзахисту критичної інфраструктури шляхом комплексного аналізу практик різних країн;

– проаналізувати інституційну систему кіберзахисту критичної інфраструктури в провідних країнах світу, визначити структуру, повноваження та механізми координації між державним та приватним секторами;

– вивчити специфічні моделі публічно-приватної взаємодії в країнах з різними інституційними традиціями (Естонія, США, Великобританія, Ізраїль, Польща, країни Балтії);

– виявити ключові елементи успішних моделей публічно-приватної взаємодії та механізми їх адаптації до українського контексту;

– розробити комплексні рекомендації щодо вдосконалення публічно-приватної взаємодії в Україні за інституційними, правовими, організаційними, технологічними, фінансовими та кадровими напрямами.

Об'єктом дослідження є система кіберзахисту критичної інфраструктури в Україні та провідних країнах світу.

Предметом дослідження є механізми публічно-приватної взаємодії у сфері забезпечення кіберстійкості критичної інфраструктури.

Методи дослідження. Для досягнення мети дослідження та вирішення поставлених завдань використано комплекс загальнонаукових та спеціальних методів, застосування яких здійснювалося відповідно до специфіки кожного етапу дослідження.

Метод термінологічного аналізу застосовано для розмежування понять «кіберстійкість», «критична інфраструктура», «публічно-приватне партнерство», «кіберзахист», що дозволило створити чітку термінологічну основу роботи; *метод теоретичного узагальнення* використано для систематизації наукових підходів до розуміння кіберзагроз та формулювання власних теоретичних висновків щодо природи кіберстійкості критичної інфраструктури; *системний підхід* застосовано для дослідження кіберзахисту критичної інфраструктури як цілісної системи взаємопов'язаних елементів, що включає державний та приватний сектори, технологічну інфраструктуру, правове регулювання та людський капітал (підрозділ 1.1).

Компаративний метод використано для порівняльного аналізу міжнародного досвіду публічно-приватної взаємодії у сфері кіберзахисту критичної інфраструктури, виявлення спільних та відмінних рис національних моделей США, Великобританії, Естонії, Ізраїлю, Польщі та країн Балтії, що дало змогу ідентифікувати успішні практики для адаптації в українських умовах; *метод кейс-стаді* застосовано для поглибленого аналізу конкретних моделей: естонської платформи X-Road, американських ISACs, британської CiSP,

ізраїльського Національного кібердиректорату, що забезпечило розуміння практичного застосування теоретичних концепцій (підрозділи 2.1, 2.2, 2.3, 3.1).

Інституційний аналіз використано для дослідження формальних та неформальних інститутів, що забезпечують кіберзахист критичної інфраструктури в різних країнах, їх структури, повноважень та механізмів взаємодії, що дозволило виявити інституційні особливості та фактори успіху різних моделей (підрозділи 2.1, 2.2, 2.3); *структурно-функціональний аналіз* застосовано для визначення ролей та функцій різних акторів (державних органів, приватних операторів, міжнародних організацій) у системі публічно-приватної взаємодії; *нормативно-правовий аналіз* використано для вивчення законодавчої бази кіберзахисту критичної інфраструктури в різних юрисдикціях, виявлення успішних правових механізмів стимулювання публічно-приватної співпраці (підрозділи 2.1, 3.2).

Метод документального аналізу застосовано для вивчення офіційних документів, стратегій, директив (зокрема NIS2), звітів міжнародних організацій щодо кіберзахисту критичної інфраструктури (підрозділи 2.1, 2.2, 2.3, 3.1); *метод синтезу міжнародного досвіду* використано для узагальнення наскрізних елементів успішних моделей публічно-приватної взаємодії незалежно від національного контексту, що дозволило сформулювати універсальні принципи ефективної співпраці (підрозділ 3.1).

Метод критичного аналізу застосовано для оцінювання релевантності різних міжнародних моделей для українського контексту з урахуванням специфіки воєнного стану, масштабу країни, рівня економічного розвитку та інституційних традицій; *метод експертних оцінок* використано для визначення пріоритетності різних напрямів вдосконалення публічно-приватної взаємодії в Україні (підрозділ 3.2).

Метод стратегічного планування використано для визначення послідовності впровадження рекомендацій з урахуванням обмежених ресурсів, поточних викликів воєнного стану та довгострокових цілей євроінтеграції; *метод моделювання* застосовано для розробки комплексної моделі публічно-

приватної взаємодії в Україні, що охоплює інституційні, правові, організаційні, технологічні, фінансові та кадрові аспекти; *метод системного синтезу* застосовано для формулювання взаємопов'язаного комплексу рекомендацій, що забезпечують цілісність та узгодженість запропонованих змін (підрозділ 3.2).

Комплексне застосування зазначених методів дозволило забезпечити всебічність та об'єктивність дослідження механізмів публічно-приватної взаємодії у сфері кіберстійкості критичної інфраструктури.

Практичне значення отриманих результатів. Результати дослідження мають конкретне практичне застосування у декількох ключових сферах:

У науково-дослідній сфері матеріали роботи формують теоретико-методологічну основу для подальших наукових досліджень механізмів публічно-приватної взаємодії у сфері кібербезпеки. Запропонована модель інтеграційної публічно-приватної взаємодії слугує аналітичним інструментом у подальших дослідженнях інституційних механізмів забезпечення кіберстійкості. Синтез елементів успішних моделей формує теоретичну основу для розробки універсальних принципів ефективної співпраці між державою та бізнесом у сфері кібербезпеки.

У практичній діяльності державних органів результати дослідження надають Раді національної безпеки і оборони України аналітичну основу при оновленні Стратегії кібербезпеки України. Центральні органи виконавчої влади можуть використати результати дослідження при розробці нормативно-правових актів з питань захисту критичної інфраструктури та адаптації директиви NIS2. Виявлені прогалини в координації між відомствами дозволяють органам влади цілеспрямовано зосередити зусилля на створенні ефективних координаційних механізмів, таких як Національна платформа кіберстійкості.

Запропоновані інституційні рекомендації, включаючи створення інституту урядового координатора з кіберстійкості та секторальних координаційних центрів, формують основу інституційної реформи системи кіберзахисту. Кадрові рекомендації щодо механізмів утримання фахівців, програм стажування та бронювання від мобілізації для критичних позицій вирішують гостру проблему

кадрового дефіциту.

У навчальному процесі матеріали дослідження можуть бути інтегровані закладами вищої освіти при викладанні дисциплін «Кібербезпека», «Публічне управління та адміністрування», «Національна безпека», «Інформаційна безпека», «Публічне управління на деокупованих територіях» збагачуючи їх компаративним аналізом міжнародних моделей та українським контекстом.

Результати дослідження можуть бути включені до програм підготовки та підвищення кваліфікації публічних службовців у Національному агентстві України з питань державної служби, ННІ «Інституті державного управління» Харківського національного університету імені В.Н. Каразіна, узагальнені практики публічно-приватної взаємодії складають основу практичних занять, воркшопів та тренінгів для працівників органів публічної влади та операторів критичної інфраструктури.

Матеріали роботи можуть бути використані при підготовці навчально-методичних посібників, монографій, наукових статей з проблематики кіберстійкості критичної інфраструктури та публічно-приватної взаємодії, при розробці нових освітньо-професійних програм у сфері кібербезпеки, національної безпеки та публічного управління. Компаративний аналіз міжнародних моделей може бути використаний у навчальному процесі як практичний матеріал для вивчення успішних практик організації кіберзахисту на конкретних прикладах різних країн, що робить навчання більш прикладним та релевантним для майбутніх фахівців.

Апробація результатів дослідження. Основні положення та результати дослідження обговорювалися на засіданнях кафедри права, національної безпеки та європейської інтеграції ННІ «Інституті державного управління» Харківського національного університету імені В.Н. Каразіна і можуть бути використані в подальшому в науковій діяльності кафедри.

РОЗДІЛ 1
СИСТЕМАТИЗАЦІЯ ТА АНАЛІЗ КІБЕРЗАГРОЗ КРИТИЧНІЙ ІНФРАСТРУКТУРІ УКРАЇНИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

1.1 Кіберзагрози та вразливості об’єктів критичної інфраструктури в умовах збройної агресії, сутність та класифікація

Критична інфраструктура України, забезпечуючи життєво важливі функції держави та суспільства, опинилася під безпрецедентним кібератаками в умовах триваючої гібридної війни. Повномасштабна збройна агресія російської федерації проти України актуалізувала питання забезпечення кіберстійкості об’єктів критичної інфраструктури, виявивши системні вразливості національної інформаційної архітектури. За даними Державного центру кіберзахисту Держспецзв’язку, у другому півріччі 2024 року кількість кіберінцидентів зросла на 48% порівняно з першим півріччям, фіксуючи 2576 атак [30; 31]. Трансформація характеру кіберзагроз від традиційних злочинних операцій до координованих державних кібердиверсій вимагає фундаментального переосмислення підходів до захисту критичної інфраструктури.

Систематизація кіберзагроз, загрожуючих критичній інфраструктурі, базується на комплексному аналізі векторів атак, цільових об’єктів та потенційних наслідків. Дослідники Скіцько О.І. та Ширшов Р.А. виокремлюють три основні категорії загроз: зовнішні, внутрішні та цільові [63]. Зовнішні загрози включають масовані DDoS-атаки, експлуатацію вразливостей інформаційних систем підприємств та комплексні багатовекторні операції проти державних ресурсів. Внутрішні загрози охоплюють інсайдерську діяльність, витік конфіденційної інформації та системні помилки персоналу, що становить до 35% усіх інцидентів кібербезпеки. Найнебезпечнішою категорією залишаються цільові загрози, засновані на соціальній інженерії та спрямовані на компрометацію мереж через фішингові розсилки.

Однак запропонована дослідниками триланкова класифікація, хоча й охоплює основні вектори загроз, потребує критичного переосмислення в контексті реалій гібридної війни. По-перше, чітке розмежування між зовнішніми та внутрішніми загрозами втрачає актуальність в умовах, коли атакуючі активно вербують інсайдерів або компрометують легітимних користувачів через складні схеми соціальної інженерії. По-друге, виокремлення цільових загроз в окрему категорію є дискусійним, оскільки практично всі сучасні атаки на критичну інфраструктуру мають цільовий характер, відрізняючись лише рівнем складності підготовки та персоналізації. Більш продуктивним видається застосування багатовимірної моделі класифікації, що враховує не тільки джерело та вектор загрози, але й мотивацію атакуючих, рівень складності атаки, потенційні наслідки та можливості атрибуції.

Критично оцінюючи запропоновану класифікацію, варто відзначити її практичну цінність для структурування превентивних заходів, однак трьохкомпонентна модель може бути недостатньою для відображення складності сучасних гібридних загроз. Автори концентруються на технічних аспектах векторів атак, проте недостатньо акцентують увагу на геополітичному контексті та стратегічній координації між різними типами загроз.

В умовах війни межі між «зовнішніми» та «внутрішніми» загрозами розмиваються, оскільки російські спецслужби активно використовують інсайдерів та агентів впливу, що потребує більш нюансованого підходу до класифікації.

Еволюція кіберзагроз в умовах війни демонструє перехід від опортуністичних атак до стратегічно скоординованих операцій, інтегрованих у загальний план гібридного впливу. Синхронізація кібератак з фізичними ударами по енергетичній інфраструктурі навесні 2024 року підтверджує формування нової доктрини кібервійни, де цифрові операції виступають мультиплікатором руйнівного ефекту традиційних засобів ураження.

Гульванська Ю.А. слушно наголошує на критичній важливості розуміння еволюції кіберзагроз у контексті військового конфлікту [28]. Кібератаки можуть

не тільки порушити роботу інфраструктури, але й призвести до серйозних економічних, соціальних та гуманітарних наслідків. Прикладом є вірус NotPetya, що у 2017 році завдав збитків українській економіці на суму понад 10 млрд доларів США. Аналіз інцидентів 2022-2024 років виявляє тенденцію до зростання складності атак та застосування передових методів, включаючи експлуатацію вразливостей нульового дня.

Варто відзначити, що позиція дослідників, хоча й слушно акцентує увагу на багатовимірності наслідків кібератак, недостатньо розкриває принципову зміну парадигми кіберконфлікту в умовах повномасштабної війни. NotPetya 2017 року був швидше «випробуванням сил», аніж повноцінною військовою кібероперацією, оскільки відбувся в період гібридного протистояння, а не відкритого збройного конфлікту. Сучасні кібератаки 2022-2024 років якісно відрізняються не тільки технічною складністю, але й стратегічною інтеграцією в загальний план військових дій, координацією з ракетними ударами та артилерійськими обстрілами. Це вимагає концептуального переосмислення кібератак не як окремих інцидентів, а як компонентів єдиної багатодоменної операції, де цифровий простір стає повноцінним театром бойових дій нарівні з сухопутним, повітряним та морським.

Позиція дослідників щодо комплексного впливу кібератак на множину суспільних сфер є обґрунтованою та підтверджується емпіричними даними. Водночас їхній підхід залишається переважно дескриптивним, фокусуючись на описі загроз без пропозиції конкретних механізмів їх нейтралізації. Посилання на кейс NotPetya є показовим, проте автори не розвивають аналіз причин, чому саме Україна стала епіцентром цієї атаки, та яких системних висновків слід було зробити для запобігання подібним інцидентам у майбутньому. Відсутність критичного аналізу інституційних провалів у реагуванні на NotPetya обмежує практичну цінність дослідження для розробки превентивних стратегій.

Критичним елементом розуміння кіберзагроз є аналіз мотивації та спроможностей акторів. Стратегія кібербезпеки України визначає чотири основні категорії загроз національній безпеці [54]:

1. Гібридна агресія Російської Федерації у кіберпросторі, що включає систематичні кібератаки на інформаційні системи державних органів та об’єкти критичної інфраструктури;

2. Кіберзлочинність, що завдає шкоди інформаційним ресурсам та призводить до значних матеріальних втрат;

3. Організовані державою кібератаки, пов’язані з викраденням чутливої інформації в політичних або військових цілях;

4. Кібертероризм, що використовує кіберпростір для вчинення актів терору та дестабілізації критичних систем.

Стратегічний документ демонструє еволюцію державного мислення у сфері кібербезпеки, переходячи від технократичного розуміння загроз до їх геополітичної контекстуалізації. Критично важливим є визнання російської федерації як основного джерела кіберзагроз, що відображає реалістичний підхід до оцінки безпекового середовища. Водночас стратегія, прийнята у 2021 році, не повною мірою передбачала масштаб та інтенсивність кібератак в умовах повномасштабної війни, що свідчить про необхідність її оновлення з урахуванням накопиченого воєнного досвіду. Зокрема, категорія «кібертероризм» потребує переосмислення, оскільки у воєнних умовах межа між терористичними актами та легітимними військовими операціями стає предметом міжнародно-правових дебатів.

Представлена класифікація (таблиця 1.1) демонструє диверсифікацію векторів кіберзагроз та їх адаптацію до специфіки українських реалій воєнного часу. Домінування DDoS-атак пояснюється їх технічною доступністю та можливістю залучення великої кількості учасників через російські хактивістські угруповання. Водночас найбільш небезпечними залишаються атаки на промислові системи управління, попри їх меншу частоту, оскільки вони можуть призвести до фізичних руйнувань об’єктів. Тривожною тенденцією є зростання інцидентів з використанням шкідливого ПЗ на 112% у другому півріччі 2024 року.

Таблиця 1.1 – Класифікація кіберзагроз для критичної інфраструктури України

Тип загрози	*Основні вектори атак*	*Цільові об'єкти*	*Рівень критичності*	*Частота 2024*
DDoS-атаки	Перевантаження мережевих ресурсів, ботнети	Державні портали, банки	Середній-Високий	45%
Шкідливе ПЗ	Фішинг, ransomware, експлуатація вразливостей	Інформсистеми підприємств	Високий-Критичний	28%
Атаки на SCADA	Промислові протоколи, backdoor	Енергетика, транспорт	Критичний	12%
Соціальна інженерія	Цільовий фішинг, підробка	Персонал критичних об'єктів	Високий	15%

Джерело: розробка автора.

Вразливості об'єктів критичної інфраструктури України формуються під впливом технологічних, організаційних та людських факторів. Згідно з дослідженням Національної академії Служби безпеки України, недосконаліть національної системи захисту обумовлена відсутністю надійної ізоляції між операційно-технологічними та корпоративними мережами [63]. Високий професійний потенціал вітчизняних програмістів парадоксально створює двосторонній ефект: забезпечуючи можливості для інноваційного розвитку кіберзахисту та формуючи потенційні ризики через можливість використання цих компетенцій зловмисниками.

