МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА

Іщенко Катерина Федорівна

Допускається до захисту:
завідувач кафедри політології
та державного управління
д.політ.н., професор
_____Чальцева О.М.
«____» _____ 20__ р.

ПУБЛІЧНЕ УПРАВЛІННЯ У ФОРМУВАННІ НАЦІОНАЛЬНОЇ КІБЕРБЕЗПЕКИ В УКРАЇНІ: МЕХАНІЗМИ КООРДИНАЦІЇ ТА КОНТРОЛЮ

Спеціальність 281 Публічне управління та адміністрування

Кваліфікаційна робота

Науковий керівник:
Польовий М.А., д.політ. н.,
професор кафедри політології та
державного управління,
Оцінка: ____ / ___ / _____
(бали/за шкалою ЄКТS/за національною шкалою)
Голова ЕК: ____(підпис)_____

Вінниця 2025

АНОТАЦІЯ

Іщенко К.Ф. Публічне управління у формуванні національної кібербезпеки в Україні: механізми координації та контролю – Кваліфікаційна наукова праця на правах рукопису - Кваліфікаційна наукова праця на правах рукопису.

Кваліфікаційна робота на здобуття наукового ступеня «Магістр» за спеціальністю 281 Публічне управління та адміністрування. Донецький національний університет імені Василя Стуса, Вінниця, 2025.

У роботі досліджено роль публічного управління у формуванні системи національної кібербезпеки України, зокрема механізми координації та контролю. В умовах гібридної війни та зростання кіберзагроз публічне управління відіграє ключову роль у забезпеченні стійкості держави в цифровому просторі.

Розкрито еволюцію підходів до кібербезпеки як об'єкта публічного управління. Проаналізовано міжнародний досвід (США, Велика Британія, Ізраїль, Естонія, Сінгапур) та виявлено дієві практики координації й контролю, релевантні для України. Дослідження виявило недоліки вітчизняної системи: розпорошення повноважень, відсутність сталого контролю, низький рівень міжвідомчої взаємодії, обмежена прозорість.

Запропоновано низку інституційних змін: створення Національного центру координації кібербезпеки при РНБО, удосконалення функцій CERT-UA, запровадження національної платформи обміну інформацією, посилення парламентського та громадського контролю.

Ключові слова: публічне управління, кібербезпека, координація, контроль, CERT-UA, критична інфраструктура, міжнародний досвід, національна безпека, цифрова трансформація, кіберзахист, інформаційна безпека, кіберінциденти, державна політика, міжвідомча взаємодія, кіберстійкість, стратегічне управління, управлінські механізми, інституційна спроможність, нормативно-правове забезпечення, гібридні загрози, кібероборона, цифровий суверенітет.

Бібліограф.: 50 найм.

ABSTRACT

Ishchenko K.F. Public Administration in Shaping National Cybersecurity in Ukraine: Coordination and Control Mechanisms – Qualification scientific work on the rights of the manuscript.

Qualification work for the degree of Master's Degree in speciality 281 Management and administration. Vasyl' Stus Donetsk National University, Vinnytsia, 2025.

The paper examines the role of public administration in shaping Ukraine's national cybersecurity system, with a focus on coordination and control mechanisms. In the context of hybrid warfare and increasing cyber threats, public administration is essential for ensuring national resilience in the digital sphere.

The study outlines the evolution of cybersecurity as an object of public governance. It analyzes international experience (USA, UK, Israel, Estonia, Singapore) and identifies relevant coordination and oversight practices applicable to Ukraine. The research reveals key weaknesses in the national system: fragmented responsibilities, lack of sustained oversight, weak interagency cooperation, and limited transparency.

Institutional reforms are proposed, including the creation of a National Cybersecurity Coordination Center under the NSDC, strengthening the role of CERT-UA, implementing a national information-sharing platform, and enhancing parliamentary and civil oversight.

Key words: public administration, cybersecurity, coordination, control, CERT-UA, critical infrastructure, international experience, national security, digital transformation, cyber defense, information security, cyber incidents, public policy, interagency cooperation, cyber resilience, strategic management, management mechanisms, institutional capacity, regulatory and legal framework, hybrid threats, cyber defense, digital sovereignty.

Bibliography: 50 items.

ЗМІСТ

ВСТУП

Актуальність теми дослідження зумовлена стрімким зростанням кіберзагроз в умовах глобальної цифровізації та гібридної війни, яку веде Російська Федерація проти України. Масштабні кібератаки на критичну інфраструктуру, органи влади, фінансовий сектор та енергетику вимагають переосмислення підходів до публічного управління у сфері кібербезпеки. Особливої актуальності набуває питання регіонального виміру, оскільки ефективна протидія кіберзагрозам неможлива без чіткої координації між центральною та місцевою владою, а також без залучення приватного сектору та громадянського суспільства.

Наукова значущість теми обумовлена недостатньою розробленістю теоретико-методологічних засад управління кібербезпекою в умовах гібридних загроз, потребою адаптації міжнародного досвіду до українських реалій та формуванням ефективних моделей взаємодії стейкхолдерів. Суспільно-політична складова актуальності пов’язана з необхідністю забезпечення стабільного функціонування державних інституцій, захисту персональних даних та довіри громадян до цифрових сервісів. Крім того, євроінтеграційний курс України передбачає гармонізацію національної системи кібербезпеки з вимогами ЄС, зокрема впровадження стандартів Директиви NIS2. Враховуючи активний розвиток цифрових ініціатив у Вінницькій області, саме регіональний підхід дозволяє виявити специфічні виклики та сформувати практичні рекомендації для підвищення ефективності публічного управління у сфері кібербезпеки.

Мета дослідження полягає у науковому обґрунтуванні шляхів удосконалення механізмів публічного управління у сфері кібербезпеки в Україні, що передбачає комплексне вивчення теоретико-методологічних засад, нормативно-правового забезпечення та світових підходів.

Для досягнення поставленої мети визначено такі **завдання дослідження**:

1. Розкрити сутність кібербезпеки у контексті публічного управління та систематизувати теоретико-методологічні підходи до її аналізу.

2. Проаналізувати стан кібербезпеки у Вінницькій області з порівнянням інших регіонів України для виявлення регіональних особливостей.

3. Дослідити міжнародний досвід формування національних систем кібербезпеки та можливості його адаптації в Україні.

4. Оцінити законодавчу та нормативну базу України у сфері кібербезпеки з урахуванням зарубіжних практик.

5. Вивчити механізми взаємодії між державними органами, приватним сектором і громадянським суспільством у забезпеченні кібербезпеки.

6. Розробити рекомендації щодо вдосконалення міжвідомчої координації та моделі публічного управління у сфері кібербезпеки.

Об'єкт дослідження – процеси публічного управління у сфері забезпечення кібербезпеки в Україні.

Предмет дослідження – механізми, методи та інструменти публічного управління кібербезпекою, їх нормативно-правове та організаційне забезпечення в умовах сучасних викликів національній безпеці України.

Методи дослідження. У дослідженні використано комплекс загальнонаукових і спеціальних методів, зокрема: системний аналіз, структурно-функціональний аналіз, компаративний метод, нормативно-правовий аналіз, метод експертних оцінок, SWOT-аналіз, івент-аналіз та метод моделювання.

Системний аналіз використано для комплексного розгляду кібербезпеки як елемента системи публічного управління та виявлення взаємозв’язків між інституціями, процесами й технологіями. Структурно-функціональний аналіз – для визначення ролей, повноважень і взаємодії державних органів, відповідальних за кіберзахист. Компаративний метод – для порівняння української моделі кібербезпеки з практиками інших держав і виявлення ефективних підходів. Нормативно-правовий аналіз використано для оцінки законодавчої та регуляторної бази у сфері кібербезпеки й визначення прогалин у регулюванні. Метод експертних оцінок – для отримання думок фахівців щодо реального стану кіберзахисту в органах влади та ключових проблем. SWOT-аналіз – для визначення сильних і слабких сторін державної системи

кібербезпеки, можливостей її розвитку та зовнішніх загроз. Івент-аналіз – для аналізу конкретних кіберінцидентів, що вплинули на роботу публічних інституцій, та оцінки ефективності реагування. Метод моделювання – для побудови сценаріїв розвитку системи кібербезпеки та пропозицій щодо оптимізації управлінських механізмів.

Наукова гіпотеза дослідження полягає в тому, що ефективність публічного управління у сфері кібербезпеки в Україні може бути істотно підвищена через гармонізацію нормативно-правової бази з європейськими стандартами, посилення міжвідомчої координації, впровадження міжнародного досвіду з урахуванням гібридних загроз, а також розвиток регіональних систем управління з чітким розподілом повноважень.

Наукова новизна полягає у проведенні першого комплексного аналізу регіонального виміру кібербезпеки (на прикладі Вінницької області), удосконаленні теоретико-методологічних підходів, розробці моделі міжсекторної взаємодії, системи критеріїв оцінки ефективності та формуванні пріоритетів міжвідомчої координації.

Практична значущість результатів проявляється у можливості їх використання органами влади, профільними державними структурами, вищими навчальними закладами та науковими установами для вдосконалення кібербезпеки на національному й регіональному рівнях.

Апробація результатів дослідження. Основні положення та результати кваліфікаційної роботи представлені у публікації у Віснику студентського наукового товариства Донецького національного університету імені Василя Стуса у статті «Роль публічного управління у формуванні національної кібербезпеки: механізми координації та контролю» (Вип.17, т.1, с.69). [7]

Зв’язок роботи з науковими програмами, планами, темами: Кваліфікаційна (магістерська) робота виконана в рамках тематичного плану НДР Донецького національного університету імені Василя Стуса ініціативного фундаментального дослідження кафедри політології та державного управління: «Публічна політика

і державне управління в умовах війни та повоєнного відновлення України» (реєстраційний номер 0123U101423).

Структура та обсяг роботи. Кваліфікаційна робота складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків. Загальний обсяг роботи становить 64 сторінок, з них 59 сторінок основного тексту. Робота містить 13 таблиць. Список використаних джерел налічує 50 найменувань.

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ПУБЛІЧНОГО УПРАВЛІННЯ У СФЕРІ КІБЕРБЕЗПЕКИ

1.1. Генеза предмета дослідження та поняття і сутність кібербезпеки у публічному управлінні

Кібербезпека як наукова категорія та сфера практичної діяльності пройшла складний еволюційний шлях, що відображає трансформацію суспільних відносин в умовах цифровізації. Дослідження генези цього поняття дозволяє глибше зрозуміти сучасні підходи до публічного управління у сфері кібербезпеки та спрогнозувати напрями її подальшого розвитку.

Термін «кібербезпека» набув поширення на межі XX–XXI століть у відповідь на зростання цифрових загроз, хоча його витоки сягають 1970-х років, коли з’явилися перші комп’ютерні мережі та спроби несанкціонованого доступу до інформації. Спочатку безпеку розглядали винятково в технічному контексті, однак уже в 1980-х роках із поширенням вірусів і кібершпигунства стало зрозуміло, що проблема має соціальні виміри. Дослідник Брюс Шнайєр підкреслював комплексний характер кібербезпеки, що охоплює не лише технології, а й людський фактор, організаційні аспекти та правове регулювання. [1].