Критична рефлексія дослідження Національної академії Служби безпеки України дозволяє виявити як сильні сторони, так і обмеження запропонованого підходу. Слушно ідентифікуючи технічну проблему відсутності сегментації мереж, дослідники не пропонують економічно реалістичних шляхів її вирішення для підприємств критичної інфраструктури в умовах обмеженого бюджетування. Твердження щодо «парадоксу» професійного потенціалу є дещо спрощеним, оскільки воно не враховує можливості створення позитивної синергії через залучення цього потенціалу до національної системи кіберзахисту. Замість розгляду висококваліфікованих спеціалістів як потенційної загрози, доцільніше було б запропонувати механізми їх інституційного залучення до захисту

критичної інфраструктури через створення привабливих умов праці у державному секторі та розвиток публічно-приватних партнерств.

Поглиблюючи критичну оцінку дослідження, варто наголосити, що фахівці академії акуратно ідентифікують технічні прогалини, однак недостатньо артикулюють системні організаційні причини їх виникнення та збереження. Відсутність ізоляції між мережами не є суто технічною проблемою, а відображає глибші інституційні дисфункції: недостатність фінансування модернізації, брак кваліфікованого персоналу для проєктування безпечних архітектур, відсутність обов'язкових регуляторних стандартів. Парадокс високого професійного потенціалу програмістів, на який вказують дослідники, насправді розкриває фундаментальну проблему «відпливу мізків» та неспроможності державного сектору конкурувати з приватним за таланти. Це вимагає не лише технічних, а й економічних та управлінських рішень на рівні державної політики.

Комісарова Н.О. та Крутіков П.Д. наголошують на важливості комплексного підходу до захисту критичної інфраструктури, що охоплює не лише технічні, а й організаційні та нормативні заходи [42]. Дослідники обґрунтовують, що ефективний захист об'єктів критичної інфраструктури вимагає ідентифікації інформаційних загроз, кібератак та операцій кібершпигунства як потенційних ризиків, а також виявлення недоліків у наявних системах захисту.

Критично оцінюючи позицію дослідників, варто визнати слушність акценту на мультидименсійності захисту, проте їхній підхід не розкриває конкретних механізмів синхронізації технічних, організаційних та нормативних компонентів у єдину систему. Твердження про «комплексність» залишається на рівні декларації без пропозиції практичних моделей інтеграції різнорідних заходів. Особливо проблемним є відсутність аналізу економічних обмежень, що ускладнюють одночасне впровадження всіх складових комплексного підходу в умовах воєнного стану та обмеженого бюджетного фінансування. Крім того, автори не артикулюють пріоритетності заходів, що є критичним для розподілу обмежених ресурсів між технічними модернізаціями, організаційними

реформами та розробкою нормативної бази.

Аналіз вразливостей критичної інфраструктури виявляє системне відставання темпів модернізації засобів захисту від темпів еволюції кіберзагроз. Особливо критичною є ситуація із застарілими промисловими системами управління на об’єктах енергетики, спроектованими за десятиліття до появи сучасних кіберзагроз. Необхідність балансування між забезпеченням безперебійності технологічних процесів та впровадженням сучасних засобів захисту створює стратегічну дилему.

Стратегія кібербезпеки України ідентифікує передумови та чинники, що формують загрози [61]:

– високу технологічну залежність від іноземних виробників інформаційно-комунікаційних технологій;

– недосконаліть нормативно-правової бази у сфері кібербезпеки;

– відсутність у державних органів структурних підрозділів з кіберзахисту;

– відсутність системи незалежного аудиту інформаційної безпеки;

– невідповідність рівня підготовки фахівців сучасним вимогам;

– відсутність законодавчого акту про критичну інфраструктуру;

– незавершеність впровадження організаційно-технічної моделі кіберзахисту.

Нормативно-правове забезпечення кіберзахисту в Україні отримало значний розвиток з прийняттям Постанови Кабінету Міністрів України № 519 від 19 червня 2019 року, що встановила загальні вимоги до кіберзахисту об’єктів критичної інфраструктури [44]. Документ визначає базові принципи та процедури мінімізації кіберризиків у державному та приватному секторі, передбачаючи впровадження заходів з управління кіберінцидентами, оцінки ризиків та обов’язкової моніторингової діяльності для операторів критичної інфраструктури.

Аналізуючи практичну імплементацію Постанови № 519, варто відзначити розбіжність між амбітними нормативними вимогами та реальними

можливостями їх впровадження операторами критичної інфраструктури. Відсутність в документі чітких механізмів фінансової підтримки для малих та середніх операторів створює ситуацію, коли регуляторні вимоги стають фактично обов'язковими лише для великих державних підприємств з достатніми ресурсами.

Крім того, п'ятирічний розрив між прийняттям постанови (2019) та повномасштабною війною (2022) виявив недостатню адаптивність нормативної бази до швидкозмінного безпекового середовища, що вимагає більш гнучких механізмів актуалізації вимог відповідно до еволюції загроз.

Міжнародний досвід показує, що найбільш резонансні інциденти стали можливими через комплексне використання множини вразливостей одночасно [50]. У випадку України ситуація ускладнюється триваючим військовим конфліктом, що створює додаткові виклики для забезпечення фізичної безпеки об'єктів інфраструктури.

Звертання до міжнародного досвіду, зокрема естонського кейсу 2007 року, є методологічно виправданим для розуміння траєкторій еволюції кіберзагроз [51]. Однак пряме перенесення естонських уроків на українські реалії має суттєві обмеження. Естонія зіткнулася з відносно обмеженою у часі кампанією DDoS-атак у мирний час, тоді як Україна протистоїть тривалій багаторівневій кібервійні, інтегрованій у широкомасштабний збройний конфлікт.

Крім того, Естонія мала можливість відбудовувати свою кіберстійкість в умовах членства в НАТО та ЄС з доступом до ресурсів альянсу, що кардинально відрізняється від української ситуації періоду 2014-2022 років.

Таким чином, український досвід протистояння кіберзагрозам у військовий час є унікальним та потребує окремої концептуалізації.

Таблиця 1.2 – Вразливості об’єктів критичної інфраструктури України

Категорія	*Конкретні прояви*	*Рівень впливу*	*Заходи мітигації*
Технологічні	Застаріле SCADA/ICS, відсутність сегментації	Критичний	Модернізація, zero trust
Організаційні	Фрагментація відповідальності, недофінансування	Високий	Єдиний координаційний центр
Людські	Недостатня обізнаність, витік кадрів	Високий	Навчання, бронювання
Нормативні	Відсутність обов’язкових стандартів	Середній	Адаптація NIS2
Фізичні	Пошкодження внаслідок бойових дій	Критичний	Резервування систем

Джерело: розробка автора.

Таким чином, багатовимірний характер вразливостей критичної інфраструктури вимагає комплексного підходу до їх усунення. Особливо проблемними є організаційні вразливості, пов’язані з фрагментацією відповідальності між численними власниками об’єктів. Відсутність чіткого розподілу повноважень між державними органами створює лакуни в системі кіберзахисту. Людський фактор залишається найслабшою ланкою, про що свідчить успішність 73% цільових фішингових атак за даними CERT-UA. В умовах війни ця вразливість посилюється стресовими умовами роботи персоналу.

Науковий вісник Ужгородського університету систематизує ключові загрози безпеці критичної інфраструктури України, серед яких виділяються критична зношеність основних фондів об’єктів інфраструктури, недостатній рівень їх фізичного захисту, недостатній рівень захищеності від терористичних посягань і диверсій, та неефективне управління ризиками [22]. Дослідження концептуалізує критичну інфраструктуру як комплекс заходів, реалізований у нормативно-правових, організаційних та технологічних інструментах, спрямованих на забезпечення безпеки та стійкості.

Критично оцінюючи цю систематизацію, слід відзначити, що акцент на «критичній зношеності» як первинній загрозі, хоча й відповідає реальному стану українських об’єктів інфраструктури, фактично перекладає відповідальність за

вразливості на недостатність інвестицій у минулому, уникаючи аналізу поточних управлінських рішень щодо пріоритизації модернізації. Твердження про «неефективне управління ризиками» залишається занадто загальним без ідентифікації конкретних інституційних провалів у системі прийняття рішень.

Більш продуктивним був би аналіз причин, чому управління ризиками залишається неефективним, зокрема розподіл відповідальності між численними державними органами, відсутність єдиної методології оцінки ризиків та недостатня кваліфікація персоналу, відповідального за ризик-менеджмент.

Кіберзлочинність набуває нових форм в умовах гібридної війни, трансформуючись з фінансово мотивованих злочинів у інструмент політичного тиску. Аналіз діяльності російських хакерських угруповань виявляє координацію їхніх дій з військовими операціями [8]. Навесні 2024 року угруповання UAC-0002 здійснювало атаки проти майже 20 об’єктів енерго- та водопостачання, причому несанкціонований доступ мав бути використаний для підсилення ефекту ракетних ударів [11].

Інтеграція кібероперацій у єдину стратегію гібридної війни створює синергетичний ефект, де кібератаки мультиплікують наслідки фізичних ударів. Це вимагає переосмислення традиційних підходів до кіберзахисту та розробки інтегрованих моделей реагування, що враховують взаємозв’язок між кіберпростором та фізичною інфраструктурою. Досвід України стає безцінним для міжнародної спільноти.

Проведене дослідження дозволяє зробити наступні висновки:

Систематизація кіберзагроз та вразливостей об’єктів критичної інфраструктури України виявила багатовимірний характер викликів, з якими стикається держава в умовах повномасштабної війни. Трансформація кіберзагроз від кримінально-мотивованих атак до стратегічних інструментів військового конфлікту засвідчує якісно новий етап розвитку кібервійни.

Аналіз класифікацій, запропонованих українськими та міжнародними дослідниками, показав необхідність адаптації теоретичних моделей до реалій гібридного конфлікту, де межі між різними типами загроз розмиваються.

Виявлені вразливості на технологічному, організаційному та людському рівнях формують комплексну картину системних слабкостей національної кіберінфраструктури.

Особливу тривогу викликає відставання темпів модернізації засобів захисту від темпів еволюції кіберзагроз, що створює стратегічне вікно вразливості для критичної інфраструктури. Досвід кібератак 2015-2024 років підтверджує, що найбільш руйнівні наслідки настають при координації цифрових операцій з фізичними ударами, що вимагає принципово нових підходів до кіберзахисту, заснованих на інтегрованому розумінні кіберпростору як повноцінного театру військових дій.

1.2 Секторальний аналіз кіберстійкості критичної інфраструктури України

Виявлені у попередньому підрозділі загальні кіберзагрози та вразливості критичної інфраструктури України набувають специфічних форм прояву в різних секторах економіки, що зумовлено технологічними особливостями, організаційними моделями управління та рівнем інвестицій у кібербезпеку. Секторальна диференціація об’єктів критичної інфраструктури за рівнем кіберстійкості є ключовою для розробки адресних стратегій захисту. Енергетичний сектор, будучи пріоритетною ціллю кібератак, демонструє найвищу інтенсивність інцидентів. Транспортна інфраструктура характеризується складністю забезпечення безпеки через розподіленість об’єктів. Телекомунікаційний сектор виявляє подвійну вразливість, виступаючи одночасно об’єктом атак та критичним інструментом координації. Фінансовий сектор, попри найвищий рівень кіберзрілості, залишається привабливою ціллю через потенціал економічної дестабілізації.

Енергетична інфраструктура України зазнала найбільш інтенсивного

кібертиску за період війни, що пояснюється її стратегічним значенням для функціонування всіх інших секторів економіки та життєзабезпечення населення. За даними Міжнародного агентства з енергетики, кількість кіберінцидентів у енергетичному секторі зросла удвічі порівняно з доповоєнним періодом [65].

Специфіка енергетики полягає у критичній залежності від промислових систем управління SCADA (Supervisory Control and Data Acquisition), які характеризуються тривалим терміном експлуатації (20-30 років), обмеженими можливостями швидкого оновлення програмного забезпечення та архітектурою, спроектованою в епоху, коли кіберзагрози не розглядалися як критичний ризик. Застарілість цих систем створює фундаментальну дилему: з одного боку, їх модернізація вимагає значних капітальних інвестицій та тривалих періодів зупинки виробництва, з іншого,- продовження експлуатації без оновлень залишає критичні вразливості відкритими для експлуатації атакуючими.

Атаки на енергетичну інфраструктуру спрямовані на досягнення подвійної мети: безпосереднє відключення електропостачання для дестабілізації суспільства та економіки, а також створення умов для пошкодження фізичного обладнання через маніпуляції параметрами технологічних процесів. Кейс атаки на українську енергетику у грудні 2015 року демонструє еволюцію тактики атакуючих та рівень їх технічної підготовки [49]. Використання шкідливого програмного забезпечення BlackEnergy для первинної компрометації корпоративних мереж, комбінація з інтенсивною соціальною інженерією для отримання облікових даних співробітників та синхронізована координація атак на кілька підстанцій одночасно створили прецедент першої у світі успішної кіберфізичної атаки, що призвела до масштабного блекауту.

Подальші атаки 2016-2024 років засвідчили якісне зростання рівня складності та використання спеціалізованого шкідливого програмного забезпечення Industroyer/CrashOverride, розробленого спеціально для атак на промислові протоколи керування енергомережами.

Все це свідчить про те, що енергетичний сектор демонструє критичну залежність від успішності публічно-приватної взаємодії у кіберзахисті. Державні

енергокомпанії володіють ресурсами для впровадження систем захисту, проте відсутність єдиних стандартів створює слабкі ланки. Приватні постачальники володіють експертизою, але потребують доступу до інформації про загрози. Тільки синергія державного регулювання, операційної спроможності енергокомпаній та технологічної експертизи приватного сектору може забезпечити адекватний рівень захисту.

Транспортна інфраструктура характеризується високою складністю та просторовою розподіленістю об'єктів, що створює множинні точки входу для потенційних кібератак та ускладнює забезпечення єдиного рівня захисту. Згідно з даними Міністерства інфраструктури України, транспортний сектор включає понад 5000 об'єктів різного рівня критичності, від міжнародних аеропортів та морських портів до локальних залізничних станцій та систем міського електротранспорту [57].

Специфіка транспорту полягає у критичній залежності від GPS-навігації для позиціонування та синхронізації руху, автоматизованих систем керування рухом поїздів та авіаційним трафіком, електронних систем продажу квитків та бронювання, інтегрованих логістичних платформ. Кожна з цих підсистем може стати об'єктом кібератаки з різними наслідками, від тимчасових затримок до створення небезпечних ситуацій, що загрожують життю пасажирів.

Ключовою проблемою транспортного сектору є відсутність централізованої системи моніторингу кіберзагроз та координації реагування між численними операторами інфраструктури. На відміну від фінансового сектору, де Національний банк України виконує функцію єдиного регулятора з чіткими вимогами до кібербезпеки, транспортна галузь характеризується фрагментацією відповідальності між Міністерством інфраструктури, Укрзалізницею, авіакомпаніями, портовими адміністраціями та муніципальними транспортними підприємствами. Ця організаційна роз'єднаність створює «сірі зони» у системі кіберзахисту, де відсутність чітких стандартів та механізмів обміну інформацією про загрози залишає вразливими критичні вузли транспортної мережі.

Міжнародний досвід демонструє зростаючу частоту та руйнівність

кібератак на транспортну інфраструктуру. Атака на Danish State Railways у лютому 2024 року, що призвела до повної паралізації залізничного сполучення на території Данії протягом кількох годин, продемонструвала вразливість навіть високотехнологічних європейських транспортних систем перед сучасними кіберзагрозами. Для України, транспортна інфраструктура якої зазнає додаткового навантаження через військові перевезення та евакуацію цивільного населення, кібератаки на транспорт можуть мати каскадний ефект, паралізуючи не тільки цивільну логістику, але й військову мобільність. Особливу тривогу викликає потенціал GPS-spoofing атак, здатних дезорієнтувати навігаційні системи та створити небезпечні ситуації для авіації та залізничного транспорту.

Телекомунікаційний сектор України також виявився в центрі гібридної війни, виконуючи подвійну роль об’єкта атак та критичного інструменту забезпечення зв’язку для військових та цивільних потреб. Атака на Київстар у грудні 2023 року стала найбільшим кіберінцидентом у телекомунікаційному секторі, що призвела до тимчасового припинення послуг для мільйонів абонентів та виявила критичні вразливості інфраструктури провідного оператора [2].

Комплексний аналіз інциденту показав використання атакуючими багаторівневої стратегії: початкова компрометація через експлуатацію вразливостей у мережевому обладнанні Cisco та Nokia, горизонтальне поширення по внутрішній мережі з використанням викрадених облікових даних адміністраторів, та фінальне застосування руйнівного шкідливого програмного забезпечення wiper-типу для знищення критичних даних та виведення з ладу систем управління мережею.