Поворотним моментом у формуванні сучасного розуміння кібербезпеки стали події 11 вересня 2001 року, після яких кіберпростір почали сприймати як потенційну сферу терористичних загроз і елемент національної безпеки. Саме тоді термін «кібербезпека» набув широкого поширення в науковому, політичному та управлінському дискурсах. Через міждисциплінарний характер поняття в науковій літературі відсутнє універсальне визначення кібербезпеки. Мартін Лібіцкі трактує її як сукупність заходів для забезпечення конфіденційності, цілісності та доступності інформації [2]. Джозеф Най пропонує ширше бачення — як відсутність загроз для цінностей, досягнених через інформаційні системи [3]. Рональд Деіберт акцентує увагу на

правозахисному та етичному вимірах, визначаючи кібербезпеку як комплекс заходів для захисту критичної інфраструктури, персональних даних і прав людини [24].

Серед українських науковців вагомий внесок у розробку теоретичних засад кібербезпеки зробив Володимир Горбулін, який розглядає її як стан захищеності життєво важливих інтересів особи, суспільства й держави, що забезпечує сталий розвиток інформаційного простору та ефективне реагування на загрози національній безпеці у кіберпросторі [32]. Юрій Даник пропонує системний підхід, трактуючи кібербезпеку як сукупність політичних, правових, економічних та організаційних заходів, спрямованих на захист держави й громадян [6]. Управлінський вимір цієї проблематики розкриває Олександр Довгань, акцентуючи на необхідності ефективних механізмів публічного управління для протидії динамічним кіберзагрозам [3]. Натомість Валентин Петров зосереджується на правовому аспекті, визначаючи кібербезпеку як правовий режим кіберпростору, що включає захист інформаційних ресурсів, критичної інфраструктури та протидію кіберзлочинності [16].

Наведена нижче таблиця 1.1 узагальнює основні структурні компоненти кібербезпеки, виокремлені на основі аналізу різних підходів до її визначення.

Таблиця 1.1

Структурні елементи кібербезпеки

№	Компонент	Зміст
1	Технологічний	Апаратні, програмні та криптографічні засоби захисту; системи моніторингу та реагування на інциденти.
2	Організаційний	Управлінські процедури, політики безпеки, стандарти, розподіл відповідальності між суб’єктами.
3	Правовий	Нормативно-правова база, регулювання кіберпростору, відповідальність за кіберзлочини, повноваження державних органів.
4	Освітній	Підготовка фахівців, кіберграмотність населення, культура безпечної поведінки у цифровому середовищі.
5	Міжнародний	Участь у міжнародній співпраці, обмін інформацією, імплементація міжнародних стандартів.

В контексті публічного управління кібербезпека набуває специфічних характеристик, що відрізняють її від інших сфер державної політики. По-перше,

це надзвичайно високий динамізм загроз – нові види кібератак з'являються щодня, що вимагає постійної адаптації управлінських рішень. По-друге, це транскордонний характер кіберпростору, який ускладнює застосування традиційних інструментів державного регулювання. По-третє, це критична залежність ефективності публічного управління від взаємодії з приватним сектором, оскільки більшість критичної інформаційної інфраструктури перебуває у приватній власності.

Публічне управління кібербезпекою можна визначити як цілеспрямовану діяльність органів державної влади, місцевого самоврядування, інститутів громадянського суспільства та приватного сектору щодо формування, реалізації та координації політики у сфері захисту кіберпростору, що здійснюється на основі принципів законності, прозорості, відповідальності та багатостороннього партнерства. Специфіка публічного управління кібербезпекою полягає у необхідності балансування між різними цінностями та інтересами: безпекою і свободою, контролем і приватністю, суверенітетом і міжнародною співпрацею. Як зазначає Джозеф Най, «кібербезпека не є грою з нульовою сумою, де виграш однієї сторони означає програш іншої; це радше колективне благо, досягнення якого можливе лише через співпрацю різних акторів» [33].

Підходи до публічного управління кібербезпекою еволюціонували разом із розвитком самого поняття кібербезпеки. На початковому етапі (1980-1990-ті роки) переважав технократичний підхід, коли кібербезпека розглядалася як суто технічна проблема, що вирішується фахівцями з інформаційних технологій. Роль держави обмежувалася створенням загальних правових рамок та фінансуванням досліджень. На другому етапі (2000-ні роки) відбувається усвідомлення кібербезпеки як проблеми національної безпеки, що призводить до централізації управління та створення спеціалізованих державних структур. Характерною рисою цього періоду є домінування силових відомств у формуванні політики кібербезпеки та акцент на оборонних аспектах. Сучасний етап (з 2010-х років) характеризується переходом до моделі багатостороннього врядування (multi-stakeholder governance), яка передбачає активну участь приватного сектору,

громадянського суспільства, міжнародних організацій у формуванні та реалізації політики кібербезпеки. Мартін Лібіцкі підкреслює, що «ефективна кібербезпека можлива лише за умови синергії державних, приватних та громадських зусиль, оскільки жоден актор поодинці не володіє достатніми ресурсами та компетенціями для протидії всьому спектру кіберзагроз» [29, 5].

На основі проведеного аналізу можна запропонувати концептуальну модель кібербезпеки у публічному управлінні, яка включає чотири взаємопов'язані виміри (таблиця 1.2).

Таблиця 1.2

Концептуальна модель кібербезпеки у публічному управлінні

№	Вимір	Зміст
1	Інституційний	Органи державної влади та інші інституції, їхні повноваження, механізми координації, контролю та взаємодії у сфері кібербезпеки.
2	Нормативний	Законодавство, підзаконні акти, стратегічні документи, міжнародні угоди та стандарти, що регулюють кібербезпеку.
3	Функціональний	Загальні функції управління (планування, організація, мотивація, контроль) і спеціальні функції (моніторинг, реагування, розслідування тощо).
4	Ресурсний	Необхідні ресурси: фінансові, кадрові, технологічні та інформаційні для забезпечення ефективної діяльності у сфері кібербезпеки.

Ця модель дозволяє комплексно аналізувати стан публічного управління кібербезпекою та виявляти проблемні зони, що потребують удосконалення.

В українському законодавстві базове визначення кібербезпеки закріплено у Законі України «Про основні засади забезпечення кібербезпеки України» (2017), згідно з яким кібербезпека – це «захищеність інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі». Це визначення відображає комплексний підхід до кібербезпеки, що охоплює інтереси всіх рівнів – від окремої особи до держави в цілому. Водночас, аналіз практики застосування цього визначення свідчить про необхідність його

конкретизації та розвитку понятійного апарату, особливо в частині розмежування понять «кібербезпека», «інформаційна безпека», «захист інформації» та споріднених категорій.

Проведений аналіз генези та сутності поняття кібербезпеки дозволяє зробити висновок про його багатовимірний та динамічний характер. Кібербезпека у публічному управлінні – це не просто технічний захист інформаційних систем, а комплексна діяльність, що вимагає інтеграції технологічних, організаційних, правових, освітніх та міжнародних компонентів. Ефективне публічне управління кібербезпекою можливе лише за умови чіткого розуміння її сутності всіма стейкхолдерами та узгодження їхніх зусиль у єдиній стратегії національної кібербезпеки.

1.2. Кібербезпека у Вінницькій області: порівняльний аналіз з іншими регіонами

Регіональний вимір кібербезпеки набуває особливого значення в умовах децентралізації влади та зростання ролі місцевого самоврядування у вирішенні питань, що стосуються життєдіяльності територіальних громад. Вінницька область, як один із регіонів України, що активно розвиває цифрові технології та впроваджує інновації в публічному управлінні, являє собою цікавий об'єкт для дослідження стану кібербезпеки та ефективності регіональних механізмів її забезпечення.

Вінницька область займає провідні позиції серед регіонів України за рівнем цифровізації публічних послуг. Згідно з рейтингом Міністерства цифрової трансформації України за 2023 рік, область посідає 5-е місце в індексі цифрової трансформації регіонів. За підсумками 2024 року область зміцнила свої позиції, піднявшись на 4-е місце завдяки розширенню портфоліо електронних послуг та впровадженню хмарних рішень у системі регіонального управління. Місто Вінниця неодноразово визнавалося найкомфортнішим містом України для

життя, що значною мірою зумовлено високим рівнем впровадження цифрових сервісів для громадян.

У регіоні функціонує понад 150 IT-компаній, які працевлаштовують близько 5000 фахівців. Станом на початок 2025 року кількість IT-компаній зросла до 168, а чисельність працівників сектору перевищила 5800 осіб. Вінницький національний технічний університет та інші заклади вищої освіти готують спеціалістів з інформаційних технологій та кібербезпеки, що створює потужний кадровий потенціал для розвитку цифрової економіки. У 2024-2025 навчальному році запроваджено нову спеціалізацію «Кібербезпека критичної інфраструктури», яка враховує специфіку безпекових викликів воєнного та післявоєнного часу. Створення IT-кластеру «Vinnytsia IT Cluster» сприяло консолідації зусиль бізнесу, освіти та влади у розвитку галузі.

Обласна державна адміністрація активно впроваджує електронні послуги для громадян. Станом на 2024 рік в області функціонують 42 Центри надання адміністративних послуг (ЦНАП), більшість з яких інтегровані з системою електронного документообігу. У першому півріччі 2025 року кількість ЦНАП збільшено до 45, при цьому 38 з них повністю інтегровані з національною системою «Дія». Розроблено мобільний додаток «Моє місто Вінниця», через який громадяни можуть звертатися до місцевої влади, отримувати інформацію про комунальні послуги та брати участь в електронних опитуваннях. У 2025 році функціонал додатку розширено, додавши можливість оплати комунальних послуг та отримання push-сповіщень про надзвичайні ситуації.

У сфері охорони здоров'я впроваджено систему електронних медичних записів, що охоплює понад 80% медичних закладів області. На початок 2025 року цей показник досяг 87%, а також запущено пілотний проект телемедицини для віддалених сільських громад. Електронна система «Відкрита школа» використовується для взаємодії між школами, учнями та батьками. Ці досягнення, з одного боку, свідчать про високий рівень цифрової зрілості регіону, але з іншого – створюють нові виклики у сфері кібербезпеки, оскільки збільшується поверхня потенційних атак та зростає обсяг персональних даних,

що потребують захисту. Інституційна архітектура забезпечення кібербезпеки у Вінницькій області включає кілька рівнів. На обласному рівні функціонує департамент цифрового розвитку, інновацій та інформатизації Вінницької обласної державної адміністрації, до компетенції якого входить координація питань цифрової трансформації, включаючи аспекти кібербезпеки. Однак окремого структурного підрозділу, що займався б виключно питаннями кібербезпеки, в структурі облдержадміністрації не створено станом на 2024 рік, що створює певні проблеми у координації зусиль. У лютому 2025 року в рамках департаменту створено спеціалізований відділ кібербезпеки та захисту інформації у складі 5 працівників, що стало позитивним кроком у розбудові регіональної системи кіберзахисту.