Відновлення повної функціональності мережі Київстар зайняло кілька тижнів, що підкреслює складність та довготривалість процесів відновлення після масштабних кібератак на телекомунікаційну інфраструктуру. Інцидент виявив системні проблеми галузі: надмірну залежність від імпортного обладнання з обмеженими можливостями оперативного патчінгу, недостатню сегментацію між управлінськими та операційними мережами, відсутність належних систем резервного копіювання критичних даних.

Парадокс телекомунікаційного сектору полягає у тому, що високий рівень цифровізації та автоматизації, з одного боку, забезпечує ефективність операцій, а з іншого – створює додаткові вектори атак та ускладнює процеси ізоляції скомпрометованих систем без припинення обслуговування абонентів.

Таблиця 1.3 – Порівняльний аналіз секторальної кіберстійкості

Сектор	*Рівень кіберзрілості*	*Основні загрози*	*Критичні вразливості*	*Пріоритетні заходи*
Енергетика	Середній	Атаки на SCADA, ransomware	Застаріле обладнання	Сегментація мереж, IDS/IPS
Транспорт	Середній-низький	GPS-spoofing, управління рухом	Відсутність резервів	Криптозахист, резервування
Телекомунікації	Середній-високий	DDoS, core-мережа	Імпортне обладнання	Диверсифікація постачальників
Фінанси	Високий	Фішинг, ransomware, платежі	Людський фактор	MFA, SOC 24/7

Джерело: розробка автора.

Секторальна диференціація зображена в таблиці 3.1 відображає не тільки технічні спроможності захисту, але й економічну спроможність інвестувати в кібербезпеку та рівень регуляторних вимог. Фінансовий сектор, перебуваючи під найсуворішим наглядом Національного Банку України демонструє найвищі показники кіберзрілості. Водночас енергетика та транспорт, маючи більш критичний вплив на фізичне функціонування держави, відстають у рівні захисту через складнощі модернізації промислових систем. Телекомунікаційний сектор знаходиться в процесі трансформації, стимульованої досвідом масштабних інцидентів.

Фінансовий сектор України, попри найвищий рівень кіберзрілості серед усіх галузей критичної інфраструктури, залишається пріоритетною ціллю кібератак через потенціал широкомасштабної економічної дестабілізації та підриву довіри громадян до банківської системи. За даними Національного банку України, у 2024 році зафіксовано понад 450 значних кіберінцидентів, з яких 12

класифіковані як критичні, що потребували залучення антикризових команд реагування та координації з правоохоронними органами [19].

Специфіка фінансових установ полягає у необхідності постійного балансування між забезпеченням високого рівня безпеки та підтриманням зручності доступу для клієнтів, оскільки надмірно складні процедури автентифікації можуть призвести до відтоку клієнтів до конкурентів з більш «friendly» інтерфейсами.

Стрімкий розвиток цифрового банкінгу та мобільних платіжних додатків, прискорений пандемією COVID-19 та військовим станом, кардинально розширив поверхню потенційних атак. Якщо традиційні банківські операції здійснювалися через захищені канали інтернет-банкінгу з потужними системами виявлення фрауду, то масовий перехід на мобільні додатки створив нові вразливості: від фішингових атак через SMS та месенджери до маніпуляцій з QR-кодами та експлуатації вразливостей мобільних операційних систем. Національний банк зафіксував зростання інцидентів з компрометацією мобільного банкінгу на 73% у 2024 році порівняно з 2023 роком, що свідчить про адаптацію атакуючих до нових каналів доступу до фінансових сервісів.

Міжнародний досвід демонструє різноманіття підходів до забезпечення кіберстійкості фінансового сектору. Європейська директива DORA встановлює комплексні вимоги до операційної стійкості [6]. США застосовують модель саморегулювання через FS-ISAC, що забезпечують обмін інформацією про загрози в реальному часі. Ізраїль впровадив модель обов’язкової участі фінансових установ у національних кібернавчаннях.

Оцінюючи міжнародні практики захисту фінансового сектору, варто наголосити на їх контекстуальній специфічності, що ускладнює пряме перенесення на українські реалії. Європейська директива DORA, попри свою комплексність, розроблялася для мирних умов функціонування фінансових ринків і не враховує необхідність підтримання безперервності бізнесу під час активних бойових дій. Американська модель саморегулювання через FS-ISAC базується на високому рівні довіри між учасниками ринку та потужній

технологічній інфраструктурі, що є викликом для України в умовах обмежених ресурсів.

Ізраїльський підхід обов'язкових кібернавчань є більш релевантним для України, враховуючи подібність безпекового контексту, проте потребує значних інвестицій у створення реалістичних сценаріїв та залучення експертів. Критично важливим для України є вироблення власної моделі, що синтезує кращі міжнародні практики з урахуванням специфіки воєнного стану.

Порівняльний аналіз міжнародних практик виявляє принципову відмінність між регуляторними підходами Європи, ринково орієнтованою моделлю США та безпеко-центричним підходом Ізраїлю. Європейська DORA, попри комплексність вимог, орієнтована на мирний час і недостатньо враховує необхідність швидкої адаптації до умов активного кіберконфлікту. Американська модель саморегулювання ефективна за умови високої зрілості галузі та довіри між учасниками, чого бракує в українських реаліях фрагментованої відповідальності.

Найбільш релевантним для України видається ізраїльський досвід інтеграції кіберзахисту фінансового сектору в загальнонаціональну систему оборони, що передбачає обов'язкову участь у навчаннях та створення резервних потужностей з урахуванням військових загроз. Однак пряме копіювання будь-якої з цих моделей без адаптації до української специфіки розподіленої власності, обмежених ресурсів та триваючого конфлікту може виявитися контрпродуктивним.

Таким чином, секторальний аналіз виявляє фундаментальну асиметрію між рівнем загроз та рівнем захищеності різних сегментів. Найбільш атакуємі сектори (енергетика та транспорт) характеризуються найнижчим рівнем кіберзрілості, що створює стратегічну вразливість. Фінансовий сектор демонструє можливість досягнення високого рівня захисту навіть в умовах інтенсивних атак. Перенесення практик фінансового сектору на енергетику та транспорт може стати шляхом до підвищення загальної кіберстійкості.

Енергетичний сектор потребує негайного впровадження систем виявлення

аномалій в промислових мережах, здатних розпізнавати підозрілу активність в реальному часі. Транспорт вимагає розробки національних стандартів кібербезпеки для автоматизованих систем управління. Телекомунікації потребують створення національних центрів моніторингу критичної мережевої інфраструктури. Фінансовий сектор має зосередитися на захисті від складних цільових атак через впровадження поведінкової аналітики.

Ключовим висновком секторального аналізу є необхідність переходу від ізольованих підходів до інтегрованої національної системи кіберстійкості.

Стратегічна координація зусиль на національному рівні отримала нормативне закріплення через Розпорядження Кабінету Міністрів України № 1163-р від 19 грудня 2023 року, яким затверджено план заходів з реалізації Стратегії кібербезпеки України [48]. Документ визначає ключові пріоритети щодо навчання спеціалістів, розвитку публічно-приватного партнерства та запровадження сучасних технологій у сфері кіберзахисту, спрямованих на підвищення стійкості та готовності критичної інфраструктури до кіберзагроз.

Критичний аналіз цього стратегічного документу виявляє суперечність між амбітністю запланованих заходів та реалістичністю їх виконання в умовах повномасштабної війни з обмеженими бюджетними ресурсами. Прийняття розпорядження наприкінці 2023 року, тобто майже через два роки після початку повномасштабного вторгнення, свідчить про певну інертність системи стратегічного планування у реагуванні на драматично змінене безпекове середовище. Акцент на «навчанні» та «публічно-приватному партнерстві» є безумовно важливим, проте відсутність чітких механізмів фінансування цих ініціатив ризикує перетворити документ на декларативний, що не матиме реального впливу на підвищення кіберстійкості критичної інфраструктури без супутніх бюджетних асигнувань та інституційних реформ.

Взаємозалежність секторів, особливо енергетики як основи функціонування всіх інших, вимагає координації зусиль. Створення секторальних центрів координації з представниками державних регуляторів, операторів та приватних провайдерів може стати організаційною основою.

Міжнародна практика організації кіберзахисту критичної інфраструктури демонструє ефективність комплексного підходу, що поєднує державне регулювання, приватну ініціативу та міжсекторальну координацію. Агентство кібербезпеки та захисту інфраструктури США (CISA), будучи національним координатором з безпеки критичної інфраструктури, реалізує модель публічно-приватного партнерства через Спільний центр кіберзахисту (JCDC), що об'єднує федеральні агентства, приватні компанії та міжнародних партнерів [25].

У 2024 році CISA надіслав 2131 попереджувальне повідомлення про загрози, що дозволило запобігти атакам до їх реалізації [53]. Ініціатива Secure by Design, започаткована CISA у 2023 році, переносить відповідальність за кібербезпеку з кінцевих користувачів на виробників технологій, вимагаючи впровадження безпеки на етапі проєктування продуктів.

Критичний аналіз американської моделі CISA виявляє як її сильні сторони, так і обмеження застосовності до українського контексту. Безперечною перевагою є системний підхід до координації між федеральними агентствами, приватним сектором та міжнародними партнерами, що забезпечує швидкий обмін інформацією про загрози та координацію відповіді. Проте американська модель базується на значних фінансових ресурсах,- лише у 2024 році CISA розподілило понад 300 мільйонів доларів грантів на підвищення кіберстійкості державних та місцевих органів влади [53].

Для України, що функціонує в умовах воєнної економіки з обмеженим бюджетом, пряме копіювання цієї моделі є нереалістичним. Водночас принципи організації роботи JCDC (горизонтальна координація, добровільний обмін інформацією та фокус на превентивних заходах) можуть бути адаптовані до українських реалій з урахуванням наявних ресурсів та специфіки воєнного стану.

Естонський досвід побудови національної системи кіберстійкості після масштабних атак 2007 року представляє особливий інтерес для України, враховуючи подібність геополітичного контексту та російської загрози. Кібератаки на Естонію у квітні-травні 2007 року, спровоковані перенесенням радянського військового меморіалу, стали першим випадком масштабної кібер-

агресії проти держави-члена НАТО, призвівши до паралізації урядових вебсайтів, банківських систем та медіа-платформ [51]. Естонська відповідь на ці атаки була багатовимірною: прийняття національної стратегії кібербезпеки у 2008 році, створення Центру передового досвіду кіберзахисту НАТО в Талліні (NATO CCDCOE), розвиток Кібероборонної одиниці Ліги оборони Естонії та впровадження обов'язкового навчання з кібербезпеки на всіх рівнях освіти [66].

Особливо важливим було формування культури кіберстійкості на рівні суспільства, де кожен громадянин розуміє свою роль у забезпеченні національної кібербезпеки.

Проте пряма екстраполяція естонського досвіду на українську ситуацію вимагає критичного переосмислення. По-перше, естонські атаки 2007 року, хоча й були масштабними, обмежувалися переважно DDoS-операціями і не супроводжувалися фізичною війною, що кардинально відрізняється від української реальності комбінованих кібер-кінетичних атак. По-друге, Естонія мала можливість розбудовувати свою кіберстійкість протягом майже двох десятиліть у відносно мирних умовах і з повною підтримкою НАТО та ЄС, тоді як Україна змушена одночасно відбивати кібератаки та протистояти повномасштабній військовій агресії [34]. По-третє, естонське суспільство є одним з найбільш цифровізованих у світі, що створювало як вразливості, так і можливості для швидкої адаптації цифрових захисних механізмів, тоді як український рівень цифровізації є нерівномірним та значно нижчим у багатьох критичних секторах.

Попри ці обмеження, естонський досвід інституціоналізації кібербезпеки, зокрема створення ефективної системи публічно-приватної взаємодії та інтеграції кіберзахисту в систему національної оборони, містить цінний досвід для України.

Комплексний аналіз міжнародного досвіду захисту критичної інфраструктури виявляє відсутність універсальної моделі, придатної для прямого перенесення на українські реалії. Американський, європейський та естонський підходи розроблялися в якісно інших безпекових контекстах, що

обмежує їх застосовність в умовах активного збройного конфлікту. Україна створює принципово новий тип кіберстійкості,- стійкості в умовах одночасного протистояння масштабній кібер-агресії та повномасштабній війні. Цей унікальний досвід має бути концептуалізований та систематизований як вклад у глобальну теорію та практику кіберзахисту критичної інфраструктури, оскільки потенційно відображає майбутнє воєн і конфліктів, де кібер- та кінетичні операції будуть нероздільно інтегровані.

Проведене дослідження дозволяє зробити наступні проміжні висновки:

Секторальний аналіз кіберстійкості критичної інфраструктури України виявив значну диференціацію між галузями за рівнем захищеності, технологічної зрілості та спроможності протистояти кіберзагрозам.

Фінансовий сектор демонструє найвищі показники кіберзрілості завдяки суворому регуляторному нагляду НБУ та значним інвестиціям у захист, проте залишається привабливою ціллю через потенціал широкомасштабної економічної дестабілізації.

Енергетичний сектор, перебуваючи під найінтенсивнішим кіберсправським тиском, виявляє критичні вразливості в застарілих промислових системах управління, що потребують складної та дорогої модернізації.

Транспортна інфраструктура характеризується високою складністю та розподіленістю об’єктів, що ускладнює забезпечення комплексного захисту.

Телекомунікаційний сектор, виконуючи подвійну роль об’єкта атак та критичного інструменту забезпечення зв’язку, перебуває в процесі болючої трансформації після масштабних інцидентів 2023-2024 років.

Міжнародний досвід, зокрема американської моделі CISA та естонського підходу до кіберстійкості, надає цінний досвід, проте вимагає критичної адаптації до українських реалій воєнного стану. Україна створює унікальну модель кіберстійкості в умовах одночасного протистояння кібер-агресії та повномасштабній війні, що може стати важливим внеском у глобальну практику захисту критичної інфраструктури.

РОЗДІЛ 2
ПУБЛІЧНЕ УПРАВЛІННЯ КІБЕРСТІЙКІСТЮ: ІНСТИТУЦІЙНА АРХІТЕКТУРА ТА МЕХАНІЗМИ КООРДИНАЦІЇ В УКРАЇНІ

2.1 Нормативно-правове регулювання, стратегічне планування та контрольно-наглядова діяльність держави при забезпеченні критичної інфраструктури

Формування ефективної національної системи кіберзахисту критичної інфраструктури в Україні потребує чітко визначеної інституційної архітектури з розмежованими повноваженнями та скоординованими механізмами взаємодії між державними органами. Патронюк С. аналізуючи роль ключових інституцій вказує, що Держспецзв'язок, Рада Національної Безпеки і Оборони України (РНБО), Служба безпеки України (СБУ) та Міністерство цифрової трансформації відіграють ключову роль у формуванні національної системи кібербезпеки, але існує дублювання функцій і проблеми взаємодії [51].

Зазначимо, що попри констатацію дублювання функцій, яка є обґрунтованою, дослідження Патронюка С. не пропонує конкретної моделі розмежування повноважень між органами. Визначення факту проблеми без пропозиції операційного механізму її розв'язання залишає питання на рівні діагностики, не переходячи до практичних рекомендацій. Особливо критичним є відсутність аналізу причин інституційного дублювання. Виникає питання,- чи це результат історичного формування системи, недосконалості законодавства, чи свідомої стратегії резервування функцій для підвищення надійності системи?

Нормативно-правову основу національної системи кібербезпеки закладено Законом України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII [56]. Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина,

суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів та основні засади координації їхньої діяльності. Закон встановлює, що основними суб'єктами національної системи кібербезпеки є Держспецзв'язок, Національна поліція, Служба безпеки України (СБУ), Міністерство оборони та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний Банк України.

Функціональний розподіл між основними суб'єктами національної системи демонструє спробу створити багаторівневу систему захисту. Держспецзв'язок як центральний орган виконавчої влади забезпечує формування державної політики, розробляє технічні стандарти та здійснює державний контроль. РНБО через Національний координаційний центр кібербезпеки виконує координуючу роль, забезпечуючи узгодження діяльності різних відомств. СБУ зосереджується на протидії кіберзлочинності, що загрожує національній безпеці, та виявленні розвідувально-підривної діяльності у кіберпросторі. Кіберполіція у складі Національної поліції відповідає за розслідування кіберзлочинів загальнокримінального характеру. Міністерство цифрової трансформації відповідає за цифровізацію державних послуг та формування політики у сфері електронного урядування.

Проте на практиці ця багаторівнева система створює проблеми координації. Лях В. та Савченко О. досліджують проблеми координації, наголошуючи що дублювання функцій між відомствами знижує швидкість реагування та ускладнює управління інцидентами кібербезпеки [45]. Відсутність чітких протоколів взаємодії між СБУ та Кіберполіцією призводить до ситуацій, коли одні й ті ж інциденти розслідуються паралельно різними відомствами.

Координаційна роль РНБО часто обмежується організацією нарад та підготовкою стратегічних документів, без реальних важелів впливу на оперативну діяльність суб'єктів. Держспецзв'язок, маючи формальні повноваження щодо державного контролю, стикається з обмеженими людськими та технічними ресурсами для його ефективного здійснення на всіх

об'єктах критичної інфраструктури.

Гульванська Ю. критично оцінює стан нормативної бази, стверджуючи що законодавство України в сфері кібербезпеки містить значні прогалини, що ускладнює координацію між державними органами і не забезпечує ефективну відповідь на сучасні кіберзагрози [29]. Омельченко І. підтримує цю позицію, зазначаючи що нормативно-правова база частково застаріла і відстає від нових загроз, що потребує оперативного перегляду і посилення контролю та санкцій [50].

Обидва дослідники справедливо вказують на проблему застарілості законодавства, проте їхні твердження потребують конкретизації. Не уточнюється, які саме положення законодавства є застарілими та які конкретні кіберзагрози не охоплюються чинною нормативною базою. Твердження про «значні прогалини» залишається занадто загальним без ідентифікації цих прогалин. Для практичної цінності дослідження необхідним є порівняльний аналіз українського законодавства з міжнародними стандартами та конкретна ідентифікація нормативних розривів.

Стратегічне планування в сфері кібербезпеки реалізується через Стратегію кібербезпеки України, затверджену Указом Президента України від 26 серпня 2021 року № 447/2021 [57]. Стратегія визначає пріоритети національних інтересів у сфері кібербезпеки, наявні та потенційно можливі кіберзагрози, цілі та завдання забезпечення кібербезпеки України. Стратегія встановлює три ключові напрями розбудови національної системи: стримування (посилення спроможності для унеможливлення агресії у кіберпросторі), кіберстійкість (здатність швидко адаптуватися до загроз і відновлювати стале функціонування), та взаємодія (розвиток координації та партнерства між суб’єктами).

Забашта Т. позитивно оцінює стратегічне планування, відзначаючи що Україна має суттєві успіхи у розробці Стратегії кібербезпеки, прикладом чого є її адаптація до європейських директив і розвиток координаційних механізмів між відомствами [34]. Проте Федоренко А. вказує на розрив між планами і реальним фінансуванням, що ускладнює імплементацію стратегії кібербезпеки [66].

Позиція Забашти Т. щодо «суттєвих успіхів» потребує емпіричної верифікації через конкретні метрики успішності стратегічного планування. Без показників виконання стратегічних цілей твердження залишається декларативним. Щодо позиції Федоренко А., то науковець обґрунтовано вказує на фінансову проблематику, але також не аналізує причини цього розриву. Чи це результат обмежень бюджету, неефективного планування видатків, чи низької пріоритетності кібербезпеки в розподілі ресурсів?

Визначаючи повноваження основних суб'єктів національної системи кібезбезпеки України спробуємо побудувати наступну таблицю:

Таблиця 2.1 – Розподіл повноважень основних суб'єктів національної системи кібербезпеки України

Державний орган	*Основні повноваження*	*Проблемні аспекти*
Держспецзв'язок	Формування та реалізація державної політики з кіберзахисту державних інформаційних ресурсів, кіберзахист критичної інфраструктури, державний контроль	Обмежені ресурси для виконання контрольно-наглядових функцій, недостатня оперативність реагування
РНБО	Координація та контроль діяльності органів виконавчої влади у сфері кібербезпеки через Національний координаційний центр кібербезпеки	Обмежені важелі впливу на оперативну діяльність суб'єктів, бюрократизація процесів координації
СБУ	Протидія розвідувально-підривній діяльності у кіберпросторі, виявлення та припинення кіберзлочинів проти національної безпеки	Відсутність публічної звітності про результати діяльності, обмежена взаємодія з приватним сектором через режим секретності
Міністерство цифрової трансформації	Формування державної політики у сфері цифровізації, розвиток електронного урядування, впровадження стандартів кібербезпеки	Нечітке розмежування повноважень з Держспецзв'язком, недостатні повноваження щодо забезпечення виконання вимог
Кіберполіція	Протидія кіберзлочинності, розслідування кіберінцидентів	Недостатня кількість спеціалізованих кадрів, обмежені технічні можливості для розслідування складних кіберзлочинів

Джерело: розробка автора.

Розподіл повноважень між п’ятьма основними суб’єктами національної системи кібербезпеки демонструє фрагментацію відповідальності, що ускладнює оперативну координацію під час кіберінцидентів. Особливо проблемним є накладання функцій Держспецзв’язку та Міністерства цифрової трансформації у сфері встановлення стандартів кібербезпеки. СБУ та Кіберполіція мають частково дублюючі повноваження щодо протидії кіберзлочинності, що може призводити до неефективного використання ресурсів та конкуренції між відомствами замість співпраці. Чернишенко П. аналізує роль Міністерства цифрової трансформації, зазначаючи що Мінцифра активно сприяє впровадженню цифрових стандартів і кращих практик у сфері кібербезпеки та підтримує ініціативи державно-приватного партнерства [67].

Процес адаптації українського законодавства до Директиви ЄС 2022/2555 (NIS2) про заходи для високого загального рівня кібербезпеки в Союзі є критично важливим для європейської інтеграції України [4]. Директива NIS2 встановлює єдині правові рамки для підтримки кібербезпеки в 18 критичних секторах по всьому ЄС, вимагаючи від держав-членів визначення національних стратегій кібербезпеки та співпраці для транскордонного реагування. Директива розширює сферу застосування порівняно з NIS1, охоплюючи середні та великі підприємства у критичних секторах, вимагаючи впровадження відповідних заходів управління кіберризиками та повідомлення про значні інциденти.

Коваленко О. аналізує виклики імплементації, зазначаючи що імплементація NIS2 створює підвищені вимоги до кіберзахисту, зокрема до обов’язкової звітності та посилення санкцій, але для України це виклик через нормативну невизначеність [40]. Зубарева І. підтримує важливість цього процесу, наголошуючи на важливості впровадження норм Директиви NIS2, які формують глобальний контекст посилення кібербезпеки держав [35].

Вважаємо, що Коваленко О. обґрунтовано ідентифікує виклик імплементації NIS2, проте не розкриває конкретних механізмів адаптації європейської директиви до українського правового поля в умовах воєнного стану. Особливо критичним є питання пріоритизації вимог директиви: які

положення NIS2 мають бути імплементовані першочергово, а які можуть бути відкладені з огляду на обмежені ресурси та воєнний стан. Відсутність такого аналізу робить рекомендації занадто загальними для практичного застосування.

Категоризація об’єктів критичної інфраструктури здійснюється відповідно до Постанови Кабінету Міністрів України від 9 жовтня 2020 року № 1109 «Деякі питання об’єктів критичної інфраструктури» [52], яка затверджує Порядок віднесення об’єктів до критичної інфраструктури, перелік секторів критичної інфраструктури та Методику категоризації. Постанова встановлює, що секторальні органи у сфері захисту критичної інфраструктури разом із операторами здійснюють категоризацію об’єктів своїх секторів згідно з методикою. Категоризація передбачає віднесення об'єктів до однієї з категорій критичності на основі оцінки потенційних наслідків порушення їх функціонування.

Загальні вимоги до кіберзахисту об’єктів критичної інфраструктури визначено Постановою Кабінету Міністрів України від 19 червня 2019 року № 518 [53]. Документ встановлює базові принципи та процедури мінімізації кіберризиків у державному та приватному секторі, передбачає впровадження заходів з управління кіберінцидентами, оцінки ризиків та обов’язкової моніторингової діяльності для операторів критичної інфраструктури.

Практичне застосування Постанови 518 виявило низку проблем. По-перше, загальні вимоги сформульовані занадто абстрактно, що ускладнює їх імплементацію операторами без спеціалізованих знань у сфері кібербезпеки. По-друге, відсутність чітких механізмів фінансування заходів кіберзахисту призводить до ситуації, коли оператори критичної інфраструктури, особливо в державному секторі, не мають бюджетних ресурсів для виконання встановлених вимог. По-третє, система моніторингу виконання вимог є недостатньо розвиненою. В ній відсутні автоматизовані засоби перевірки відповідності, а ручні перевірки є епізодичними та часто формальними.

Контрольно-наглядова діяльність у сфері кібербезпеки також залишається проблемною ділянкою державного управління. Климчук В. критично оцінює

ефективність контролю, зазначаючи що контрольно-наглядова діяльність часто носить формальний характер, брак ресурсів і нестача кваліфікації уповноважених органів знижує ефективність заходів [38]. Мельник Д. підтримує цю позицію, стверджуючи що брак ефективності санкцій та штучна формальність перевірок негативно впливає на загальний рівень кібербезпеки [47].

Обидва дослідники справедливо ідентифікують проблему формальності контрольно-наглядової діяльності, проте не пропонують альтернативної моделі контролю, яка б забезпечила реальну ефективність без надмірного адміністративного навантаження на операторів. Критика існуючої системи без пропозиції конструктивних альтернатив має обмежену практичну цінність. Необхідним є аналіз міжнародних практик ризик-орієнтованого нагляду, де контрольні заходи концентруються на об’єктах з найвищими ризиками, а не розподіляються рівномірно між усіма операторами незалежно від рівня загроз.

Проведене дослідження дозволяє зробити наступні проміжні висновки:

Аналіз державної системи забезпечення кіберзахисту критичної інфраструктури виявляє суперечність між амбітністю нормативно-правової бази та реальними можливостями її імплементації. Україна створила комплексну законодавчу основу, включаючи Закон про кібербезпеку (2017), Стратегію кібербезпеки (2021) та відповідні постанови уряду, проте практична реалізація цих документів стримується інституційними проблемами.

Ключовими викликами є дублювання функцій між Держспецзв’язком, СБУ, Міністерством цифрової трансформації та Кіберполіцією, що призводить до неефективної координації та дублювання зусиль. Процес адаптації до Директиви NIS2 ускладнюється необхідністю балансування між європейськими стандартами та реаліями воєнного стану.

Контрольно-наглядова діяльність потребує реформування від формального дотримання процедур до ризик-орієнтованого підходу з фокусом на об’єктах найвищої критичності. Розрив між стратегічним плануванням та фінансуванням залишається критичною перешкодою для досягнення

стратегічних цілей у сфері кібербезпеки.

2.2 Місце і значення приватного сектору у забезпеченні національної кіберстійкості України

Приватний сектор відіграє критично важливу роль у забезпеченні кіберстійкості національної економіки, оскільки більшість об'єктів критичної інфраструктури належить або управляється приватними компаніями. Проценко Є. аналізує інвестиційні тренди, зазначаючи що приватні інвестиції у кібербезпеку перевищують 9% IT-бюджетів, однак більшість компаній зіткнулися з недоліком досвідчених працівників [58].

Показник 9% від IT-бюджетів є відносним і не дає розуміння абсолютних обсягів інвестицій чи їх достатності для забезпечення належного рівня захисту. Для об'єктивної оцінки необхідним є порівняння українських показників з міжнародними бенчмарками та аналіз кореляції між рівнем інвестицій і фактичною кіберстійкістю організацій. Відсутність такого порівняльного аналізу робить неможливим визначення, чи є 9% достатнім рівнем інвестування для забезпечення ефективного захисту від сучасних кіберзагроз.

Шевчук Л. досліджує трансформацію корпоративного ставлення до кібербезпеки, стверджуючи що зростаюча кіберзагроза змушує бізнес змінити ставлення до кібербезпеки від формального виконання норм до стратегічної інвестиції, але брак кадрів і репутаційні ризики стримують відкритість [68]. Барбашина М. підтримує цю позицію, відзначаючи що мотивація бізнесу змінюється, кібербезпека стає фактором конкурентоспроможності та захисту репутації [21].

Вважаємо твердження про зміну мотивації бізнесу від compliance до стратегічного підходу потребує емпіричного підтвердження через конкретні кейс-стаді українських компаній. Без такої емпіричної бази залишається

незрозумілим, наскільки широко поширеним є цей тренд та які фактори сприяють або перешкоджають цій трансформації. Особливо важливим є питання: чи є ця зміна результатом усвідомлення загроз, чи реакцією на реальні інциденти, що вже мали місце?

Детальніший аналіз практик провідних українських компаній виявляє неоднорідність підходів до кібербезпеки залежно від сектору економіки. Фінансовий сектор демонструє найбільш формалізований підхід до кібербезпеки завдяки жорсткому регулюванню Національного банку України. Топ-банки за активами мають власні центри реагування на інциденти (SOC), що працюють цілодобово та інтегровані з міжнародними системами обміну інформацією про загрози. Проте менші банки та небанківські фінансові установи часто не мають достатніх ресурсів для створення власних SOC, покладаючись на аутсорсингові сервіси, що створює додаткові ризики через необхідність надання доступу до чутливої інформації зовнішнім провайдерам.

Енергетичний сектор стикається з особливими викликами через спадщину застарілих промислових систем управління, спроектованих без урахування кіберзагроз. Модернізація цих систем потребує значних інвестицій та не може бути здійснена швидко через необхідність забезпечення безперебійного постачання електроенергії. У відповідь на інтенсивні кібератаки під час війни, енергетичні компанії впровадили додаткові рівні захисту, включаючи сегментацію мереж, посилений моніторинг та створення резервних систем управління.

Телекомунікаційний сектор має подвійну роль: з одного боку, оператори є об’єктами критичної інфраструктури, з іншого,- надають послуги кібербезпеки для бізнес-клієнтів. Це створює як мотивацію до інвестицій у власну безпеку (для захисту репутації), так і можливості для монетизації експертизи через продаж сервісів захисту.

ІТ-сектор демонструє найвищу зрілість у питаннях кібербезпеки через природу бізнесу. Однак навіть тут існує значний розрив між великими компаніями, що працюють з міжнародними клієнтами та мають ресурси для

впровадження передових практик, та малими студіями, де кібербезпека часто обмежується базовими заходами через дефіцит фінансових та людських ресурсів.

Дмитренко О. аналізує роль галузевих об'єднань, зазначаючи що IT Ukraine Association та асоціації фінтех-компаній сприяють формуванню добровільних стандартів кібербезпеки та підтримують обмін інформацією між бізнесом і державою [32]. Ковальчук Л. розвиває цю тему, стверджуючи що колективне саморегулювання через галузеві об'єднання дає змогу підвищити взаємодію та обмін інформацією між приватним сектором і державою [41].

Загалом роль галузевих асоціацій оцінюється переважно позитивно, проте відсутній аналіз обмежень саморегулювання. Добровільні стандарти, на відміну від обов'язкових регуляторних вимог, мають обмежену ефективність, оскільки їх дотримання залежить від доброї волі учасників ринку. Компанії, які не є членами асоціацій або свідомо уникають дотримання добровільних стандартів для економії коштів, створюють ризики для всього сектору через ланцюги постачання та взаємозв'язки між системами.

Романенко О. ідентифікує кадрову проблематику як критичний виклик, зазначаючи що недостатня кількість кваліфікованих фахівців, еміграція і мобілізація погіршують ситуацію, що ставить під загрозу стійкість систем кібербезпеки [60]. Іванова Н. підтримує цю позицію, наголошуючи що важливо спрямувати зусилля на підвищення кваліфікації спеціалістів, комунікаційні навички та підготовку майбутніх кадрів [36].

Вважаємо, що кадрова проблематика справедливо ідентифікується як критичний виклик, проте дослідники не пропонують конкретних механізмів вирішення дефіциту фахівців. Традиційні підходи через розширення освітніх програм мають тривалий лаг-ефект та не вирішують термінових потреб. Альтернативні стратегії, такі як залучення іноземних фахівців, програми перекваліфікації спеціалістів з суміжних галузей, або автоматизація рутинних функцій кібербезпеки через штучний інтелект, залишаються поза межами аналізу.

Гончарук Н. досліджує публічно-приватне партнерство, стверджуючи що партнерство між державою і бізнесом в Україні розвивається повільно через брак стимулів і законодавчого базису, що стримує інвестиції у кіберзахист [27]. Співаковський С. конкретизує фінансову проблематику, зазначаючи що відсутність податкових пільг знижує мотивацію бізнесу інвестувати у довгострокові проєкти кібербезпеки [64].