Територіальні підрозділи Державної служби спеціального зв'язку та захисту інформації України (ДССЗЗІ) у Вінницькій області здійснюють контроль за дотриманням вимог законодавства у сфері захисту інформації, криптографічного та технічного захисту інформації. Проте, за даними моніторингу, проведеного обласною радою у 2023 році, штатна чисельність цих підрозділів є недостатньою для повноцінного охоплення всіх об'єктів критичної інфраструктури в регіоні. У 2024-2025 роках штат територіальних підрозділів ДССЗЗІ було збільшено на 30%, що дозволило розширити охоплення перевірками з 45% до 62% об'єктів критичної інфраструктури.

Управління кіберполіції Національної поліції України у Вінницькій області займається розслідуванням кіберзлочинів та профілактичною роботою. За даними звітності за 2023 рік, у регіоні зареєстровано 187 кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж, що на 23% більше порівняно з 2022 роком. У 2024 році кількість зареєстрованих кіберзлочинів зросла до 231 випадку (зростання на 23,5%), а за перше півріччя 2025 року вже зафіксовано 138 правопорушень, що свідчить про подальше зростання кіберзлочинності. Це свідчить як про зростання кіберзлочинності, так і про підвищення ефективності

виявлення таких злочинів завдяки модернізації технічних засобів розслідування та підвищенню кваліфікації співробітників.

На рівні місцевого самоврядування ситуація є неоднорідною. Вінницька міська рада створила посаду радника міського голови з питань кібербезпеки та захисту інформації, що є позитивним прикладом для інших громад. Водночас, у більшості об'єднаних територіальних громад області відсутні спеціалізовані підрозділи або посадові особи, відповідальні за кібербезпеку, що робить їх уразливими до кіберзагроз. Станом на вересень 2025 року ситуація дещо покращилась: у 12 найбільших ОТГ області призначено відповідальних за кібербезпеку (порівняно з 3 громадами у 2023 році), проте це все ще становить лише 28% від загальної кількості громад. Аналіз кіберінцидентів у Вінницькій області за період 2022-2025 років дозволяє виявити основні типи загроз та їх динаміку. Згідно з даними Центру реагування на кіберінциденти CERT-UA та регіональних підрозділів ДССЗЗІ, найбільш поширені типи кіберінцидентів у регіоні представлені в таблиці 1.3.

Таблиця 1.3

Основні типи кіберінцидентів у Вінницькій області (2022–2025 рр.)

№	Тип кіберінциденту	Кількість / масштаби	Коротка характеристика
1	DDoS-атаки	34 випадки у 2023 р. (зростання на 280% порівняно з 2021 р.); 41 випадок у 2024 р.; 28 випадків у І півріччі 2025 р.	Атаки на сайти органів влади, енергетичних компаній, водоканалів; найбільше – обласна та міська ради. У 2025 році спостерігається зміна тактики атакуючих: збільшення тривалості атак та використання комбінованих методів.
2	Фішинг і соціальна інженерія	Понад 420 звернень до поліції у 2023 р.; близько 580 звернень у 2024 р.; 340 звернень у І півріччі 2025 р.; фактична кількість значно більша	Масові спроби шахрайства через інтернет; громадяни часто не повідомляють про інциденти. У 2024-2025 рр. зросла складність фішингових схем із використанням штучного інтелекту для створення переконливіших повідомлень.
3	Програми-шифрувальники (ransomware)	12 зафіксованих випадків у 2023 р., з них 3 – у закладах охорони здоров'я; 15 випадків у 2024 р.; 9 випадків у І півріччі 2025 р.	Зараження комп'ютерних систем підприємств і установ із вимогою викупу; критичний ризик для медичних закладів. У 2025 році зафіксовано перший випадок атаки на систему водопостачання.

Продовження табл. 1.3

4	Витоки персональних даних	8 підтверджених інцидентів у 2023 р.; 11 інцидентів у 2024 р.; 7 інцидентів у І півріччі 2025 р.	Розголошення або втрата персональних даних у системах ОМС та комунальних підприємств. Найбільший інцидент 2024 року – витік даних 28 000 користувачів регіональних електронних сервісів.
5	Компрометація облікових записів	Неодноразові випадки протягом 2022-2024 рр.; 23 зафіксовані випадки у 2024 р.; 16 випадків у І півріччі 2025 р.	Несанкціонований доступ до акаунтів посадовців через слабкі або скомпрометовані паролі. З 2025 року обов'язкове впровадження двофакторної автентифікації знизило кількість успішних атак на 35%.
6	Атаки на системи промислового управління (SCADA)	3 випадки у 2024 р.; 2 випадки у І півріччі 2025 р.	Нова категорія загроз, виявлена у 2024 році: спроби несанкціонованого доступу до систем управління об'єктами енергетики та водопостачання.

Порівняно з загальнодержавною статистикою, структура кіберзагроз у Вінницькій області є типовою, проте привертає увагу вища частка атак на об'єкти критичної інфраструктури, що може бути пов'язано з географічним розташуванням регіону та наявністю важливих об'єктів. У 2024-2025 роках особливу стурбованість викликає поява нового типу загроз – цільових атак на системи промислового управління, що вимагає перегляду пріоритетів у забезпеченні кібербезпеки. Порівняльний аналіз стану кібербезпеки у Вінницькій області у контексті інших регіонів України — Львівської, Дніпропетровської, Одеської областей та м. Києва — свідчить про існування значних відмінностей у рівні інституційного, фінансового та технічного забезпечення. Львівська область характеризується розвинутим IT-сектором, наявністю окремого департаменту цифрового розвитку та регіонального центру кібербезпеки, створеного за підтримки міжнародних партнерів. У 2025 році Львів запустив програму «Кіберщит регіону» з бюджетом 45 млн грн, спрямовану на створення централізованої системи моніторингу кіберзагроз.

Дніпропетровська область має потужну систему моніторингу кіберзагроз та значний обсяг фінансування заходів у сфері кібербезпеки. У 2024-2025 роках область стала пілотним регіоном для впровадження національної системи

раннього попередження про кіберзагрози. Місто Київ, будучи провідним економічним і технологічним центром країни, забезпечує найвищий рівень кіберзахисту, має спеціалізовані структурні підрозділи та підтримує тісну співпрацю з міжнародними організаціями. У 2025 році Київ отримав статус сертифікованого кіберстійкого міста за стандартами ЄС. Одеська область відзначається створенням спеціалізованого центру кібербезпеки для портової інфраструктури та активною взаємодією з громадськими організаціями. У 2025 році в Одесі відкрито перший в Україні навчальний полігон для практичної підготовки фахівців з кібербезпеки критичної інфраструктури.

Водночас у Вінницькій області спостерігається нижчий рівень розвитку системи кібербезпеки, що проявляється у відсутності регіонального центру реагування на кіберінциденти, недостатньому фінансуванні відповідних заходів та відсутності затвердженої регіональної стратегії станом на 2024 рік. Проте у 2025 році ситуація почала змінюватися: у травні затверджено «Регіональну програму кібербезпеки Вінницької області на 2025-2027 роки» з бюджетом 18,5 млн грн, розпочато створення регіонального центру реагування на кіберінциденти (CERT) на базі обласного департаменту цифрового розвитку.

Аналіз наявних даних вказує на необхідність посилення інституційної бази, підвищення рівня фінансової підтримки та впровадження ефективних механізмів координації з метою забезпечення комплексного захисту інформаційного простору Вінницької області. Таблиця 1.4 наочно демонструє динаміку показників кібербезпеки у Вінницькій області порівняно з іншими регіонами. Вінницька область поступається іншим досліджуваним регіонам за більшістю показників інституційного та ресурсного забезпечення кібербезпеки, хоча у 2025 році спостерігається позитивна динаміка. Водночас, відносно невисока кількість кіберінцидентів може свідчити як про об'єктивно меншу привабливість регіону для кіберзлочинців, так і про недостатньо розвинуту систему виявлення інцидентів. Дані за 2024 рік наведено станом на грудень 2024 року; дані за 2025 рік — станом на вересень 2025 року.

Таблиця 1.4

Порівняльна таблиця основних показників кібербезпеки регіонів України

Показник	Вінницька обл. (2024/2025)	Львівська обл. (2024/2025)	Дніпро. обл. (2024/2025)	Одеська обл. (2024/2025)	м. Київ (2024/2025)
Кількість кіберінцидентів на 1 млн населення	51 / 58	68 / 74	98 / 107	65 / 71	295 / 318
Наявність окремого підрозділу з кібербезпеки в ОДА	Ні / Так	Так / Так	Так / Так	Так / Так	Так / Так
Фінансування кібербезпеки (% від обласного бюджету)	0,12% / 0,18%	0,21% / 0,28%	0,36% / 0,42%	0,19% / 0,23%	0,23% / 0,29%
Наявність регіональної програми кібербезпеки	Розробляється / Так	Так / Так	Так / Так	Так / Так	Так / Так
Кількість фахівців з кібербезпеки в органах влади	3 / 8	14 / 18	17 / 22	9 / 12	28 / 35
Наявність регіонального CERT	Ні / У процесі створення	Так / Так	Так / Так	Ні / Так	Так / Так
Охоплення системою моніторингу держ. сайтів	40% / 58%	78% / 85%	87% / 92%	63% / 72%	96% / 98%
Проведення навчань з кібербезпеки (разів на рік)	1 / 3	5 / 6	7 / 8	5 / 6	14 / 16
Впровадження двофакторної автентифікації для держ. сервісів	25% / 67%	65% / 82%	78% / 88%	52% / 74%	85% / 93%
Участь у міжнародних програмах кібербезпеки	Ні / Так	Так / Так	Так / Так	Так / Так	Так / Так

Позитивна динаміка у Вінницькій області у 2025 році включає: створення спеціалізованого відділу кібербезпеки, збільшення фінансування майже у 1,5 рази, суттєве розширення впровадження двофакторної автентифікації та початок співпраці з міжнародними програмами кібербезпеки в рамках проєкту

EU4Digital. Водночас регіон все ще відстає від лідерів за показниками охоплення моніторингом та кількістю спеціалізованого персоналу, що вказує на необхідність подальших системних зусиль у розбудові регіональної системи кібербезпеки.

Для комплексного оцінювання стану кібербезпеки Вінницької області проведено SWOT-аналіз, що дозволяє виділити сильні та слабкі сторони системи, а також визначити основні виклики і потенційні можливості для її удосконалення. Такий підхід дає змогу розробити стратегічні рекомендації, спрямовані на підвищення ефективності заходів із захисту інформаційних ресурсів регіону (таблиця 1.5).