Акцент на податкових стимулах є обґрунтованим, проте також не враховує ширшого контексту фіскальної політики держави в умовах воєнного стану. Надання податкових пільг для інвестицій у кібербезпеку конкурує з іншими пріоритетами використання обмежених бюджетних ресурсів. Більш реалістичним підходом могли б бути нефінансові стимули, такі як спрощення регуляторних процедур для компаній з високим рівнем кіберзахисту, пріоритетний доступ до державних контрактів, або публічне визнання лідерів галузі для створення репутаційних переваг.

Таблиця 2.2 – Секторальні відмінності у підходах до кібербезпеки в Україні

Сектор	*Рівень зрілості кібербезпеки*	*Драйвери інвестицій*	*Основні виклики*
Фінансовий	Високий	Жорстке регулювання НБУ, репутаційні ризики	Високі витрати на утримання SOC, дефіцит кадрів
Енергетичний	Середній	Критичність для національної безпеки, кібератаки під час війни	Legacy-системи, складність модернізації без зупинки виробництва
Телекомунікаційний	Середньо-високий	Подвійна роль (об’єкт захисту + провайдер послуг), комерційні можливості	Баланс між безпекою та доступністю послуг
IT	Високий (великі компанії) / Низький (малі)	Вимоги міжнародних клієнтів, репутація	Значний розрив між великими та малими гравцями
Інші сектори	Низький-середній	Регуляторний тиск, поодинокі інциденти	Обмежене розуміння загроз, брак ресурсів

Джерело: розробка автора.

Секторальний аналіз (Таблиця 2.2) виявляє значну неоднорідність у рівні

кіберзрілості українських компаній. Фінансовий та ІТ-сектори лідирують завдяки комбінації регуляторного тиску та комерційних стимулів, тоді як інші сектори демонструють відставання. Особливо проблемним є енергетичний сектор, де необхідність забезпечення безперервності постачання конфліктує з потребами модернізації застарілих систем. Ця неоднорідність створює вразливості на рівні національної економіки, оскільки кібератаки часто використовують найслабші ланки в ланцюгах постачання.

Міжнародний досвід провідних країн у сфері кібербезпеки демонструє різноманітні підходи до організації державно-приватного партнерства та створення ефективних механізмів обміну інформацією про кіберзагрози.

Так, у Сполучених Штатах Америки Агентство з кібербезпеки та безпеки інфраструктури (CISA) реалізує програму Automated Indicator Sharing (AIS), яка функціонує з 2016 року як механізм обміну індикаторами кіберзагроз між державним та приватним секторами. Програма базується на принципі добровільної участі та взаємної вигоди: приватні компанії надають інформацію про виявлені кіберінциденти та індикатори компрометації, натомість отримуючи доступ до урядових розвідувальних даних про загрози.

Технічна архітектура AIS побудована на використанні відкритих стандартів: Structured Threat Information Expression (STIX) для представлення інформації про кіберзагрози та Trusted Automated Exchange of Indicator Information (TAXII) для машинної комунікації між системами. Використання стандартизованих форматів дозволяє автоматизувати процес обміну та інтегрувати AIS з існуючими системами кібербезпеки учасників без потреби у складних технічних модифікаціях.

У 2022 році CISA запустила модернізовану версію програми,- AIS 2.0, яка відповідає на критику попередньої версії щодо недостатньої контекстуалізації даних та складності використання. Бюджет програми становив 31 мільйон доларів у 2021 році та 35 мільйонів у 2022 році, що свідчить про стратегічну важливість цієї ініціативи для національної безпеки США. Програма надає учасникам юридичний захист від відповідальності за обмін інформацією про

кіберзагрози, що усуває один з основних бар'єрів для відкритості приватного сектору.

Станом на 2024 рік CISA оголосила про двох річний стратегічний план модернізації підходів до обміну інформацією про кіберзагрози в рамках ініціативи Threat Intelligence Enterprise Services (TIES). Основний акцент робиться на забезпеченні контекстуалізації даних, що дозволяє учасникам пріоритизувати дії на основі релевантності загроз для їхніх конкретних систем, та на створенні механізмів, які забезпечують відчутну додаткову цінність для існуючих можливостей кібербезпеки організацій.

Критичною характеристикою американської моделі є її децентралізована природа: CISA виступає центральним хабом, але не створює єдину централізовану базу даних про загрози. Натомість агентство фасилітує peer-to-peer обмін між учасниками, дозволяючи організаціям зберігати контроль над власними даними. Ця архітектура підвищує довіру приватного сектору до системи, оскільки мінімізує ризики витоку конфіденційної інформації.

Національний центр кібербезпеки Великобританії (NCSC), створений у 2016 році як підрозділ GCHQ, реалізує фундаментально відмінну модель взаємодії з приватним сектором. Замість покладатися виключно на обмін інформацією, NCSC надає операторам критичної інфраструктури безкоштовні захисні сервіси, фінансовані з державного бюджету.

За даними Annual Review 2024, NCSC управляв 89 інцидентами національного значення протягом періоду з вересня 2023 по серпень 2024 року, включаючи 20 випадків ransomware-атак, 13 з яких класифіковано як nationally significant (зокрема атаки на British Library та траст National Health Service). Порівняно з попереднім роком кількість severe attacks зросла втричі, що демонструє інтенсифікацію кіберзагроз. У 2024 році NCSC отримав майже 2000 повідомлень про кібератаки, з яких 89 визнано nationally significant, включаючи 12 критичних інцидентів.

NCSC розробляє галузеві керівництва з кібербезпеки, адаптовані до специфічних загроз та технологічних особливостей різних секторів економіки.

Важливим досягненням є програма Cyber Essentials,- базовий сертифікаційний стандарт кібербезпеки, який у 2024 році отримали понад 33,000 організацій (зростання на 20% порівняно з попереднім роком). Дослідження показують, що організації з сертифікацією Cyber Essentials на 92% рідше подають claims до страхових компаній через кіберінциденти, що емпірично підтверджує ефективність базових захисних заходів.

Бюджет NCSC перевищує 100 мільйонів фунтів стерлінгів щорічно, що дозволяє агентству надавати широкий спектр безкоштовних сервісів: аналіз захищеності інфраструктури, консультації щодо впровадження захисних заходів, моніторинг загроз та раннє попередження про кібератаки. Ця модель усуває фінансові бар'єри для впровадження кіберзахисту малими та середніми операторами критичної інфраструктури, які не мають власних ресурсів для створення спеціалізованих підрозділів кібербезпеки.

Особливою характеристикою британської моделі є Vulnerability Reporting Service,- платформа для повідомлення про виявлені вразливості в урядових сервісах. У 2024 році спостерігалося значне зростання кількості повідомлень про вразливості, більшість яких стосувалася сервісів місцевих органів влади. Ця ініціатива створює механізм crowdsourced виявлення вразливостей, залучаючи широку спільноту дослідників безпеки до зміцнення національної кіберстійкості.

NCSC також відіграв ключову роль у захисті виборчого процесу під час загальних виборів 2024 року, впроваджуючи превентивні заходи для захисту інфраструктури та надаючи цільову підтримку особам з високим ризиком. Згідно зі звітом, вибори були проведені «smoothly and securely» без жодних значних інцидентів, що вплинули б на результат, демонструючи ефективність проактивного підходу до кіберзахисту.

Естонія створила унікальну модель цифрової довіри через платформу X-Road (X-Tee в естонському контексті), яка функціонує з 2001 року як національна інфраструктура обміну даними. X-Road є open-source рішенням, що забезпечує безпечний обмін даними між понад 450 публічними та приватними організаціями через 1,300 підключених IT-систем, підтримуючи функціонування

більше 3,000 цифрових сервісів.

Станом на грудень 2024 року Естонія досягла безпрецедентного показника 100% цифровізації урядових сервісів, піднявшись з 16-го місця у 2018 році до 2-го місця у 2024 році в United Nations E-Government Development Index. Це досягнення безпосередньо пов'язане з функціонуванням X-Road як технологічного хребта цифрової держави.

Архітектурним принципом X-Road є децентралізоване зберігання даних: кожна організація управляє власною базою даних, але може надавати контрольований доступ до неї іншим авторизованим учасникам через захищені API. Система використовує цифрові підписи для верифікації автентичності та цілісності даних, шифрування для захисту конфіденційності під час передачі, та детальне логування всіх транзакцій для забезпечення підзвітності. Ця розподілена архітектура усуває єдину точку відмови та підвищує загальну кіберстійкість системи.

Унікальною характеристикою X-Road є можливість федерації з’єднання двох незалежних X-Road екосистем для транскордонного обміну даними. У лютому 2018 року Естонія та Фінляндія з’єднали свої системи X-Road, створивши першу у світі транснаціональну платформу обміну урядовими даними. Ця федерація дозволяє громадянам та бізнесам обох країн отримувати безшовні транскордонні послуги у сферах охорони здоров’я, оподаткування та бізнес-реєстрації. Понад 100,000 громадян Естонії є щоденними комутерами до Фінляндії, що робить транскордонну інтероперабельність критично важливою для обох економік.

Дві треті організацій, підключених до естонського X-Road, є приватними компаніями, що демонструє успішну інтеграцію приватного сектору в національну систему цифрового урядування. Платформа створює екосистему, де приватні компанії можуть будувати інноваційні сервіси на основі урядових даних, отримуючи стандартизований та безпечний доступ до необхідної інформації.

Глобальне поширення X-Road підтверджує його технологічну зрілість:

станом на 2024 рік платформа впроваджена у понад 25 країнах, включаючи Україну (платформа «Трембіта», запущена у 2019 році), Японію, Малайзію, Намібію та Аргентину. Nordic Institute for Interoperability Solutions (NIIS), створений Естонією, Фінляндією та Ісландією у 2017 році, координує розвиток X-Road як міжнародного стандарту цифрової інтероперабельності.

Таблиця 2.3 – Порівняльна характеристика міжнародних моделей державно-приватного партнерства у кібербезпеці

Характеристика	*США (CISA AIS)*	*Великобританія (NCSC)*	*Естонія (X-Road)*
Рік запуску	2016 (AIS 2.0 у 2022)	2016	2001
Основний принцип	Добровільний обмін загрозами	Урядові захисні сервіси	Платформа довіри та інтероперабельності
Річний бюджет	$31-35 млн (тільки AIS)	£100+ млн	Розподілений між учасниками
Модель фінансування	Державне фінансування хабу	Повне державне фінансування сервісів	Hybrid: держава + приватний сектор
Юридичні стимули	Liability protection для учасників	Cyber Essentials certification	Data sovereignty та privacy by design
Технічна основа	STIX/TAXII стандарти	Bespoke services + standards	Open-source distributed architecture
Кількість учасників	Тисячі організацій	33,000+ (Cyber Essentials 2024)	450+ організацій, 1,300+ систем
Транскордонна інтеграція	Обмежена (двосторонні угоди)	Обмежена (через Brexit)	Федерація з Фінляндією з 2018
Роль приватного сектору	Рівноправний учасник обміну	Споживач урядових сервісів	Два третіх учасників-приватні
Виміряні результати (2024)	Continuous modernization	92% reduction в insurance claims	100% digitalization досягнута

Джерело: розробка автора.

Порівняльний аналіз (Таблиця 2.3) виявляє, що не існує універсальної моделі державно-приватного партнерства у кібербезпеці, яка була б оптимальною для всіх контекстів. Американська модель добровільного обміну ефективна в умовах розвиненої культури кібербезпеки та високої довіри між бізнесом і урядом, які історично формувалися в США. Британська модель безкоштовних урядових сервісів потребує значних бюджетних витрат, що може

бути викликом для країн з обмеженими фіскальними можливостями. Естонська модель X-Road була розроблена з нуля як частина пост-радянської трансформації, коли країна мала можливість будувати цифрову інфраструктуру без обмежень legacy-систем.

Для України найбільш релевантними є елементи всіх трьох моделей, адаптовані до специфічного контексту. Від США варто запозичити принцип юридичного захисту учасників обміну інформацією для зниження бар'єрів відкритості. Від Великобританії,- концепцію базових стандартів кібербезпеки на кшталт Cyber Essentials, які можуть стати обов'язковими для операторів критичної інфраструктури. Від Естонії,- технологічну платформу інтероперабельності, яка вже частково впроваджена через «Трембіту», але потребує масштабування та інтеграції з європейськими системами в контексті NIS2.

Критичним є питання довіри між приватним сектором та державними органами безпеки. В умовах України історична недовіра до спецслужб та побоювання щодо використання наданої інформації для контрольно-наглядових цілей є значним бар'єром. Подолання цього бар'єру потребує не лише технологічних рішень (як-от анонімізація даних в AIS), але й інституційних реформ, включаючи створення незалежних oversight механізмів для моніторингу використання інформації державними органами.

Транскордонна інтероперабельність, продемонстрована естонсько-фінською федерацією X-Road, є стратегічно важливою для України в контексті європейської інтеграції. Створення механізмів обміну інформацією про кіберзагрози з країнами-членами ЄС через стандартизовані протоколи може значно підвищити ефективність національної системи кіберзахисту, надаючи доступ до ширшого контексту загроз та можливості координованого реагування на транснаціональні кіберкампанії.

Резюмуючи слід зазначити, що роль приватного сектору у забезпеченні кіберстійкості України еволюціонує від пасивного об'єкта регулювання до активного партнера держави у створенні національної системи кіберзахисту.

Провідні українські компанії демонструють зростаючі інвестиції у кібербезпеку (близько 9% від IT-бюджетів), проте ця позитивна динаміка обмежується структурними викликами.

Критичний дефіцит кваліфікованих фахівців посилюється еміграцією та мобілізацією, відсутність податкових стимулів знижує мотивацію до довгострокових інвестицій, репутаційні ризики стримують відкритість у повідомленні про інциденти.

Галузеві асоціації відіграють позитивну роль у формуванні добровільних стандартів, проте саморегулювання має обмежену ефективність без державної підтримки та координації. Державно-приватне партнерство розвивається повільно через відсутність чіткого законодавчого базису та механізмів взаємодії.

Для посилення ролі приватного сектору необхідним є створення екосистеми стимулів (як фінансових, так і нефінансових), розвиток програм підготовки кадрів, та формування культури довіри між бізнесом і державними органами для ефективного обміну інформацією про загрози.

Міжнародний досвід провідних країн у сфері кібербезпеки демонструє різноманітні підходи до організації державно-приватного партнерства та створення ефективних механізмів обміну інформацією про кіберзагрози. Аналіз цих моделей є критично важливим для України в контексті адаптації кращих практик до власних умов функціонування національної системи кіберзахисту.

РОЗДІЛ 3
МОДЕЛЬ ІНТЕГРАЦІЙНОЇ ПУБЛІЧНО-ПРИВАТНОЇ ВЗАЄМОДІЇ У СФЕРІ КІБЕРСТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

3.1 Міжнародний досвід організації публічно-приватної співпраці у сфері кіберзахисту критичної інфраструктури

Ефективне забезпечення кіберстійкості критичної інфраструктури в сучасних умовах є неможливим без тісної взаємодії між державним та приватним секторами. Міжнародний досвід демонструє різноманітні моделі організації такої співпраці, кожна з яких відповідає специфічним національним контекстам, рівням загроз та інституційним традиціям. Компаративний аналіз провідних моделей дозволяє ідентифікувати ключові елементи успішної публічно-приватної взаємодії та адаптувати їх до українських реалій.

Естонська модель: трансформація після кризи 2007 року.

Естонська модель публічно-приватного партнерства у кібербезпеці сформувалася як відповідь на масштабні кібератаки 2007 року, які паралізували критичну інфраструктуру країни. Ці події стали каталізатором фундаментальної перебудови національної системи кіберзахисту з акцентом на інтеграцію приватного сектору як рівноправного партнера держави. Ottis та Lorents підкреслюють, що естонський досвід свідчить про комплексність кібербезпеки як задачі, яка потребує координації міжурядових структур та активної залученості приватного сектору, оскільки поняття кіберпростору включає не лише технічні компоненти, але й соціальні та політичні аспекти [13].

Rebane зазначає, що після кібернападів 2007 року Естонія сформувала модель ефективної публічно-приватної взаємодії, в якій ключову роль відіграє державний департамент інформаційних систем (RIA) та технологічна платформа X-Road, що дозволяє забезпечувати безпечний обмін даними між державою та

бізнесом, демонструючи важливість довіри і прозорої координації для національного кіберзахисту [14, 24]. Як зазначалося в попередньому розділі, платформа X-Road стала технологічною основою цієї інтеграції, забезпечуючи безпечний обмін даними між державними та приватними організаціями. Департамент державних інформаційних систем (RIA) виконує функцію координатора взаємодії, забезпечуючи методологічну підтримку, розробку стандартів та моніторинг їх дотримання.

Критично важливою особливістю естонської моделі є участь приватного сектору в національній кібероборони через створення Кіберліги оборони, тобто добровільного резерву IT-спеціалістів з приватного сектору, які в разі кіберкризи можуть бути оперативно залучені до захисту критичної інфраструктури. Ця модель військово-цивільної синергії дозволяє максимально ефективно використовувати обмежені людські ресурси країни з населенням 1.3 мільйони людей.

Естонія активно підтримує Україну в розбудові національної системи кіберзахисту через програми Академії електронного управління, передаючи накопичений досвід організації публічно-приватної співпраці. Ця підтримка є особливо цінною, оскільки Естонія та Україна стикаються з подібними викликами гібридної війни та кібератак з боку одного й того ж агресора.

Американська модель: секторальні центри обміну інформацією.

Сполучені Штати розробили модель публічно-приватної взаємодії, яка базується на секторальному принципі організації через Information Sharing and Analysis Centers (ISACs). Кожен ISAC обслуговує конкретний сектор економіки (фінанси, енергетику, охорону здоров'я, транспорт тощо) і функціонує як довірче середовище для обміну оперативною інформацією про кіберзагрози між учасниками сектору та урядовими агентствами.

За даними ENISA, ISACs забезпечують централізовану платформу для обміну оперативною інформацією про кіберзагрози між державними та приватними структурами, сприяючи швидкому виявленню та реагуванню [5]. Anomali підкреслює, що ISACs створюють довірче середовище, де учасники

безпечно обмінюються інформацією про загрози, забезпечуючи раннє попередження та підтримку спільних заходів [1]. Ця модель «довіреного середовища» є ключовою для подолання природної нехоті бізнесу розкривати інформацію про власні вразливості та інциденти.

CISA, як було детально розглянуто в попередньому розділі, виступає координуючим хабом для ISACs через програму Automated Indicator Sharing (AIS), забезпечуючи горизонтальний обмін інформацією між секторами. Критично важливим елементом американської моделі є National Institute of Standards and Technology (NIST) Cybersecurity Framework, тобто добровільна структура управління кіберризиками, яка базується на п’яти функціях: ідентифікація, захист, виявлення, реагування та відновлення для комплексного управління ризиками [15].

Visure Solutions підкреслює, що NIST CSF допомагає організаціям адаптувати підходи до кіберризиків, поєднуючи гнучкість та найкращі практики у кібербезпеці [18]. Добровільний характер NIST Framework дозволяє організаціям різного розміру та зрілості впроваджувати його поетапно, адаптуючи до власних специфічних потреб та ресурсних можливостей. Водночас, де-факто NIST Framework став галузевим стандартом, на який посилаються регуляторні вимоги та контракти з державними органами, створюючи непрямі стимули для його впровадження.

Вважаємо, що американська модель ISACs демонструє ефективність секторального підходу, який враховує специфічні загрози та технологічні особливості різних галузей економіки. Проте ця модель потребує критичної маси учасників у кожному секторі для створення ефекту мережі, коли обмін інформацією стає взаємовигідним. В умовах України, де деякі сектори економіки є значно менш розвиненими порівняно з США, пряме копіювання секторальної моделі може призвести до створення «порожніх» ISACs без достатньої кількості активних учасників.

Більш прагматичним може бути гібридний підхід, де секторальні центри створюються лише для найбільш критичних та розвинених галузей (енергетика,

фінанси, телеком), тоді як менші сектори об'єднуються в мультисекторальний ISAC.

Британська модель: урядова платформа CiSP.

Велика Британія реалізує модель публічно-приватної взаємодії через Cyber Security Information Sharing Partnership (CiSP),- безпечну віртуальну платформу для обміну інформацією про кіберзагрози між урядом та приватним сектором. Як зазначає офіційна сторінка UK National Cyber Security Centre, CiSP створює безпечну віртуальну платформу для обміну інформацією про кіберзагрози між урядом та приватним сектором, підтримуючи підвищення кіберзрілості бізнесу [16].

Мартін Т. підкреслює, що програма дозволяє приватним компаніям отримувати реальнодіючі підказки і просувати найкращі практики для зменшення ризиків [46]. На відміну від американської секторальної моделі, CiSP є мультисекторальною платформою, відкритою для організацій з будь-яких галузей економіки. Станом на 2024 рік CiSP налічує понад 13,000 зареєстрованих організацій, що робить її однією з найбільших національних платформ обміну інформацією про кіберзагрози у світі.

Ключовою характеристикою CiSP є її інтеграція з послугами NCSC: учасники платформи отримують доступ до урядових аналітичних продуктів, попереджень про загрози та методологічних рекомендацій. NCSC також організовує через CiSP програми підвищення кіберзрілості для малого та середнього бізнесу, надаючи безкоштовні навчальні ресурси та інструменти самооцінки. Як було зазначено в попередньому розділі, програма Cyber Essentials, інтегрована з CiSP, демонструє високу ефективність: організації з сертифікацією на 92% рідше подають claims до страхових компаній.

На нашу думку, британська модель CiSP є особливо релевантною для України через її мультисекторальний характер та акцент на підтримку малого та середнього бізнесу. Проте успіх CiSP значною мірою залежить від довіри приватного сектору до урядових інституцій, яка у Великобританії є історично високою. В українському контексті, де довіра бізнесу до державних органів

безпеки є обмеженою через побоювання використання інформації для контрольно-наглядових цілей, створення подібної платформи потребує додаткових правових гарантій конфіденційності та незалежних механізмів oversight для запобігання зловживанням.

Ізраїльська модель: військово-цивільна інтеграція.

Ізраїль, функціонуючи в умовах перманентної безпекової загрози, розробив унікальну модель публічно-приватного партнерства, яка інтегрує військові та цивільні ресурси для забезпечення національної кібероборони. Так, Вишневська П.В. зазначає, що ізраїльський кібердиректорат поєднує військовий та цивільний сектори, що дає змогу ефективно координувати національну кібероборону, залучаючи приватний сектор і міжнародних партнерів [23]. В свою чергу, Кузьменко І.С. підкреслює, що військово-цивільна синергія і розвинуті координаційні центри забезпечують швидке реагування на кіберзагрози, що є прикладом для України [43].

Національний кібердиректорат Ізраїлю виконує функцію центрального координатора між військовими підрозділами кіберкомандування, цивільними урядовими агентствами та приватним сектором. Критично важливою є система підготовки кадрів через військову службу: елітні підрозділи кіберкомандування (зокрема знаменитий Unit 8200) функціонують як інкубатори талантів, які після завершення служби переходять до приватного сектору, створюючи потужну екосистему кібербезпекових стартапів. Ця ротація кадрів між військовим та приватним секторами забезпечує постійний трансфер технологій та методологій.

Ізраїльська модель також передбачає активну участь приватного сектору в розробці оборонних кіберрішень через державні контракти та програми підтримки інновацій. Держава виступає не лише регулятором, але й першим клієнтом для інноваційних кібербезпекових продуктів, створюючи попит та сприяючи розвитку національної індустрії кібербезпеки.

Вважаємо Ізраїльську модель високорелевантною для України через подібність безпекового контексту обох країн, що функціонують в умовах активного протистояння з агресором. Система підготовки кадрів через військову

службу може бути частково адаптована в українських реаліях, де значна кількість ІТ-спеціалістів проходить військову службу під час повномасштабної війни. Проте пряме копіювання ізраїльської моделі стримується відмінностями у масштабі: населення Ізраїлю становить приблизно 9 мільйонів, тоді як України понад 40 мільйонів, що вимагає пропорційно більших ресурсів для створення еквівалентної системи.

Досвід Польщі та країн Балтії: регіональна співпраця в контексті NIS2.

Польща та країни Балтії (Литва, Латвія, Естонія) демонструють модель регіональної співпраці у сфері кібербезпеки в рамках Європейського Союзу. Гончарук Н.В. відзначає, що Балтійські країни і Польща активно імплементували директиву NIS2, створюючи міждержавні платформи обміну інформацією та стандарти кіберзахисту [26]. Андрієвський С.І. підкреслює, що регіональні ініціативи ЄС у сфері кібербезпеці посилюють колективний захист критичної інфраструктури через інформаційний обмін та спільні навчання [20].

Ці країни сформували неформальне регіональне співтовариство практиків кібербезпеки, що регулярно проводить спільні кібернавчання, обмінюється інформацією про актуальні загрози та координує позиції у міжнародних форумах. Географічна близькість до РФ та спільний досвід протистояння російським кібератакам створює природний стимул для тісної співпраці. Ці країни також активно використовують можливості EU Cybersecurity Agency (ENISA) для отримання методологічної підтримки та участі в загальноєвропейських ініціативах.

Процес імплементації Директиви NIS2 в цих країнах характеризується прагматичним підходом: замість створення нових інституцій, функції координації кібербезпеки інтегруються в існуючі структури з чітким розмежуванням повноважень. Особлива увага приділяється транскордонному обміну інформацією та створенню механізмів взаємної підтримки під час кіберкриз.

Досвід Польщі та Балтії демонструє важливість регіональної співпраці для посилення національної кіберстійкості. За нашим переконанням, для України

регіональне співробітництво може бути розвинуто в кількох напрямах: з країнами Вишеградської групи, з країнами Балтії через існуючі зв'язки програм цифрової трансформації, та з країнами Східного партнерства. Критично важливим є уникнення дублювання зусиль та концентрація на практичному обміні інформацією про загрози, спільних навчаннях та розробці сумісних технічних рішень, а не на бюрократичних структурах регіональної координації.

Синтез міжнародного досвіду: ключові елементи успішних моделей.

Компаративний аналіз міжнародних моделей публічно-приватної взаємодії дозволяє ідентифікувати декілька наскрізних елементів, присутніх у всіх успішних практиках незалежно від національного контексту.

По-перше, всі розглянуті моделі базуються на принципі довірчого середовища, де приватний сектор має гарантії конфіденційності та захисту від негативних наслідків розкриття інформації про інциденти. Юридичні механізми захисту (як у США через CISA Act) або технологічні рішення анонімізації (як у британській CiSP) є необхідною передумовою для відкритості бізнесу.

По-друге, успішні моделі забезпечують взаємну вигоду для учасників: приватний сектор отримує доступ до урядової розвідувальної інформації, аналітичних продуктів та методологічної підтримки в обмін на надання даних про інциденти та загрози. Односторонній потік інформації від бізнесу до держави без зворотного надання цінності призводить до пасивності учасників.

По-третє, всі моделі передбачають технологічну інфраструктуру для автоматизованого обміну інформацією в машинно-читабельних форматах. Використання стандартизованих протоколів (STIX/TAXII в США, інтеграція з X-Road в Естонії) дозволяє масштабувати обмін без пропорційного зростання адміністративного навантаження.

По-четверте, успішні моделі інтегрують підготовку кадрів як невід’ємну частину публічно-приватного партнерства. Ротація кадрів між державним та приватним секторами (як в Ізраїлі), спільні навчальні програми (як в Естонії), або підтримка сертифікаційних програм (як Cyber Essentials у Великобританії) забезпечують поширення знань та найкращих практик.

По-п’яте, ефективні моделі включають механізми регулярної практичної взаємодії через спільні кібернавчання, tabletop exercises та real-world incident response drills. Ці активності дозволяють тестувати процедури координації в контрольованих умовах та виявляти слабкі місця до настання реальних кризових ситуацій.

Таким чином, компаративний аналіз міжнародного досвіду демонструє, що успішна публічно-приватна взаємодія у сфері кіберзахисту критичної інфраструктури не є результатом простого копіювання універсальних рецептів, а потребує адаптації до національного контексту з урахуванням інституційних традицій, рівня загроз, економічного розвитку та культури довіри між державою та бізнесом.

Водночас, незалежно від обраної моделі, ключовими факторами успіху залишаються політична воля на найвищому рівні, правові гарантії конфіденційності для учасників обміну інформацією, технологічна інфраструктура автоматизованого обміну, інвестиції в людський капітал та механізми регулярної практичної взаємодії.

Для України найбільш релевантними є досвіди Естонії (через подібність масштабу та трансформаційний характер реформ), Ізраїлю (через подібність безпекового контексту), та країн Балтії і Польщі (через географічну близькість та спільність загроз). Синтез цих практик має стати основою для розробки власної моделі, яка враховуватиме українську специфіку та максимально використовуватиме можливості міжнародної підтримки.

3.2 Рекомендації щодо вдосконалення публічно-приватної взаємодії в Україні: інституційні, правові, організаційні та технологічні аспекти

Розробка ефективної моделі публічно-приватної взаємодії для України потребує комплексного підходу, який враховує як міжнародний досвід успішних

практик, так і специфічний національний контекст. Гульванська Ю.А. пропонує створення інтегрованої системи кіберзахисту та удосконалення міжвідомчої координації, включно із запровадженням інституту урядового координатора [29]. РНБО України визнає, що недостатня координація між відомствами і відсутність ефективних механізмів взаємодії стримує розвиток кіберстійкості країни [59]. Наступні рекомендації синтезують досвід інших держав з урахуванням української специфіки.

1. Інституційні рекомендації.

Створення ефективної інституційної архітектури публічно-приватної взаємодії, що потребує балансу між централізацією стратегічної координації та децентралізацією оперативного виконання. Досвід Естонії та Ізраїлю демонструє, що наявність єдиного координуючого органу з чіткими повноваженнями є критично важливою для подолання міжвідомчої роз'єднаності.

Національна платформа кіберстійкості має функціонувати як постійно діючий координаційний орган при РНБО з участю представників Держспецзв'язку, СБУ, Міністерства цифрової трансформації, ключових операторів критичної інфраструктури та галузевих асоціацій бізнесу. На відміну від епізодичних нарад, платформа повинна мати власний секретаріат, бюджет та повноваження щодо розробки методологічних рекомендацій. Естонський досвід RIA демонструє, що такий орган може ефективно виконувати роль мосту між державою та бізнесом, будучи достатньо близьким до уряду для впливу на політику, але достатньо незалежним для збереження довіри приватного сектору.

Інститут урядового координатора з кіберстійкості критичної інфраструктури на рівні віце-прем'єра або секретаря РНБО забезпечить політичний вага для подолання міжвідомчих бар'єрів та прийняття стратегічних рішень. Досвід Ізраїлю показує, що централізована координація на найвищому політичному рівні дозволяє швидко мобілізувати ресурси та забезпечити узгодженість дій під час кризових ситуацій. Координатор має головувати в Національній платформі кіберстійкості та мати мандат на координацію

бюджетних процесів, пов'язаних з кібербезпекою критичної інфраструктури.

Секторальні координаційні центри за галузевим принципом (енергетика, фінанси, телекомунікації, транспорт, охорона здоров’я) мають створюватися на базі існуючих галузевих регуляторів або асоціацій операторів. Американський досвід ISACs демонструє ефективність секторального підходу, який враховує специфічні технологічні особливості та загрози кожної галузі. Проте в українських умовах доцільним є поетапне створення таких центрів, починаючи з найбільш критичних та організаційно зрілих секторів. Секторальні центри мають фокусуватися на практичному обміні інформацією про загрози, спільних навчаннях та розробці галузевих методологічних рекомендацій, а не на дублюванні регуляторних функцій.

2. Правові рекомендації.

Правова основа публічно-приватної взаємодії потребує комплексного реформування для створення стимулів до співпраці та усунення бар'єрів для обміну інформацією. Проєкт Закону «Про критичну інфраструктуру» спрямований на забезпечення цілісності та захисту критичної інфраструктури шляхом установлення чітких повноважень і обов’язків [37]. Проте прийняття цього закону є лише першим кроком у створенні комплексної правової рамки.

Закон «Про критичну інфраструктуру» має чітко розмежувати повноваження між Держспецзв’язком як регулятором технічних стандартів кіберзахисту, СБУ як органом протидії кібершпигунству та розвідувально-підривній діяльності, Міністерством цифрової трансформації як координатором цифровізації та секторальними регуляторами як відповідальними за специфічні галузеві вимоги. Досвід Польщі та Балтії демонструє, що успішна імплементація NIS2 базується на чіткому законодавчому розмежуванні функцій без дублювання.

Обов’язкова звітність про кіберінциденти має супроводжуватися правовими гарантіями конфіденційності та захисту від негативних наслідків. Британський досвід CiSP та американський CISA Act показують, що бізнес готовий ділитися інформацією про інциденти за умови юридичного захисту від

використання цієї інформації для санкцій або публічного розкриття.

Законодавство має встановлювати, що інформація про кіберінциденти, надана добровільно або у виконання обов'язкової звітності, не може бути використана для накладення штрафів (якщо інцидент не є результатом грубого недбальства), не підлягає розкриттю третім сторонам без згоди оператора, та захищена від запитів на основі законодавства про доступ до публічної інформації.