Таблиця 1.5

SWOT-аналіз системи кібербезпеки Вінницької області

Сильні сторони (S)	Слабкі сторони (W)
- Високий рівень цифровізації публічних послуг - Потужний кадровий потенціал завдяки провідним університетам - Активність місцевої влади у цифровій трансформації - Розвинута IT-спільнота та можливості державно-приватного партнерства - Відносно низький рівень складних кібератак порівняно з промисловими регіонами	- Відсутність спеціалізованого підрозділу з кібербезпеки в ОДА - Недостатнє фінансування заходів з кібербезпеки - Відсутність регіонального CERT - Низький рівень кіберграмотності посадових осіб - Недостатнє технічне оснащення, зокрема захист від DDoS-атак - Слабка координація між суб'єктами кібербезпеки - Нерозвинена система проактивного моніторингу кіберзагроз
Можливості (O)	Загрози (T)
- Створення окремого підрозділу з кібербезпеки в ОДА - Розробка та впровадження регіональної програми кібербезпеки - Заснування Вінницького CERT на базі університету та IT-компаній - Впровадження централізованої системи моніторингу і захисту держсайтів - Організація регулярних навчань і тренінгів - Розвиток державно-приватного партнерства - Залучення міжнародної технічної допомоги - Створення системи обміну інформацією про кіберзагрози між усіма зацікавленими сторонами	- Географічна близькість до зони бойових дій - Наявність об'єктів критичної інфраструктури - Зростання обсягів персональних даних із ризиком витоків - Дефіцит кваліфікованих кадрів у державному секторі - Фінансові обмеження через воєнний стан - Використання застарілого програмного забезпечення

SWOT-аналіз демонструє, що Вінницька область має суттєвий потенціал для розвитку ефективної системи кібербезпеки, зокрема завдяки цифровізації та кадровим ресурсам. Водночас існуючі структурні та фінансові обмеження, а також низький рівень координації і технічного забезпечення потребують системних заходів і впровадження передових практик для посилення кіберзахисту регіону.

1.3. Міжнародні підходи до формування національної системи кібербезпеки

Глобальний характер кіберпростору та транскордонна природа кіберзагроз зумовлюють необхідність вивчення міжнародного досвіду формування національних систем кібербезпеки. Провідні країни світу напрацювали різноманітні моделі організації кібербезпеки, які відображають їхні політичні системи, рівень технологічного розвитку та національні пріоритети.

Американська модель характеризується високим ступенем децентралізації, множинністю суб'єктів забезпечення кібербезпеки та активною роллю приватного сектору. Інституційна архітектура включає понад 50 федеральних агенцій. Головну роль відіграють Агентство з кібербезпеки та захисту інфраструктури (CISA) в складі Департаменту внутрішньої безпеки, Агентство національної безпеки (NSA), Кіберкомандування США (US Cyber Command) та Федеральне бюро розслідувань (FBI). Координацію здійснює Рада національної безпеки при Президентові через посаду Національного координатора з кібербезпеки [18].

Головною особливістю є тісна взаємодія держави з приватним сектором. Понад 85% критичної інфраструктури США перебуває у приватній власності, що робить неможливим забезпечення кібербезпеки виключно державними засобами. Для координації створено галузеві центри обміну інформацією (ISACs), які функціонують у 16 секторах критичної інфраструктури. Федеральний бюджет на кібербезпеку у 2024 фінансовому році склав 13,2 млрд

доларів, що на 12% більше порівняно з попереднім роком. Національна ініціатива з освіти у сфері кібербезпеки координує зусилля університетів у підготовці фахівців, створено понад 380 Центрів академічної досконалості з кібербезпеки.

Для України цінним є американський досвід чіткого розподілу відповідальності між різними агенціями при забезпеченні координації на найвищому рівні, критична роль державно-приватного партнерства, масштабне фінансування та інвестиції в освіту. Водночас, надмірна складність інституційної архітектури може бути неефективною для України в умовах гібридної війни.

Великобританія розробила одну з найбільш ефективних національних систем кібербезпеки у Європі, що базується на інтеграції державних можливостей, приватного сектору та академічних інституцій. Інституційною основою є Національний центр кібербезпеки (NCSC), створений у 2016 році в структурі Центру урядового зв'язку (GCHQ). NCSC виконує функції національного CERT, надає консультації урядовим структурам та приватному сектору, проводить аудити безпеки критичної інфраструктури, розробляє керівництва та стандарти. Стратегічне бачення визначається Національною стратегією кібербезпеки, яка оновлюється кожні 5 років. Чинна стратегія на 2022-2030 роки визначає п'ять стратегічних пріоритетів: зміцнення кіберекосистеми, побудова стійкої цифрової економіки, протидія кіберзлочинності, стримування та реагування на ворожі кібердії, лідерство у глобальному кіберпросторі. На реалізацію стратегії виділено 2,6 млрд фунтів стерлінгів на період 2022-2025 років. Особливістю британської моделі є програма CyberFirst, спрямована на залучення талановитої молоді до сфери кібербезпеки. За 7 років існування програми в ній взяли участь понад 100 тисяч молодих людей.

Великобританія активно розвиває міжнародну співпрацю у сфері кібербезпеки. NCSC підтримує партнерські відносини з аналогічними структурами понад 30 країн. Особливо тісна співпраця налагоджена в рамках альянсу «Five Eyes». Для України корисним є британський досвід створення

єдиного центру компетенцій з кібербезпеки, довгострокового стратегічного планування, інвестицій у молодь та освіту, міжнародної співпраці [11].

Естонія, попри невеликий розмір, є визнаним лідером у сфері кібербезпеки та цифрової трансформації. Після кібератак 2007 року країна радикально переосмислила підходи до кібербезпеки. Було створено Управління з кібербезпеки при Міністерстві оборони, яке відповідає за стратегічне планування та координацію. Оперативні функції виконує Центр реагування на комп'ютерні інциденти CERT-EE, який працює в режимі 24/7. Унікальною є концепція «кіберзахисту на рівні держави», яка передбачає залучення не лише державних структур, а й бізнесу, громадських організацій та окремих громадян. Створено Лігу кіберзахисту Естонії – добровільну організацію з понад 200 IT-фахівців, які в критичних ситуаціях можуть бути мобілізовані для захисту критичної інфраструктури. Технологічною основою є розподілена архітектура державних інформаційних систем, побудована на технології блокчейн (X-Road), яка забезпечує безпечний обмін даними між різними державними базами даних.

Естонія розробила концепцію «електронного резидентства» та «цифрового посольства». Також державні дані резервуються на серверах у Люксембурзі, що забезпечує їх збереження навіть у разі окупації території. Цей досвід є надзвичайно актуальним для України в умовах війни. Освіта з кібербезпеки інтегрована в естонську систему освіти на всіх рівнях. В столиці Естонії розміщено Кооперативний центр передового досвіду з кіберзахисту НАТО. Естонський досвід демонструє можливість створення ефективної системи кібербезпеки навіть при обмежених ресурсах, важливість залучення всього суспільства, переваги розподіленої архітектури, необхідність резервування критичних даних за кордоном.

Ізраїль є однією з провідних кібердержав світу, що зумовлено постійними безпековими викликами та високорозвиненою технологічною індустрією. Ізраїльська модель характеризується тісним зв'язком між військовим та цивільним секторами кібербезпеки. Центральним органом є Національне управління з кібербезпеки (NCD) при апараті Прем'єр-міністра, створене у 2017

році. NCD відповідає за формування національної політики, координацію діяльності різних відомств, захист критичної інфраструктури, розвиток національної кіберіндустрії. Особливістю є роль військової розвідки, зокрема Підрозділу 8200 – елітного кіберпідрозділу Армії оборони Ізраїлю. Військова служба у кіберпідрозділах стає трампліном для кар'єри у приватному секторі кібербезпеки, що забезпечує постійний потік високоякісних кадрів та трансфер технологій. Ізраїль розробив національну програму розвитку людського капіталу, яка включає виявлення талановитої молоді ще у шкільному віці, створення спеціалізованих класів, стипендіальні програми [17].

Ізраїльська кіберіндустрія є однією з найбільш розвинутих у світі. Понад 500 компаній працюють у сфері кібербезпеки, щорічно залучаючи понад 1 млрд доларів інвестицій. Держава активно підтримує цю індустрію через програму Israel Innovation Authority. Ізраїль розробив доктрину «активного кіберзахисту», яка передбачає не лише оборонні, а й наступальні кібероперації проти ворожих акторів. Для України головним є досвід інтеграції військових та цивільних можливостей, ефективність системи виявлення та розвитку талантів, потенціал розвитку національної кіберіндустрії.

Сінгапур розробив одну з найбільш ефективних систем кібербезпеки в Азійсько-Тихоокеанському регіоні, поєднуючи високий рівень централізації з технологічними інноваціями. Центральним органом є Агентство з кібербезпеки Сінгапуру (CSA), створене у 2015 році під егідою Прем'єр-міністра. CSA виконує функції національного регулятора, координатора, оператора національного CERT та центру компетенцій. У 2016 році прийнято Акт про кібербезпеку, який встановив жорсткі вимоги до власників критичної інформаційної інфраструктури. Визначено 11 секторів CII, власники яких зобов'язані дотримуватися суворих стандартів безпеки, регулярно проходити аудити, повідомляти про інциденти.

Сінгапур розробив Національну стратегію кібербезпеки 2021, яка визначає чотири стратегічні пріоритети. На реалізацію виділено понад 1 млрд сінгапурських доларів. Особливістю є програма SG Cyber Safe, спрямована на

підвищення рівня кібергігієни населення та бізнесу. Програма включає масштабні освітні кампанії, безкоштовні консультації для малого та середнього бізнесу, розробку зрозумілих керівництв. Сінгапур активно залучає міжнародні таланти через спеціальні імміграційні програми для фахівців з кібербезпеки. Для України цінним є досвід централізованої моделі управління, чіткого законодавчого регулювання з жорсткими вимогами до критичної інфраструктури, масштабних освітніх програм.

Європейський Союз розробив наднаціональну модель кібербезпеки, яка координує зусилля країн-членів та встановлює спільні стандарти. Нормативною основою є Директива NIS 2016 року та оновлена Директива NIS2 2022 року, яка розширила коло суб'єктів регулювання, встановила жорсткіші вимоги до управління ризиками, посилила вимоги до повідомлення про інциденти, передбачила суворі санкції за недотримання вимог (до 10 млн євро або 2% глобального річного обороту). Регламент про кібербезпеку 2019 року створив загальноєвропейську систему сертифікації продуктів, послуг та процесів кібербезпеки. Агентство ЄС з кібербезпеки (ENISA) виконує роль центру експертизи, надає рекомендації країнам-членам, проводить дослідження, організовує навчання. Щорічні пан'європейські кіберучення Cyber Europe залучають сотні організацій з усіх країн-членів. У 2023 році запущено Закон про кіберстійкість, який встановлює обов'язкові вимоги до кібербезпеки для всіх продуктів з цифровими елементами. Європейський досвід демонструє першість гармонізації національного законодавства з міжнародними стандартами, ефективність регіональної співпраці, необхідність встановлення вимог до виробників [34].

Аналіз розглянутих моделей виявив спільні елементи успішних систем: наявність центрального координаційного органу з чіткими повноваженнями, автоматизація обміну інформацією про загрози в реальному часі, чітке розмежування ролей між учасниками, регулярні масштабні навчання для відпрацювання координації, формалізовані механізми державно-приватного партнерства, активна міжнародна інтеграція. Відмінності полягають у ступені

централізації, співвідношенні ролі держави та приватного сектору, акценті на оборонних чи наступальних можливостях, моделі фінансування, рівні відкритості діяльності структур кібербезпеки (таблиця 1.6).

Таблиця 1.6

Порівняльна характеристика моделей кібербезпеки

Критерій	США	Великобританія	Естонія	Ізраїль	Сінгапур
Ступінь централізації	Низький	Середній	Високий	Високий	Дуже високий
Роль держави	Координація	Регулювання + сервіси	Мобілізація	Інтеграція	Жорсткий контроль
Участь приватного сектору	Дуже висока	Висока	Висока	Дуже висока	Середня
Фінансування (% ВВП)	0,08%	0,12%	0,15%	0,25%	0,18%
Фокус	Інфраструктура	Екосистема	Стійкість	Наступ + оборона	Регулювання
Освіта та кадри	Університети + ISACs	Програми для молоді	Інтеграція в освіту	Військові + цивільні	Залучення талантів

Міжнародний досвід демонструє, що універсальної моделі кібербезпеки не існує. Кожна країна формує свою систему відповідно до власних умов, викликів та можливостей. Для України найбільш релевантними є елементи естонської моделі (розподілена архітектура, резервування даних за кордоном, залучення громадськості через Лігу кіберзахисту), британської моделі (централізація експертизи у єдиному центрі на зразок NCSC, стратегічне планування з горизонтом 5-10 років), ізраїльської моделі (інтеграція військових та цивільних можливостей, система підготовки кадрів через військову службу, розвиток кіберіндустрії як джерела технологій), європейської моделі (гармонізація законодавства з директивами ЄС, регіональна співпраця, участь у спільних навчаннях).

Головними уроками для України є необхідність створення єдиного центру координації з широкими повноваженнями, розвиток автоматизованих систем обміну інформацією про загрози, інвестиції в освіту та підготовку кадрів на всіх

рівнях, формалізація державно-приватного партнерства через створення механізмів обміну інформацією та спільного реагування, приведення законодавства у відповідність до європейських стандартів, резервування критичних даних за кордоном для забезпечення стійкості. Водночас, пряме копіювання будь-якої моделі є неможливим через специфіку викликів, які стоять перед Україною в умовах гібридної війни.

Висновки до розділу 1

Дослідження теоретико-методологічних засад публічного управління у сфері кібербезпеки показало, що кібербезпека еволюціонувала від технічного питання до комплексного елементу національної безпеки, який охоплює правові, організаційні, технологічні, освітні та міжнародні аспекти. Сучасна модель управління вимагає багатосторонньої взаємодії між державою, бізнесом і громадянським суспільством. Аналіз ситуації у Вінницькій області виявив суттєві розбіжності між рівнем цифровізації та слабкістю інституційної спроможності в порівнянні з іншими регіонами. Міжнародний досвід підтверджує необхідність централізованої координації, стратегічного планування, підготовки кадрів, захисту критичної інфраструктури та розвитку партнерств. Для України найбільш доцільним є комбінований підхід із впровадженням елементів естонської, британської, ізраїльської та європейської моделей кібербезпеки.

РОЗДІЛ 2. НОРМАТИВНО-ПРАВОВЕ ТА ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

2.1. Аналіз законодавчої та нормативної бази України у сфері кібербезпеки: зарубіжний досвід та українські реалії

Конституційною основою правового регулювання кібербезпеки в Україні є стаття 17 Основного Закону, яка визначає забезпечення інформаційної безпеки як одну з найважливіших функцій держави. Стаття 31 гарантує таємницю листування та іншої кореспонденції, що у цифрову епоху поширюється на електронні комунікації. Стаття 32 закріплює право на невтручання в особисте життя, включаючи захист персональних даних.

Базовим законом є Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року [8]. Закон визначає кібербезпеку як захищеність життєво важливих інтересів людини, суспільства та держави під час використання кіберпростору, встановлює об'єкти кібербезпеки, визначає суб'єкти забезпечення та їх повноваження. Проте закон має недоліки: недостатньо чітке розмежування повноважень різних суб'єктів, відсутність механізмів притягнення до відповідальності, обмежене коло об'єктів критичної інфраструктури, відсутність деталізації процедур реагування на кіберінциденти.

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 1994 року встановлює правові та організаційні засади захисту інформації, проте потребує комплексного перегляду через застарілість та невідповідність сучасним технологічним реаліям [9]. Закон України «Про захист персональних даних» від 2010 року регулює правовідносини щодо обробки персональних даних, проте після прийняття GDPR потребує суттєвого оновлення. У 2023 році Верховна Рада прийняла у першому читанні проєкт нового закону для приведення у відповідність до європейських стандартів. Кримінальний кодекс України містить Розділ XVI про

злочини у сфері використання комп'ютерів, який встановлює відповідальність за кіберзлочини. Проте правозастосовча практика свідчить про недостатню ефективність через складність доказування, обмежені можливості міжнародної співпраці та недостатню кваліфікацію правоохоронців.

Стратегія кібербезпеки України, затверджена Указом Президента від 14 березня 2016 року, визначила п'ять стратегічних цілей: досягнення необхідного рівня кіберзахисту критичної інфраструктури, ефективність системи управління, захист прав людини у кіберпросторі, розвиток людського капіталу, міжнародне співробітництво. Моніторинг виконання плану заходів виявив, що лише 60% запланованих заходів було виконано повністю або частково. У 2021 році розпочалася розробка нової Стратегії на період до 2025 року з урахуванням досвіду протидії російській агресії. Стратегія національної безпеки України 2020 року визначає кібербезпеку як один з пріоритетів національної безпеки та передбачає розбудову національної системи, спроможної протидіяти загрозам в умовах гібридної війни. Доктрина інформаційної безпеки України 2017 року розглядає кібербезпеку як складову інформаційної безпеки, визначає основні загрози та встановлює пріоритетні напрями державної політики.

Постанова КМУ «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» від 19 червня 2019 року №518 встановлює базові вимоги до організації кіберзахисту, визначає категорії об'єктів, вимоги до організаційних та технічних заходів захисту [15]. Постанова КМУ «Про затвердження Порядку формування переліку об'єктів критичної інфраструктури» від 9 жовтня 2020 року №943 встановлює процедуру визначення критично важливих об'єктів. Станом на 2024 рік до переліку включено понад 1200 об'єктів у різних секторах. Наказ ДССЗЗІ «Про затвердження Порядку інформування про кіберінциденти» від 22 лютого 2019 року №9 встановлює процедури повідомлення про інциденти, їх класифікацію та порядок реагування, зобов'язує суб'єктів повідомляти CERT-UA про серйозні кіберінциденти [14]. Наказ Міністерства цифрової трансформації від 2 листопада 2022 року встановлює вимоги до захисту інформаційних систем органів

державної влади, включаючи технічні та організаційні заходи, періодичність аудитів, вимоги до навчання персоналу.

Директива NIS2, прийнята ЄС у 2022 році, є основним документом у сфері кібербезпеки. Вона розширює коло суб'єктів регулювання до середніх та великих підприємств у 18 секторах, встановлює жорсткіші вимоги до управління ризиками, посилює вимоги до повідомлення про інциденти (протягом 24 годин), передбачає суворі санкції (до 10 млн євро або 2% глобального обороту). Порівняно з NIS2, український Закон про кібербезпеку має переваги у більш широкому визначенні кіберпростору та об'єктів захисту, закріпленні координаційної ролі РНБО, врахуванні специфіки гібридних загроз. Недоліки включають менш чітке визначення секторів критичної інфраструктури, відсутність детальних вимог до управління ризиками, нечіткі терміни повідомлення про інциденти, відсутність конкретних санкцій, обмежене коло суб'єктів регулювання [12].

Загальний регламент про захист даних (GDPR) 2016 року встановив нові стандарти захисту персональних даних. Він визначає принципи обробки персональних даних, права суб'єктів даних (доступ, виправлення, видалення, перенесення), обов'язки контролерів та обробників даних, значні штрафи за порушення (до 20 млн євро або 4% глобального обороту). Чинний український закон про захист персональних даних частково відповідає GDPR, проте має суттєві прогалини: відсутність чіткого визначення ролей контролера та обробника, обмежені права суб'єктів даних, відсутність вимоги оцінки впливу на захист даних, неефективна система санкцій (таблиця 2.1).

Акт про кіберстійкість, прийнятий ЄС у 2023 році, встановлює обов'язкові вимоги до кібербезпеки продуктів з цифровими елементами: безпека за замовчуванням, надання оновлень протягом мінімум 5 років, повідомлення про вразливості протягом 24 годин, процедури сертифікації, санкції за недотримання (до 15 млн євро або 2,5% обороту). В Україні відсутнє аналогічне законодавство, що створює значні ризики для користувачів [6].

Таблиця 2.1

Порівняння українського законодавства з європейськими стандартами

Аспект	Україна	ЄС (NIS2 / GDPR)	Рівень відповідності
Визначення критичної інфраструктури	Обмежене	18 секторів	Низький
Вимоги до управління ризиками	Загальні	Деталізовані	Середній
Терміни повідомлення про інциденти	Нечіткі	24–72 години	Низький
Санкції за порушення	Символічні	До 4% річного обороту	Дуже низький
Захист персональних даних	Частковий	Повна відповідність GDPR	Середній
Вимоги до продуктів	Відсутні	Акт про кіберстійкість (CRA)	Відсутній

Законодавство США характеризується фрагментарністю та наявністю численних секторальних актів. Ключовими є Акт про безпеку федеральних інформаційних систем (FISMA) 2002 року, Акт про обмін інформацією про кіберзагрози (CISA) 2015 року, Акт про звітність про кіберінциденти (CIRCIA) 2022 року, який зобов'язує операторів критичної інфраструктури повідомляти про серйозні інциденти протягом 72 годин. Україна може запозичити механізми стимулювання добровільного обміну інформацією з обмеженням відповідальності, підхід до встановлення вимог через галузеві стандарти, практику регулярних аудитів інформаційних систем [21, 22].

Законодавство Великобританії після Brexit включає Закон про захист даних 2018 року, що імплементував GDPR з доповненнями, та Закон про комп'ютерні зловживання 1990 року з численними поправками. Особливістю є активна роль NCSC у розробці керівництв та рекомендацій, які фактично стають галузевими стандартами. Україна може запозичити практику розробки детальних керівництв для різних категорій суб'єктів, систему добровільної сертифікації продуктів кібербезпеки. Естонія створила комплексне законодавство, що інтегрує всі аспекти цифрової трансформації та кібербезпеки. Закон про кібербезпеку 2018 року імплементував Директиву NIS з додатковими вимогами. Закон про цифровий підпис створив правову основу для електронних

підписів на основі блокчейн-технології. Для України цінним є естонський досвід законодавчого закріплення розподіленої архітектури державних систем, обов'язкового резервування критичних даних, прав громадян контролювати доступ до своїх персональних даних, відповідальності посадових осіб за несанкціонований доступ [25].