Податкові стимули для інвестицій у кібербезпеку мають включати знижку на прибуток для витрат на впровадження сертифікованих систем кіберзахисту, пришвидшену амортизацію для обладнання та програмного забезпечення кібербезпеки, та податковий кредит для витрат на підготовку та сертифікацію персоналу з кібербезпеки. Досвід європейських країн показує, що податкові стимули є ефективним механізмом для прискорення впровадження передових практик, особливо в секторі малого та середнього бізнесу, де бюджетні обмеження є найбільш критичними.

Правові гарантії для обміну інформацією про загрози мають включати виключення з-під дії антимонопольного законодавства для колективних дій з протидії кіберзагрозам, захист комерційної таємниці при обміні технічними деталями про вразливості, та обмеження відповідальності за добросовісний обмін інформацією, навіть якщо ця інформація згодом виявиться неточною. Американський досвід демонструє, що без таких правових гарантій компанії уникають обміну інформацією через побоювання юридичних наслідків.

3. Організаційні рекомендації

Організаційна інфраструктура публічно-приватної взаємодії має забезпечувати постійну комунікацію, регулярну практичну взаємодію та механізми швидкого реагування на кризові ситуації.

Національний центр обміну інформацією про кіберзагрози (UA-ISAC) за секторальним принципом має функціонувати як central clearing house для збору, аналізу та дисемінації інформації про кіберзагрози. NATO Cooperative Cyber Defence Centre of Excellence надає експертну підтримку створення

Національного центру обміну інформацією про кіберзагрози [12]. Центр має працювати в режимі 24/7, забезпечуючи оперативний обмін інформацією між державними органами та операторами критичної інфраструктури. Досвід американських ISACs та британської CiSP демонструє, що ефективність такого центру визначається не лише технологічною платформою, але й людським капіталом: наявністю аналітиків, здатних контекстуалізувати сирі дані про загрози та перетворювати їх на actionable intelligence.

Регулярні міжсекторальні навчання та кібернавчання мають проводитися не рідше двох разів на рік за участю всіх ключових стейкхолдерів. Досвід Польщі та Балтії показує, що спільні навчання є критично важливими для виявлення прогалин у координації та тестування процедур реагування. Навчання мають включати як tabletop exercises для відпрацювання процедур прийняття рішень на стратегічному рівні, так і technical drills для тестування технічних механізмів реагування. Особливу увагу слід приділити сценаріям, що передбачають координацію між кількома секторами (наприклад, кібератака на енергосистему з каскадними ефектами на телекомунікації та транспорт).

Програма сертифікації фахівців з кібербезпеки критичної інфраструктури має розроблятися у партнерстві між державою, університетами та приватним сектором. Коваленко І. зазначає, що втрата кваліфікованих фахівців, мобілізація і відтік до приватного сектору створюють гостру нестачу кадрів, що потребує комплексних заходів утримання [39]. Mind UA та KSE реалізують модель вирішення кадрового дефіциту в кібербезпеці через освітні програми та партнерства з приватним сектором [10]. Сертифікація має базуватися на міжнародних стандартах (таких як CISSP, CISM) з додатковими модулями, специфічними для українського регуляторного контексту та загроз. Держава може стимулювати проходження сертифікації через часткову компенсацію вартості для працівників операторів критичної інфраструктури.

Механізм швидкого реагування має включати цілодобову «гарячу лінію» між державними органами та операторами критичної інфраструктури для повідомлення про критичні інциденти та отримання оперативної підтримки.

Ізраїльський досвід показує, що наявність прямих каналів комунікації, що bypass звичайні бюрократичні процедури, є критично важливою для швидкої мобілізації під час кіберкриз. «Гаряча лінія» має підтримувати як телефонну комунікацію для ескалації на високому рівні, так і технічні канали для обміну індикаторами компрометації та технічними деталями про атаки.

4. Технологічні рекомендації.

Технологічна інфраструктура публічно-приватної взаємодії має забезпечувати автоматизований, безпечний та масштабований обмін інформацією.

Національна платформа автоматизованого обміну індикаторами компрометації за стандартами STIX/TAXII має інтегруватися з існуючою платформою «Трембіта» (український аналог естонського X-Road) для забезпечення захищеного обміну між державними та приватними системами. Використання міжнародних стандартів STIX (Structured Threat Information Expression) та TAXII (Trusted Automated Exchange of Intelligence Information) дозволить забезпечити сумісність з європейськими та трансатлантичними платформами обміну, що є критично важливим для отримання інформації про глобальні кіберкампанії, які можуть вплинути на Україну.

Захищена комунікаційна платформа для координації під час інцидентів має забезпечувати засоби для безпечного голосового, відео та текстового зв'язку між учасниками реагування. Платформа має бути незалежною від публічного інтернету (функціонувати через виділені канали зв'язку) та захищеною від можливих спроб компрометації з боку атакуючих. Естонський досвід після атак 2007 року показує важливість наявності резервних каналів комунікації, які можуть функціонувати навіть у разі масштабного порушення роботи публічних телекомунікаційних мереж.

Єдина система моніторингу кіберзагроз для об'єктів категорії І має агрегувати дані з систем виявлення вторгнень операторів найбільш критичної інфраструктури для забезпечення загальнонаціонального situational awareness. Система має використовувати технології big data analytics та machine learning для

ідентифікації патернів координованих атак, які можуть не бути очевидними при аналізі даних окремого оператора. Критично важливим є збалансування між централізацією даних для ефективного аналізу та захистом приватності й комерційної таємниці операторів.

Впровадження архітектури zero trust для критичної інфраструктури має стати довгостроковим стратегічним пріоритетом. Принципи zero trust (never trust, always verify) передбачають, що жоден користувач чи система не мають довіри за замовчуванням, і кожен запит на доступ до ресурсів має автентифікуватися та авторизуватися. Міжнародний досвід показує, що архітектура zero trust є найбільш ефективною для захисту від advanced persistent threats та інсайдерських загроз, які є пріоритетними в контексті гібридної війни.

5. Фінансові рекомендації.

Забезпечення адекватного фінансування кіберзахисту критичної інфраструктури потребує диверсифікації джерел та створення інноваційних механізмів співфінансування.

Фонд кіберстійкості для співфінансування проектів захисту критичної інфраструктури має формуватися з державного бюджету, міжнародної донорської підтримки та добровільних внесків великих операторів критичної інфраструктури. Європейська Комісія надає фінансування проектів із підвищення кіберстійкості критичної інфраструктури, зокрема через NIS2, із акцентом на розвиток інституцій і технологій [33]. Світовий банк фокусується на комплексному підході інтеграції державного та приватного секторів для зміцнення кібербезпеки з урахуванням глобального досвіду [62]. Фонд має працювати на конкурсній основі, співфінансуючи проекти операторів (наприклад, 50% державного фінансування, 50% власних коштів оператора) для впровадження сучасних засобів кіберзахисту, модернізації legacy-систем та підготовки персоналу.

Механізм кібер-страхування з державною підтримкою для об’єктів критичної інфраструктури має включати державні гарантії для покриття катастрофічних кіберризиків, які є незастрахованими в комерційному ринку.

Досвід розвинених країн показує, що ринок кібер-страхування є ефективним механізмом для стимулювання впровадження передових практик кібербезпеки, оскільки страховики диференціюють премії на основі рівня кіберзрілості організації. Державна підтримка може включати субсидування частини страхових премій для малих операторів критичної інфраструктури та створення механізму reinsurance для покриття системних ризиків.

Програми міжнародної технічної допомоги мають координуватися для максимізації їх ефекту та уникнення дублювання. USAID підтримує розвиток людських ресурсів та модернізацію технологічної бази кібербезпеки в секторі критичної інфраструктури [17]. Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) реалізує підтримку реформ законодавства та впровадження міжнародних стандартів для сектору кібербезпеки [3]. Microsoft надає технологічну допомогу, навчальні програми та розвиток партнерств між IT-компаніями та державними органами [9]. Координація цих програм через єдиний державний орган (наприклад, Національну платформу кіберстійкості) дозволить узгодити пріоритети донорів із національними потребами та забезпечити синергію між різними ініціативами.

6. Кадрові рекомендації

Вирішення кадрової кризи у сфері кібербезпеки потребує комплексного підходу до підготовки, залучення та утримання фахівців.

Національна програма підготовки фахівців з кіберзахисту критичної інфраструктури має інтегрувати академічну освіту, галузеві сертифікації та практичне навчання на робочому місці. Програма має розроблятися у тісному партнерстві між Міністерством освіти, університетами, операторами критичної інфраструктури та міжнародними партнерами. Ізраїльський досвід підготовки кадрів через військову службу може бути частково адаптований через створення спеціалізованих програм для військовослужбовців, які після демобілізації можуть продовжити кар'єру в цивільному секторі кібербезпеки.

Механізми утримання кадрів мають включати бронювання від мобілізації для критичних спеціалістів з кібербезпеки, що забезпечують функціонування

об'єктів категорії І. Це рішення є контроверсійним в умовах повномасштабної війни, проте міжнародний досвід демонструє, що забезпечення кіберстійкості критичної інфраструктури є невід'ємною частиною національної оборони. Бронювання має супроводжуватися суворим контролем та періодичною ревалідацією критичності позицій для запобігання зловживанням. Додатковими механізмами утримання мають бути конкурентні компенсаційні пакети для державних службовців, що працюють у сфері кібербезпеки, включаючи надбавки за специфіку роботи та можливості професійного розвитку.

Програми стажування державних службовців у приватному секторі та навпаки мають забезпечити ротацію кадрів та трансфер знань між секторами. Естонський та ізраїльський досвід показують, що така ротація є ефективним механізмом для подолання культурних бар’єрів між державою та бізнесом, поширення найкращих практик та створення неформальних мереж, які полегшують координацію під час кризових ситуацій. Програма має включати формалізовані процедури для тимчасового переведення державних службовців на роботу в компанії приватного сектору (на 6-12 місяців) з збереженням посади та аналогічні механізми для залучення приватних фахівців до роботи в державних органах.

Отже, вдосконалення публічно-приватної взаємодії в Україні потребує комплексної стратегії, що охоплює інституційні, правові, організаційні, технологічні, фінансові та кадрові аспекти. Запропоновані рекомендації базуються на синтезі міжнародного досвіду та враховують українську специфіку, пов'язану з повномасштабною війною та процесами євроінтеграції.

Критичним фактором успіху є забезпечення довіри між державою та бізнесом через правові гарантії конфіденційності, створення механізмів взаємовигідного обміну інформацією, та забезпечення реальної цінності участі для приватного сектору. Технологічна інфраструктура має бути сумісною з європейськими та трансатлантичними платформами, що дозволить Україні інтегруватися в глобальну систему обміну інформацією про кіберзагрози. Фінансове забезпечення має поєднувати державне фінансування, міжнародну

донорську підтримку та інвестиції приватного сектору, стимульовані податковими пільгами.

Вирішення кадрової кризи вимагає не лише підготовки нових фахівців, але й утримання існуючих через конкурентні умови та механізми бронювання від мобілізації для критичних позицій. Успішна реалізація цих рекомендацій дозволить створити дієву модель публічно-приватної взаємодії, що забезпечить підвищення кіберстійкості критичної інфраструктури України та наблизить країну до європейських стандартів кібербезпеки.

ВИСНОВКИ

За результатами дослідження сформульовано нижченаведені основні висновки та пропозиції:

1. Комплексний аналіз кіберзагроз критичній інфраструктурі України в умовах гібридної війни виявляє безпрецедентну трансформацію характеру, інтенсивності та складності кібератак, що відображає еволюцію сучасного воєнного конфлікту в епоху цифрових технологій. Зростання кількості кіберінцидентів на 48% у другому півріччі 2024 року, досягнення позначки 2576 зафіксованих атак та збільшення використання шкідливого програмного забезпечення на 112% підтверджують критичне загострення ситуації у сфері кібербезпеки національної інфраструктури.

Принципова новизна сучасного етапу полягає у стратегічній інтеграції кібероперацій у загальний план військових дій, де цифрові атаки синхронізуються з ракетними ударами та артилерійськими обстрілами для досягнення синергетичного руйнівного ефекту. Виявлення навесні 2024 року підготовки російського угруповання UAC-0002 до координованих атак на енергетичну інфраструктуру підтверджує стратегічний характер кібероперацій противника та їх спрямованість на досягнення фізичних наслідків через цифрові засоби.

2. Систематизація кіберзагроз за векторами, цілями та наслідками дозволила ідентифікувати чотири основні категорії: гібридна агресія російської федерації у кіберпросторі, кіберзлочинність, організовані державою цільові атаки та кібертероризм. Критичний аналіз класифікацій, запропонованих українськими та міжнародними дослідниками, виявив необхідність їх адаптації до реалій гібридного конфлікту, де межі між різними типами загроз розмиваються, а мотивація атакуючих трансформується від кримінально-фінансової до геополітично-військової.

Багатовимірний аналіз вразливостей критичної інфраструктури виявив

критичні слабкості на технологічному рівні (застаріле обладнання SCADA/ICS, відсутність надійної сегментації мереж), організаційному рівні (фрагментація відповідальності між численними операторами, недостатнє фінансування модернізації) та людському рівні (недостатня кіберобізнаність персоналу, успішність 73% цільових фішингових атак). Особливу тривогу викликає системне відставання темпів модернізації засобів захисту від темпів еволюції кіберзагроз, що створює стратегічне вікно вразливості для критичної інфраструктури, особливо в енергетичному та транспортному секторах.

3. Секторальний аналіз кіберстійкості демонструє значну диференціацію між галузями критичної інфраструктури за рівнем захищеності та спроможності протистояти кіберзагрозам. Фінансовий сектор, маючи найвищий рівень кіберзрілості завдяки суворому регуляторному нагляду Національного банку України та значним інвестиціям у засоби захисту, протистоїть найбільш інтенсивному потоку атак з відносно високою ефективністю.

Енергетика та транспорт, попри критичну важливість для фізичного функціонування держави, відстають у рівні захищеності через об’єктивні складнощі модернізації розподілених промислових систем управління, спроектованих за десятиліття до появи сучасних кіберзагроз.

Телекомунікаційний сектор перебуває в процесі болючої трансформації, стимульованої масштабними інцидентами 2023-2024 років, що виявили критичні вразливості інфраструктури провідних операторів.

4. Компаративний аналіз міжнародного досвіду захисту критичної інфраструктури (американської моделі CISA, європейського підходу на основі директиви NIS2 та естонського досвіду побудови кіберстійкості після атак 2007 року) виявляє відсутність універсальної моделі, придатної для прямого перенесення на українські реалії воєнного стану.

Україна створює принципово новий тип кіберстійкості в умовах одночасного протистояння масштабній кібер-агресії та повномасштабній війні, що має бути концептуалізований та систематизований як унікальний вклад у глобальну теорію та практику кіберзахисту критичної інфраструктури.

5. Аналіз публічного управління кіберстійкістю в Україні виявляє складну систему інституційних, нормативно-правових та організаційних механізмів, ефективність яких обмежується множинними структурними викликами. Держава створила амбітну законодавчу базу через Закон про кібербезпеку (2017), Стратегію кібербезпеки (2021) та відповідні підзаконні акти, проте практична імплементація цих документів стримується дублюванням функцій між Держспецзв'язком, СБУ, Міністерством цифрової трансформації та Кіберполіцією. Ця інституційна фрагментація призводить до неефективної координації, уповільнення реагування на інциденти та нераціонального використання обмежених ресурсів.

Процес адаптації до Директиви NIS2 ЄС створює як можливості для модернізації національної системи кіберзахисту, так і виклики через необхідність впровадження підвищених вимог до звітності та санкцій в умовах нормативної невизначеності та воєнного стану. Механізми категоризації об’єктів критичної інфраструктури функціонують, проте контрольно-наглядова діяльність часто носить формальний характер через обмежені ресурси уповноважених органів та недостатню кваліфікацію інспекторів. Розрив між стратегічним плануванням та реальним фінансуванням залишається критичною перешкодою для досягнення цілей Стратегії кібербезпеки.

6. Приватний сектор демонструє зростаюче усвідомлення важливості кіберзахисту, про що свідчать інвестиції на рівні близько 9% від IT-бюджетів та впровадження міжнародних стандартів провідними компаніями. Секторальний аналіз виявляє неоднорідність підходів: фінансовий сектор демонструє найвищі стандарти через жорстку регуляцію НБУ, енергетичний стикається з викликами модернізації застарілих промислових систем, телекомунікаційний поєднує роль об'єкта захисту та провайдера послуг безпеки, а IT-сектор показує найвищу зрілість проте з значним розривом між великими та малими гравцями.