Комплексний аналіз виявляє системні недоліки: фрагментарність та несистемність – норми розпорошені по численних законах без єдиної термінології; застарілість окремих норм – ряд законів 1990-х років не відповідає сучасним технологічним реаліям; неузгодженість з європейськими стандартами – відсутність повної імплементації NIS2, GDPR, Акту про кіберстійкість; недостатня деталізація вимог – базові закони встановлюють загальні принципи без конкретних вимог; відсутність ефективних санкцій – штрафи є символічними (від 17 до 255 грн) і не створюють стримуючого ефекту; нечіткість повноважень суб'єктів – дублювання або недостатнє розмежування компетенції; обмеженість механізмів державно-приватного партнерства – відсутність правових стимулів для участі бізнесу; недостатнє регулювання нових технологій – відсутність вимог до AI, квантових обчислень, блокчейн, 5G мереж.

На основі проведеного аналізу сформульовано рекомендації: кодифікація законодавства через розробку Кодексу кібербезпеки або нової редакції базового закону; повна імплементація європейських директив – завершення імплементації NIS2, прийняття нового закону про захист персональних даних відповідно до GDPR, розробка законодавства про кіберстійкість продуктів; модернізація системи санкцій – встановлення адекватних штрафів (2-4% річного обороту); чітке розмежування повноважень через внесення змін до базового закону з функціональним розподілом компетенції; створення правових основ державно-приватного партнерства – прийняття законодавства про механізми обміну інформацією з гарантіями конфіденційності; регулювання нових технологій – розробка законодавства про штучний інтелект, оновлення вимог до криптографічного захисту, врегулювання блокчейн-технологій; вдосконалення процедур реагування – встановлення чітких термінів повідомлення про

інциденти; гармонізація термінології через розробку національного стандарту термінології у сфері кібербезпеки [4].

2.2. Взаємодія державних органів, приватного сектору та громадянського суспільства у забезпеченні кібербезпеки

Закон України «Про основні засади забезпечення кібербезпеки України» визначає 14 суб'єктів забезпечення кібербезпеки. Рада національної безпеки і оборони України є головним координаційним органом, координує діяльність органів виконавчої влади, розробляє стратегії, здійснює щорічну оцінку стану кібербезпеки. При РНБО функціонує Ситуаційний центр забезпечення кібербезпеки. Проте РНБО не є оперативним органом, засідання проводяться епізодично, що не відповідає динаміці кіберзагроз. Служба безпеки України здійснює контррозвідувальні заходи у кіберпросторі, виявлення та припинення кібератак з боку іноземних спецслужб, захист державних інформаційних ресурсів з державною таємницею.

У 2022-2024 роках роль СБУ у сфері кібербезпеки значно зросла – виявлено та нейтралізовано понад 150 спроб проникнення в державні системи з боку російських спецслужб. Розвідувальні органи України здійснюють кіберрозвідку, збір інформації про кіберзагрози. Станом на 2025 рік СБУ продовжує активно протидіяти кіберзагрозам з боку росії, нейтралізуючи кібератаки на критичну інфраструктуру та державні системи, викриваючи агентурні мережі кібершпигунства, блокуючи пропагандистські ресурси та дезінформаційні кампанії. Кіберфронт залишається одним з ключових напрямків протистояння в російсько-українській війні, а СБУ разом з іншими органами забезпечує захист цифрового суверенітету України та запобігає втраті критично важливої інформації. Діяльність розвідувальних органів України у кіберпросторі є важливою складовою національної безпеки в умовах триваючої повномасштабної агресії [10]

Міністерство оборони та Збройні Сили відповідають за кіберзахист військових об'єктів, проведення кібернетичних операцій у рамках бойових дій. У структурі ЗСУ створено кіберкомандування, кількість військовослужбовців кіберпідрозділів зросла з 500 осіб у 2020 році до понад 3000 у 2024 році. Національна поліція, зокрема Департамент кіберполіції, розслідує кіберзлочини, проводить профілактичну роботу. У 2023 році розслідувано понад 5000 кримінальних проваджень, заблоковано понад 2000 фішингових сайтів. Державна служба спеціального зв'язку та захисту інформації є центральним органом виконавчої влади у сфері кіберзахисту. При ДССЗЗІ функціонує CERT-UA, який є національним центром реагування на кіберінциденти. У 2023 році CERT-UA обробив понад 7500 повідомлень про інциденти, випустив понад 250 попереджень, надав технічну допомогу у реагуванні на понад 1000 серйозних інцидентів. Міністерство цифрової трансформації формує політику у сферах цифровізації, електронного урядування, відповідає за впровадження принципів «безпеки за замовчуванням» у всі цифрові ініціативи. Національний банк України регулює кібербезпеку у фінансовому секторі, встановлює вимоги до банків, проводить аудити [20].

Аналіз виявляє низку проблем: дублювання функцій та конкуренція за ресурси – повноваження різних відомств перетинаються, що призводить до марнування до 20-30% ресурсів; обмежений обмін інформацією – відомства неохоче діляться інформацією про загрози, мотивуючи це вимогами секретності; відмінності у організаційних культурах – військові структури, спецслужби, правоохоронні органи та цивільні відомства мають різні підходи до комунікації; недостатні повноваження координаційного органу – РНБО має обмежені важелі впливу на суб'єкти забезпечення кібербезпеки. Приватний сектор володіє більшістю критичної інфраструктури та відіграє критично важливу роль. Оператори критичної інфраструктури (енергетичні компанії, телекомунікаційні оператори, банки) несуть відповідальність за захист своїх систем. Дослідження 2023 року виявило, що рівень захищеності суттєво відрізняється – великі

компанії мають високий рівень кібербезпеки, менші компанії часто мають недостатній захист через обмежені ресурси [13].

Український ринок послуг кібербезпеки активно розвивається. За оцінками, обсяг ринку у 2023 році склав близько 200 млн доларів, зростаючи темпами 25-30% щорічно. У 2024-2025 роках ринок продовжив розширюватись, досягнувши обсягу понад 250 млн доларів, що зумовлено зростаючим попитом на послуги кіберзахисту в умовах війни. Провідні компанії надають послуги з оцінки вразливостей, розробки систем захисту, реагування на інциденти. Фінансовий сектор є однією з найбільш атакованих категорій. У 2023 році зафіксовано понад 200 значних кібератак на фінансові установи, а до 2025 року їх кількість зросла до понад 300, що відображає інтенсифікацію кібервійни. Банки інвестують близько 5-7% бюджету IT-департаментів у кібербезпеку, при цьому провідні установи збільшили цей показник до 8-10% у 2025 році. Національний банк України у 2019 році створив Центр кіберзахисту фінансового сектору для координації зусиль банків [28, 23].

CERT-UA створив платформу обміну інформацією про кіберзагрози. За 2023 рік у програмі взяли участь понад 300 компаній, а станом на 2025 рік кількість учасників зросла до понад 450 організацій. Проте система має недоліки: відсутність правових гарантій конфіденційності, обмежена кількість учасників, одностороннє спрямування інформації. ДССЗЗІ спільно з приватними компаніями проводить кіберучення. У 2023 році відбулося 4 масштабні учення за участю понад 50 організацій, а у 2024-2025 роках кількість таких заходів збільшилась до 6-8 щорічно з участю понад 80 організацій. При ДССЗЗІ, Міністерстві цифрової трансформації, Національному банку функціонують консультативні ради з участю представників бізнесу, проте їх вплив на політику залишається обмеженим.

В Україні функціонують активні громадські організації: ГО «Лабораторія цифрової безпеки», що надає консультації журналістам та активістам; ГО «Центр демократії та верховенства права», що досліджує питання приватності; ГО «Інтернет-асоціація України», що об'єднує провайдерів. Ці організації

виконують функції підвищення обізнаності населення, адвокації змін у законодавстві, моніторингу дотримання прав людини, надання безкоштовних консультацій. Університети відіграють подвійну роль: готують фахівців та проводять дослідження. Провідні університети мають спеціалізовані кафедри та дослідні центри кібербезпеки, активно співпрацюють з державою та бізнесом. Етичні хакери роблять значний внесок у виявлення вразливостей. У 2023 році в Україні відбулося кілька хакатонів з кібербезпеки, учасники виявили десятки вразливостей. У 2024-2025 роках кількість таких заходів зросла, проте відсутність культури bug bounty programs все ще обмежує залучення хакерської спільноти. ЗМІ відіграють важливу роль у підвищенні обізнаності громадськості, проте рівень компетентності журналістів у питаннях кібербезпеки часто є недостатнім. Кожен громадянин є як об'єктом захисту, так і потенційною вразливістю. Недостатня кібергігієна користувачів створює ризики не лише для них самих, а й для організацій, де вони працюють.

Ефективна взаємодія стикається з бар'єрами: недовіра між секторами – історична недовіра між державою та бізнесом ускладнює партнерство; відмінності у цілях та пріоритетах – держава фокусується на національній безпеці, бізнес керується економічною доцільністю, громадянське суспільство акцентує права людини; асиметрія інформації та компетенцій – держава володіє розвідувальною інформацією, бізнес має технології та експертизу, громадянське суспільство має довіру населення; правові обмеження – чинне законодавство не створює достатніх правових підстав для повноцінного партнерства; дисбаланс у ресурсах – великі компанії мають значні ресурси, малий бізнес та громадські організації мають обмежені можливості.

Попри виклики, є успішні приклади: програма «Армія кіберзахисту», запущена Міністерством цифрової трансформації у 2022 році, об'єднала понад 1000 IT-фахівців, які на волонтерських засадах допомагають державі, а станом на 2025 рік кількість учасників перевищила 1500 осіб; партнерство з міжнародними IT-компаніями (Microsoft, Google, Amazon, Cisco), які надають рішення на преференційних умовах та у 2024-2025 роках розширили підтримку

через програми навчання та передачі технологій; Центр кіберзахисту фінансового сектору НБУ, який об'єднав банки для спільної протидії загрозам та за період з 2022 по 2025 рік допоміг запобігти понад 150 серйозним атакам; програма «Дія. City» для IT-компаній, що включає підвищені вимоги до кібербезпеки та створює стимули для впровадження міжнародних стандартів [19].

На основі аналізу сформульовано рекомендації: створення Національної платформи обміну інформацією про кіберзагрози за зразком британської CiSP з правовими гарантіями конфіденційності; запровадження галузевих центрів кібербезпеки (ISACs) для ключових секторів економіки за американською моделлю; розвиток інституту кіберволонтерів через формалізацію програми «Армія кіберзахисту» з чіткою структурою та системою мотивації; створення програм bug bounty для державних систем; посилення ролі консультативних рад через надання реальних повноважень; запровадження програми підтримки кібербезпеки для малого та середнього бізнесу за зразком сінгапурської SG Cyber Safe; розвиток академічного партнерства через створення мережі регіональних центрів компетенцій; посилення медіаграмотності через національну кампанію з підвищення кіберграмотності населення.

2.3. Оцінка ефективності чинної моделі управління кібербезпекою в Україні

Для комплексної оцінки ефективності системи управління кібербезпекою використано комбінацію підходів: індексний підхід через використання Global Cybersecurity Index (GCI) ITU, оцінку ризиків через аналіз зменшення ймовірності успішних атак, порівняльний підхід (benchmarking) з іншими країнами, підхід на основі зрілості (maturity model). За даними GCI 2021, Україна посіла 57-е місце серед 182 країн з балом 78,7 зі 100, що відповідає середньому рівню (таблиця 2.2).

Таблиця 2.2

Інтегральна оцінка ефективності системи кібербезпеки України

Вимір	Оцінка (0–10)	Характеристика
Правовий	5,7	Середній – є базове законодавство, але потребує модернізації
Організаційний	4,25	Нижче середнього – проблеми координації та кадровий дефіцит
Технічний	5,25	Середній – наявна технічна база, але інфраструктура потребує оновлення
Розвиток потенціалу	3,75	Низький – гострий брак фахівців, слабка підготовка та обізнаність населення
Міжнародний	7,5	Вище середнього – активна міжнародна взаємодія та технічна допомога
ЗАГАЛЬНИЙ	5,29	Середній рівень ефективності

Правовий вимір кібербезпеки в Україні демонструє наявність основних нормативно-правових засад: діє базовий Закон про кібербезпеку, ухвалено Стратегію, існують галузеві закони, що забезпечує певну основу (оцінка 7/10). Разом із тим, імплементація європейських директив відбувається частково, ратифіковано Будапештську конвенцію, але процес повної гармонізації законодавства з європейськими стандартами ще не завершено (6/10). Ефективність правозастосування залишається низькою через символічність санкцій і брак відповідної кваліфікації у відповідальних органах (4/10). Загальна оцінка правового виміру становить 5,7/10.

В організаційному вимірі створено ключові інституції — CERT-UA, кіберпідрозділи в СБУ, Міноборони, Нацполіції, функціонує координаційний центр при РНБО (7/10). Водночас спостерігається обмежена координація між структурами, дублювання функцій і слабкий обмін інформацією (4/10), а також хронічний дефіцит кадрів, низький рівень зарплат і значний відтік фахівців (3/10). Додатково, рівень фінансування галузі — лише близько 0,15% бюджету — суттєво нижчий за міжнародні рекомендації (3/10), що формує загальну оцінку організаційного виміру на рівні 4,25/10. У технічному вимірі державні системи частково мають сучасні засоби захисту, а CERT-UA забезпечена базовим технічним оснащенням, хоча значна частина державних систем використовує застаріле програмне забезпечення (5/10). CERT-UA виконує цілодобовий моніторинг, хоча він охоплює переважно державний сектор (5/10);

середній час реагування є досить оперативним — 2–4 години (7/10). Водночас використання інструментів штучного інтелекту, машинного навчання та автоматизації залишається обмеженим (4/10), що визначає загальну оцінку технічного виміру на рівні 5,25/10.

Вимір розвитку потенціалу у сфері кібербезпеки в Україні має низку важливих складників, однак загалом оцінюється як недостатній. Університети щороку випускають близько 1000 фахівців у галузі, що значно менше від потреби у 5000–7000 нових спеціалістів (4/10). Хоча в Україні діють національні стандарти, розроблені на основі міжнародних (ISO 27001, NIST), їхнє впровадження не є обов'язковим, що обмежує загальний рівень кіберстійкості (5/10). Кампанії з підвищення обізнаності населення про загрози в кіберпросторі мають епізодичний характер і не є системними — згідно з даними КМІС, лише 23% українців знають, як розпізнати фішинг (3/10). Крім того, фінансування наукових досліджень у сфері кібербезпеки є обмеженим, більшість інновацій генерується у приватному секторі, що знижує рівень державного впливу на розвиток технологій (3/10). Загальна оцінка цього виміру становить 3,75/10.

Міжнародний вимір демонструє значно вищі результати. Україна є учасником Будапештської конвенції та активно співпрацює з НАТО й Європейським Союзом (8/10). Налагоджено стабільні зв'язки з провідними міжнародними партнерами — США, Великобританією, країнами ЄС, Ізраїлем, із якими підписано понад 20 міждержавних меморандумів (7/10). CERT-UA бере участь в обміні інформацією з іноземними кіберцентрами, що сприяє оперативному реагуванню на інциденти (6/10). Окрім цього, обсяг міжнародної технічної допомоги у 2022–2023 роках перевищив 100 мільйонів доларів, що суттєво підвищило спроможність національної системи кібербезпеки (9/10). Загальна оцінка міжнародного виміру становить 7,5/10. Інтегральний показник ефективності становить 5,29 з 10, що відповідає середньому рівню ефективності національної системи кібербезпеки:

$$\text{Інтегральний показник ефективності} = (5{,}7 + 4{,}25 + 5{,}25 + 3{,}75 + 7{,}5)/5 = 5{,}29/10$$

Система має сформовані базові інститути, нормативно-правову основу та міжнародну підтримку, що дозволяє ефективно реагувати на типові кіберзагрози. Водночас вона стикається з суттєвими викликами у сферах кадрового та фінансового забезпечення, міжвідомчої координації, розвитку людського капіталу й інноваційного потенціалу. Ці фактори обмежують її здатність адаптуватися до складніших і високотехнологічних загроз. Чинна модель кібербезпеки в Україні має комплексну структуру, яка поєднує державні ініціативи, міжнародну підтримку та громадянську активність. Водночас система стикається з низкою внутрішніх та зовнішніх викликів, які стримують її розвиток. Нижче наведено узагальнений SWOT-аналіз, що дозволяє оцінити потенціал і загрози для подальшого вдосконалення моделі (таблиця 2.3).

Таблиця 2.3

SWOT-аналіз національної моделі кібербезпеки України

Сильні сторони (S)	Слабкі сторони (W)
– Є стратегія, закони і бачення розвитку. – Працює CERT-UA — швидко реагує і має міжнародне визнання. – Маємо досвід боротьби з великими кібератаками. – Отримуємо підтримку і технології від інших країн. – Сильна IT-індустрія, яка може допомагати державі. – Ативне громадянське суспільство — створена "Армія кіберзахисту".	– Дуже мало фінансування. – Бракує фахівців, особливо через низькі зарплати в держсекторі. – Погана координація між державними структурами. – Багато старої техніки й програм. – Люди та чиновники мало знають про кібербезпеку. – Санкції за порушення слабкі. – Повільно впроваджуються стандарти ЄС.
Можливості (O)	**Загрози (T)**
– Євроінтеграція стимулює розвиток кібербезпеки. – Можна залучати міжнародну допомогу. – Цифровізація створює попит на кіберзахист. – Наш досвід можна продавати іншим країнам. – Можна ефективно працювати з IT-компаніями. – Нові технології (AI, автоматизація) можуть покращити захист. – Молодь має хороші цифрові навички.	– Зростає кількість атак з боку Росії. – IT-фахівці виїжджають за кордон. – Обмежений бюджет через війну. – Важко встигати за новими технологіями. – Більше кіберзлочинності під час війни. – Залежність від іноземних технологій. – З’являються нові загрози — як-от штучний інтелект чи квантові технології.

Порівняння демонструє, що Україна відстає від лідерів за більшістю показників, особливо у фінансуванні, кадровому забезпеченні та охопленні моніторингом критичної інфраструктури (таблиця 2.4).

Таблиця 2.4

Порівняння України з міжнародними бенчмарками

Показник	Україна	Естонія	Ізраїль	Великобританія	США
Фінансування (% ВВП)	0,02%	0,15%	0,25%	0,12%	0,08%
Фахівці на 100 тис. населення	12	45	60	35	28
Час реагування (години)	2–4	1–2	1–3	2–3	1–3
Охоплення моніторингом КІ	40%	95%	90%	85%	70%
Позиція в GCI 2021	57	8	6	3	1

В умовах повномасштабної війни (2022-2025) система демонструє вищу ефективність, ніж можна було очікувати. Позитивні результати включають: стійкість критичної інфраструктури попри інтенсивні кібератаки; швидке реагування CERT-UA зі скороченням часу з 6-8 до 2-4 годин; успішну мобілізацію волонтерів та міжнародної підтримки; інформаційну прозорість через регулярні публікації про загрози. Проблеми включають: фізичне знищення інфраструктури ракетними ударами; перевантаження ресурсів через інтенсивність атак; витік інформації через окупацію територій; психологічне навантаження на фахівців.

Загалом, в умовах війни українська система кібербезпеки демонструє вищу ефективність та адаптивність, що свідчить про професіоналізм фахівців та ефективність міжнародної підтримки. Проте довгострокова стійкість під загрозою через вичерпання ресурсів.

Висновки до розділу 2

Проведений аналіз дозволяє сформулювати наступні висновки. Нормативно-правова база України має базові елементи, проте потребує суттєвого вдосконалення для приведення у відповідність до європейських стандартів. Ключові недоліки включають фрагментарність законодавства, застарілість окремих норм, відсутність ефективних санкцій, повільну імплементацію директив ЄС. Взаємодія державних органів, приватного сектору та громадянського суспільства характеризується наявністю окремих успішних ініціатив, проте системні механізми партнерства розвинені недостатньо через недовіру між секторами, відмінності у цілях, правові обмеження, дисбаланс у ресурсах.

Ефективність чинної моделі управління кібербезпекою оцінюється як середня (5,29/10). Найсильнішим є міжнародний вимір (7,5/10), найслабшими – організаційний (4,25/10) та вимір розвитку потенціалу (3,75/10). В умовах війни система демонструє вищу ефективність та адаптивність порівняно з мирним

часом, проте довгострокова стійкість під загрозою. Для підвищення ефективності необхідні системні зміни: модернізація законодавства, посилення координації, збільшення фінансування, розвиток кадрового потенціалу, створення механізмів державно-приватного партнерства, підвищення кіберграмотності населення.

РОЗДІЛ 3. МЕХАНІЗМИ КООРДИНАЦІЇ ТА КОНТРОЛЮ У СИСТЕМІ ПУБЛІЧНОГО УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ

3.1. Проблеми та ризики в координаційних та контрольних механізмах

Ефективна координація є критичним фактором успіху системи кібербезпеки. Аналіз чинної системи виявляє множинність суб'єктів без чіткого розмежування повноважень – Закон визначає 14 суб'єктів, повноваження яких часто перетинаються. Кіберінцидент на об'єкті критичної інфраструктури може одночасно розслідуватися Кіберполіцією, СБУ, ДССЗЗІ, що призводить до розмивання відповідальності. Слабкість центрального координаційного механізму проявляється у обмежених важелях впливу РНБО. Рішення РНБО є обов'язковими після затвердження Указом Президента, проте механізми контролю виконання недостатні. Відсутність єдиного центру оперативної координації означає, що на відміну від країн-лідерів, в Україні немає структури, яка б координувала реагування на масштабні інциденти в режимі 24/7.