Проте ця позитивна динаміка обмежується критичним дефіцитом кваліфікованих фахівців, посиленим еміграцією та мобілізацією, відсутністю податкових стимулів для довгострокових інвестицій, та репутаційними

ризиками, що стримують відкритість у повідомленні про інциденти. Галузеві асоціації відіграють позитивну роль у формуванні добровільних стандартів та обміні інформацією, проте ефективність саморегулювання обмежена без державної підтримки.

7. Для підвищення ефективності публічного управління кіберстійкістю необхідним є:

1) чітке розмежування повноважень між державними органами з ліквідацією дублювання функцій через оновлення законодавства;

2) перехід від формального до ризик-орієнтованого контрольно-наглядового підходу з концентрацією ресурсів на об’єктах найвищої критичності;

3) створення ефективних механізмів державно-приватного партнерства з чіткими процедурами взаємодії та захистом конфіденційності наданої інформації;

4) впровадження системи стимулів (фінансових та нефінансових) для заохочення інвестицій приватного сектору у кібербезпеку, включаючи спрощення регуляторних процедур та пріоритетний доступ до держконтрактів;

5) розвиток програм підготовки та утримання кваліфікованих кадрів через партнерство між університетами, бізнесом та державою;

6) поступова імплементація вимог NIS2 з пріоритизацією найкритичніших положень директиви. Лише комплексний підхід, що поєднує ефективне державне регулювання з активною участю приватного сектору, може забезпечити достатній рівень кіберстійкості критичної інфраструктури України в умовах зростаючих загроз.

8. Міжнародний досвід організації публічно-приватної взаємодії у сфері кіберзахисту критичної інфраструктури виявляє універсальні принципи успішних моделей, які можуть бути адаптовані до українського контексту. Естонська модель після трансформації 2007 року демонструє ефективність технологічної платформи безпечного обміну даними (X-Road) та участі приватного сектору в національній кібероборони.

Американська секторальна модель ISACs показує переваги галузевого підходу для врахування специфічних загроз та технологій різних секторів економіки. Британська мультисекторальна платформа CiSP ілюструє можливості масштабної інтеграції малого та середнього бізнесу через урядову платформу обміну.

Ізраїльський досвід військово-цивільної синергії є особливо релевантним для України через подібність безпекового контексту. Досвід Польщі та Балтії демонструє важливість регіональної співпраці та прагматичного підходу до імплементації європейських директив.

9. Синтез міжнародного досвіду дозволяє сформулювати комплексні рекомендації для України, структуровані за шістьма напрямами.

Інституційні рекомендації включають створення Національної платформи кіберстійкості як координаційного органу, запровадження інституту урядового координатора на найвищому політичному рівні, та формування секторальних координаційних центрів за галузевим принципом.

Правові рекомендації передбачають прийняття Закону про критичну інфраструктуру з чітким розмежуванням повноважень, запровадження обов'язкової звітності про кіберінциденти з гарантіями конфіденційності, податкові стимули для інвестицій у кібербезпеку, та правові гарантії для обміну інформацією без ризику антимонопольного переслідування.

Організаційні рекомендації охоплюють створення Національного центру обміну інформацією про кіберзагрози (UA-ISAC), регулярні міжсекторальні навчання, програму сертифікації фахівців, та механізм швидкого реагування через «гарячу лінію».

Технологічні рекомендації включають національну платформу автоматизованого обміну індикаторами компрометації за стандартами STIX/TAXII, захищену комунікаційну платформу для координації під час інцидентів, єдину систему моніторингу для найбільш критичних об’єктів, та поступове впровадження архітектури zero trust.

Фінансові рекомендації передбачають створення Фонду кіберстійкості для

співфінансування проектів, механізм кібер-страхування з державною підтримкою, та координацію програм міжнародної технічної допомоги.

Кадрові рекомендації охоплюють національну програму підготовки фахівців, механізми утримання через бронювання від мобілізації для критичних позицій, та програми стажування між державним та приватним секторами.

Критично важливим є комплексність та узгодженість впровадження цих рекомендацій. Ізольоване впровадження окремих елементів без системного підходу не забезпечить необхідного ефекту. Успішна модель публічно-приватної взаємодії вимагає одночасного прогресу в інституційній архітектурі, правовій базі, організаційних процедурах, технологічній інфраструктурі, фінансових механізмах та розвитку людського капіталу. Поетапна реалізація має базуватися на чітких пріоритетах, де першочергові заходи (створення координаційних органів, прийняття базового законодавства, запуск платформи обміну інформацією) закладають фундамент для наступних етапів трансформації.

10. Специфіка української ситуації, пов’язана з повномасштабною війною, одночасно створює як виклики (мобілізація кадрів, обмеженість бюджетних ресурсів, інтенсивність кіберзагроз), так і можливості (підвищена усвідомленість критичності кібербезпеки, готовність бізнесу до співпраці з державою в питаннях національної безпеки, значна міжнародна підтримка). Ефективне використання цього вікна можливостей потребує політичної волі на найвищому рівні, прагматичного підходу до запозичення міжнародного досвіду, та готовності до експериментування та адаптації рішень на основі реального feedback від учасників системи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Anomali. What is an Information Sharing and Analysis Center (ISAC)? Technical Brief, 2025. URL: https://www.anomali.com/resources/what-is-an-isac (last accessed: 12.11.2025).

2. CISA. Partnerships and Collaboration: Building a Resilient Cyber Ecosystem. Washington, DC : Department of Homeland Security, 2024. 89 p.

3. Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ). Підтримка реформ в кібербезпеці України. Bonn : GIZ, 2025. 89 с.

4. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union. 2022. L 333. P. 80-152.

5. ENISA. Information Sharing and Analysis Centers (ISACs) в ЄС: практичний досвід. Брюссель, 2022. 89 с.

6. European Commission. Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector (DORA). *Official Journal of the European Union*. 2022. L 333. P. 1-79.

7. Hybrid CoE. Cyber Deterrence: A Case Study on Estonia's Policies and Practice. Helsinki : The European Centre of Excellence for Countering Hybrid Threats, 2021. 42 p.

8. International Energy Agency. Energy Security in Ukraine: Cyber Threats and Resilience. IEA Report. Paris : IEA Publications, 2024. 156 p.

9. Microsoft. Ініціативи підтримки кібербезпеки України, 2023-2025. Redmond : Microsoft Corp., 2024. URL: https://blogs.microsoft.com/on-the-issues/category/ukraine/ (дата звернення: 12.11.2025).

10. Mind UA. KSE реалізує модель вирішення кадрового дефіциту в кібербезпеці. 2025. URL: https://mind.ua/news/ (дата звернення: 12.11.2025).

11. NATO Cooperative Cyber Defence Centre of Excellence. Hybrid Threats

and Critical Infrastructure: Lessons from Estonia. Tallinn : NATO CCDCOE, 2019. 234 p.

12. NATO Cooperative Cyber Defence Centre of Excellence. Support to Ukraine in Cybersecurity. Tallinn : NATO CCDCOE, 2024. 78 p.

13. Ottis R., Lorents P. Cyberspace: Definition and Implications. Proceedings of the 5th International Conference on Information Warfare and Security. Tallinn : Estonian National Defence College, 2010. P. 267-270.

14. Rebane K. Estonian Public-Private Partnership in Cybersecurity: Lessons from 2007 Cyberattacks. *Baltic Security & Defence Review*. 2023. Vol. 25. No. 1. P. 78-96.

15. U.S. National Institute of Standards and Technology (NIST). Cybersecurity Framework. Version 1.1, 2018 (оновлення 2.0, 2024). URL: https://www.nist.gov/cyberframework (last accessed: 12.11.2025).

16. UK National Cyber Security Centre. Cyber Security Information Sharing Partnership (CiSP). London : NCSC, 2013-2025. URL: https://www.ncsc.gov.uk/information/cyber-security-information-sharing-partnership-cisp (last accessed: 12.11.2025).

17. USAID. Програма боротьби з кіберзагрозами в Україні. Washington, DC : USAID, 2024. URL: https://www.usaid.gov/ukraine (дата звернення: 12.11.2025).

18. Visure Solutions. Розуміння NIST Cybersecurity Framework. 2025. URL: https://visuresolutions.com/nist-cybersecurity-framework (last accessed: 12.11.2025).

19. White House. National Security Memorandum on Critical Infrastructure Security and Resilience (NSM-22). Washington, DC, 2024.

20. Андрієвський С. І. Регіональна співпраця в кібербезпеці: польський та балтійський досвід. *Безпека держави*. 2024. № 3. С. 145-163.

21. Барбашина М. Корпоративна культура та кібербезпека: огляд українських компаній. *Бізнес і суспільство*. 2023. № 4. С. 89-105.

22. Будко Т. В., Мусієнко А. П. Побудова моделі загроз національній

критичній інфраструктурі України. *Науковий вісник Харківського національного університету внутрішніх справ*. 2023. № 2. С. 78-89.

23. Вишневська П. В. Кібербезпека в умовах сучасних загроз: ізраїльський досвід. *Вісник юридичного університету*. 2024. № 2. С. 78-94.

24. Герасименко О. М. Інтеграція державних та приватних ресурсів у захисті критичної інфраструктури. *Науковий вісник Ужгородського університету*. 2024. Вип. 79. С. 145-152.

25. Герасименко О. М. Критична інфраструктура України як предмет наукового пізнання: теоретичний аспект. *Науковий вісник Ужгородського університету*. Серія: Право. 2024. Вип. 78. С. 234-240.

26. Гончарук Н. В. Адаптація директиви NIS2 у державах Балтії та Польщі: уроки для України. *Європейська політика*. 2023. № 4. С. 89-107.

27. Гончарук Н. Розвиток публічно-приватного партнерства у кібербезпеці. *Економіка і управління*. 2025. № 1. С. 34-51.

28. Гульванська Ю. А. Кібербезпека в Україні: виклики та шляхи вдосконалення законодавчого регулювання. *Актуальні проблеми державного управління*. 2023. № 2. С. 78-89.

29. Гульванська Ю. А. Правове регулювання кібербезпеки в Україні: проблеми та шляхи удосконалення. *Юридичний вісник*. 2024. № 2. С. 67-85.

30. Держспецзв’язок. Аналітичний звіт «Кіберзагрози критичній інфраструктурі» Н1'2024 /Державна служба спеціального зв’язку, 2024. 98 с.

31. Держспецзв’язок. Аналітичний звіт «Російські кібероперації» Н2’2024 / Державна служба спеціального зв’язку, 2025. 124 с.

32. Дмитренко О. Роль ІТ-асоціацій у розвитку кіберстійкості в Україні. *Інновації та розвиток*. 2023. № 3. С. 112-128.

33. Європейська Комісія. Програми технічної допомоги Україні у сфері кібербезпеки, 2023-2025. Брюссель : ЄК, 2024. 124 с.

34. Забашта Т. Стратегічне планування в кібербезпеці: практика України і світовий досвід. *Публічне управління*. 2024. № 1. С. 34-47.

35. Зубарева І. Досвід інших країн у становленні національних систем

кібербезпеки. *Міжнародний досвід і Україна*. 2023. № 3. С. 112-131.

36. Іванова Н. Роль освіти та підготовки кадрів у забезпеченні кіберстійкості. *Освітній простір України*. 2024. № 1. С. 89-107.

37. Кабінет Міністрів України. Проєкт Закону «Про критичну інфраструктуру». 2021. URL: https://www.kmu.gov.ua (дата звернення: 12.11.2025).

38. Климчук В. Проблеми контролю і нагляду у сфері кібербезпеки в Україні. *Адміністративне право України*. 2024. № 2. С. 145-159.

39. Коваленко І. Кадрові виклики в кібербезпеці України: аналіз 2022-2025. *Безпека інформації*. 2025. № 1. С. 34-52.

40. Коваленко О. Вплив імплементації Директиви NIS2 на українську критичну інфраструктуру. *Безпека інформації*. 2025. № 1. С. 56-71.

41. 41 Ковальчук Л. Міжгалузеві асоціації України у протидії кіберзагрозам. *Науковий вісник УжНУ*. Серія: Економіка. 2024. Вип. 52. С. 78-91.

42. Комісарова Н. О., Крутіков П. Д. Система кіберзахисту об’єктів критичної інфраструктури: комплексний підхід. *Вісник національної безпеки*. 2024. № 2. С. 43-48.

43. Кузьменко І. С. Інтеграція ізраїльських практик кібербезпеки в українські реалії. *Право і суспільство*. 2024. № 1. С. 112-128.

44. Кулик М. Й. Інформаційна безпека та кіберзахист у системі державної безпеки України. *Національні інтереси України: безпековий вимір*. 2024. № 3. С. 56-67.

45. Лях В., Савченко О. Координація кібербезпеки між державними структурами: проблеми і можливості. *Урядовий кур’єр*. 2024. 15 березня.

46. Мартін Т. Модель CiSP і її роль у зміцненні кібербезпеки Великої Британії. *Cybersecurity Review*, 2024. Vol. 15. P. 45-62.

47. Мельник Д. Ефективність контрольно-наглядових механізмів у сфері кібербезпеки України. *Право і безпека*. 2024. № 4. С. 78-93.

48. Міністерство розвитку громад та територій України. Законодавство

у сфері кіберзахисту об’єктів критичної інформаційної інфраструктури: аналітичний огляд. Київ, 2025. 34 с.

49. Національний банк України. Огляд стану кібербезпеки фінансового сектору України за 2024 рік. Київ : НБУ, 2025. 45 с.

50. Омельченко І. Оцінка законодавчої бази кіберзахисту критичної інфраструктури в Україні. *Юридичний збірник*. 2023. № 4. С. 112-125.

51. Патронюк С. В. Інституційна архітектура управління кібербезпекою України. *Вісник Харківського національного університету внутрішніх справ*. 2024. № 3. С. 45-58.

52. Про деякі питання об’єктів критичної інфраструктури : Постанова Кабінету Міністрів України від 9 жовтня 2020 р. № 1109. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-п (дата звернення: 12.11.2025).

53. Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури : Постанова Кабінету Міністрів України від 19 червня 2019 р. № 519. URL: https://zakon.rada.gov.ua/laws/show/519-2019-п (дата звернення: 12.11.2025).

54. Про затвердження плану заходів щодо реалізації Стратегії кібербезпеки України : Розпорядження Кабінету Міністрів України від 19 грудня 2023 р. № 1163-р. URL: https://zakon.rada.gov.ua/laws/show/1163-2023-р (дата звернення: 12.11.2025).

55. Про затвердження Рекомендацій щодо організації кіберзахисту об’єктів критичної інфраструктури : Наказ Адміністрації Держспецзв’язку та Служби безпеки України від 19 грудня 2024 р. № 627/772.

56. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 12.11.2025).

57. Про рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України» : Указ Президента України від 26 серпня 2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021 (дата звернення: 12.11.2025).

58. Проценко Є. Інвестиції приватного сектору у кібербезпеку України: аналіз трендів. *Економіка розвитку*. 2024. № 2. С. 67-82.

59. РНБО України. Річний аналітичний огляд кібербезпеки, 2024. Київ : Апарат РНБО, 2024. 156 с.

60. Романенко О. Виклики кадрового потенціалу в кібербезпеці України. *Інновації в освіті*. 2023. № 2. С. 145-162.

61. Російські кібератаки: зміна характеру атак у 2024 році. *MediaSapiens*. 2024. 15 листопада. URL: https://ms.detector.media/kiberbezpeka/

62. Світовий банк. Підвищення кіберстійкості в Україні: проекти та результати. Washington, DC : World Bank, 2024. 145 p.

63. Скіцько О. І., Ширшов Р. А. Актуальні питання забезпечення кібербезпеки об'єктів критичної інфраструктури. *Юридичний науковий електронний журнал*. 2024. № 10. С. 312-315.

64. Співаковський С. Створення умов для податкових стимулів інвестицій у кібербезпеку. *Економіка і право*. 2025. № 2. С. 67-84.

65. Україна зазнала 2576 російських кібератак у другому півріччі 2024 року. *AIN.UA*. 2025. 8 січня. URL: https://ain.ua/2025/01/08/

66. Федоренко А. Скорочення розриву між законодавством і практикою у кібербезпеці України. *Право і політика*. 2022. № 3. С. 89-103.

67. Чернишенко П. Роль Міністерства цифрової трансформації у розвитку кіберстійкості. *Технологічний вісник*. 2023. № 4. С. 23-38.

68. Шевчук Л. Механізми корпоративної відповідальності в контексті кіберзахисту українських компаній. *Бізнес і право*. 2024. № 3. С. 45-61.