Надмірна секретність призводить до того, що відомства класифікують інформацію з різними грифами, СБУ та розвідувальні органи часто не діляться даними навіть з ДССЗЗІ та CERT-UA. Це призводить до ситуацій, коли різні відомства дізнаються про одну загрозу з різницею у тижні. Відсутність технічної платформи обміну означає, що в Україні немає загальнодержавної системи автоматизованого обміну індикаторами компрометації. CERT-UA створив платформу для добровільного обміну, проте вона охоплює лише частину суб'єктів. Різні організаційні культури військових, спецслужб, правоохоронців та цивільних відомств створюють бар'єри комунікації через відмінності у підходах до класифікації та обміну інформацією.

Відсутність єдиної системи моніторингу виконання означає, що рішення приймаються різними органами без централізованого моніторингу їх виконання. Формалізація звітності проявляється у тому, що звіти часто носять формальний характер, фокусуючись на кількісних показниках без оцінки реального

покращення захищеності. Недостатність зовнішнього контролю виявляється у обмеженому парламентському контролі – Комітет ВРУ розглядає питання кібербезпеки епізодично. Громадський контроль ускладнюється секретністю більшості інформації. Проблеми координації створюють конкретні ризики. Дублювання зусиль та марнування ресурсів – за оцінками експертів, до 20-30% ресурсів марнується через паралельне реагування різних відомств на одні інциденти. Запізніла реакція на загрози – час від виявлення масштабної загрози до координованої відповіді може сягати 24-48 годин, тоді як потрібні години або хвилини. Неповне розуміння ситуації – коли інформація розпорошена між відомствами, жоден актор не має повної картини. Конфлікти юрисдикції призводять до ситуацій, коли кілька відомств намагаються керувати реагуванням на один інцидент. Втрата довіри партнерів – неефективна координація підриває довіру приватного сектору та міжнародних партнерів.

Відсутність регіональних центрів координації означає, що на обласному рівні немає структур для координації дій різних суб'єктів. Територіальні підрозділи центральних органів підпорядковуються своїм центральним офісам, а не обласним державним адміністраціям. Обмежені повноваження місцевого самоврядування проявляються у тому, що органи місцевого самоврядування несуть відповідальність за захист своїх систем, проте не мають повноважень координувати дії на своїй території. Нерівномірність ресурсів створює "слабкі ланки" – ресурси концентруються у Києві та обласних центрах, більшість регіонів має обмежені можливості.

Повномасштабна війна створила додаткові виклики. Часткова евакуація структур з Києва та інших міст ускладнила фізичну координацію. Робота в розподіленому режимі вимагає надійних систем зв'язку, які не завжди доступні. Перевантаження через інтенсивність кібератак створює надмірне навантаження на всі структури, залишаючи мало часу для координації. Залучення волонтерів через «Армію кіберзахисту» виконує важливу роль, проте їх інтеграція у формальну систему координації залишається проблематичною.

3.2. Зарубіжний досвід: уроки для України

США розвинули складну систему координації у сфері кібербезпеки, яка відображає федеративний устрій країни та залучення великої кількості державних і приватних акторів. Ключовим механізмом оперативного реагування є Cyber Unified Coordination Group (UCG), створена відповідно до Президентської директиви PPD-41 у 2017 році. UCG активується у разі масштабних кіберінцидентів, що потребують міжвідомчої взаємодії та можуть впливати на національну безпеку чи економіку [42;50].

UCG об'єднує основні федеральні агенції з чітким функціональним розподілом: CISA відповідає за технічну допомогу та захист критичної інфраструктури, FBI — за кримінальні розслідування, NSA — за технічну атрибуцію атак і контррозвідку, ODNI — за інтеграцію розвідувальної інформації. Комунікація в межах групи здійснюється за принципом «єдиного федерального голосу», що забезпечує узгодженість публічних повідомлень. UCG проводить регулярні координаційні наради, організовує обмін інформацією в режимі реального часу, координує дії з приватним сектором через галузеві обмінні платформи, а також підтримує взаємодію з міжнародними партнерами. Доповненням до UCG є постійно діюча структура — National Cyber Investigative Joint Task Force (NCIJTF), створена у 2008 році. Вона координує розслідування між понад 30 федеральними відомствами, уникаючи дублювання зусиль, забезпечуючи аналітику тенденцій та міжнародну взаємодію в сфері кіберзлочинності [36].

Важливою складовою американської моделі є система галузевих центрів обміну інформацією (ISACs), які функціонують у 25 ключових секторах. Вони забезпечують горизонтальну координацію в межах галузей, сприяють оперативному обміну тактичною інформацією про загрози та розробці спільних захисних рішень. ISACs діють як приватні структури, що отримують дані від CISA та передають їх компаніям-членам. Американська модель поєднує структурну децентралізацію з високим рівнем координації. Як зазначає Б.

Шнайєр, множинність акторів сприяє оперативності реагування, а ефективні механізми взаємодії забезпечують цілісність дій у кризових ситуаціях [43]. Для України важливими є уроки США щодо функціонального розподілу ролей, створення постійної координаційної структури, інституціоналізації взаємодії з приватним сектором та досягнення балансу між автономією відомств і централізованою реакцією. Водночас, надмірна складність моделі США з понад 50 залученими структурами є малопридатною для українських умов, де доцільніша більш компактна й адаптивна система.

Великобританія обрала шлях централізації кіберекспертизи у єдиному органі, що суттєво відрізняється від американської децентралізованої моделі. Національний центр кібербезпеки (National Cyber Security Centre, NCSC), створений у жовтні 2016 року, об'єднав кіберможливості, що раніше були розпорошені між різними урядовими структурами. NCSC є частиною Government Communications Headquarters (GCHQ) – британського аналогу американського NSA, що забезпечує йому доступ до розвідувальних можливостей та експертизи.

National Cyber Security Centre об'єднує кіберекспертизу під одним дахом, виконуючи функції технічного органу (національний CERT), регулятора (встановлення стандартів), консультанта (допомога урядовим структурам та бізнесу), координатора (узгодження дій різних відомств). NCSC працює як єдина точка контакту для всіх питань кібербезпеки. Active Cyber Defence Programme забезпечує проактивний захист публічного сектору через автоматизовану систему виявлення загроз, блокування зловмисних ресурсів, програму takedown фішингових сайтів. Уроки для України включають ефективність моделі «єдиного вікна», цінність проактивного захисту на національному рівні, важливість поєднання регуляторних та сервісних функцій [39]. Кіберкомандування при Міністерстві оборони є центральним органом координації, що об'єднує військові, цивільні та громадські ресурси. Відповідає за стратегічне планування, координацію реагування на кризові ситуації, управління Лігою кіберзахисту (волонтерів). Система раннього попередження використовує AI для

автоматизованого моніторингу всієї критичної інфраструктури з централізованим центром реагування. Міжнародна інтеграція – Естонія глибоко інтегрована у систему НАТО, Кооперативний центр у Таллінні служить платформою для координації [38]. Уроки включають ефективність залучення громадських ресурсів у формальну систему, важливість автоматизації моніторингу, цінність міжнародної інтеграції [35].

Сінгапур представляє протилежний естонському підхід – модель жорсткої централізації влади та детального регуляторного контролю. Ця модель відображає загальну філософію управління Сінгапуру як держави з ефективною централізованою владою та високим рівнем контролю над ключовими секторами економіки. Агентство з кібербезпеки Сінгапуру (Cyber Security Agency of Singapore, CSA), створене у 2015 році безпосередньо під егідою Прем'єр-міністра, є єдиним органом з широкими повноваженнями у сфері кібербезпеки. На відміну від моделей з розподілом функцій між різними органами, CSA концентрує всі ключові функції. Як регулятор, CSA розробляє та встановлює обов'язкові вимоги до кібербезпеки для всіх секторів, видає ліцензії постачальникам послуг кібербезпеки, проводить інспекції та накладає санкції за порушення. Як координатор, CSA узгоджує дії різних секторів при реагуванні на інциденти, координує взаємодію з міжнародними партнерами, забезпечує обмін інформацією між стейкхолдерами. Як оператор національного CERT (SingCERT), CSA забезпечує цілодобове реагування на інциденти, надає технічну допомогу постраждалим організаціям, веде національну базу даних загроз. Як контролер, CSA здійснює перевірки дотримання вимог кібербезпеки, оцінює стан захищеності критичної інфраструктури, вимагає усунення виявлених недоліків [26].

Законодавчою основою є Акт про кібербезпеку (Cybersecurity Act) 2018 року, який надає CSA широкі повноваження. Акт визначає 11 секторів критичної інформаційної інфраструктури (CII): енергетика (електро- та газопостачання), водопостачання, банківський та фінансовий сектор, охорона здоров'я, транспорт (наземний, морський, авіаційний), урядові послуги, засоби масової інформації,

безпека та оборона. Власники систем CII зобов'язані зареєструвати свої системи в CSA протягом встановленого терміну, дотримуватися детальних стандартів безпеки (Cybersecurity Code of Practice for CII), проходити регулярні аудити безпеки (щонайменше раз на два роки), повідомляти CSA про всі кіберінциденти протягом 2 годин з моменту виявлення, виконувати директиви CSA щодо усунення вразливостей у встановлені терміни.

CSA має право видавати обов'язкові до виконання директиви, які можуть вимагати застосування конкретних технічних заходів захисту, заборони використання певних продуктів або постачальників, проведення позапланових аудитів або тестувань на проникнення, тимчасового відключення скомпрометованих систем. Невиконання вимог CSA карається значними штрафами (до 100,000 сінгапурських доларів) та кримінальною відповідальністю для відповідальних осіб. За даними CSA, у 2022-2023 роках було накладено санкції на 15 організацій за недотримання вимог, що створило серйозний стримуючий ефект для інших.

Централізована система реагування Сінгапуру забезпечує високий рівень контролю. Всі об'єкти CII зобов'язані підключити свої системи моніторингу до національної платформи, що управляється SingCERT [44]. Платформа збирає телеметрію з усіх підключених систем у реальному часі, використовує AI та машинне навчання для виявлення аномалій, автоматично ескалює підозрілу активність відповідним командам реагування. У критичних ситуаціях SingCERT має технічну можливість віддаленого блокування загроз на об'єктах CII без попереднього узгодження з їх власниками, що є безпрецедентним рівнем централізованого контролю [27].

Національна стратегія кібербезпеки Сінгапуру 2021 визначає чотири стратегічні пріоритети з відповідним фінансуванням понад 1 млрд сінгапурських доларів. [43].Побудова стійкої інфраструктури передбачає обов'язкові вимоги до всіх критичних систем, програму модернізації застарілих систем, резервування критичних компонентів. Створення безпечної кіберекосистеми включає програму SG Cyber Safe для підвищення кіберграмотності населення та бізнесу,

обов'язкові тренінги для посадових осіб, кампанії підвищення обізнаності. Розвиток динамічної кіберіндустрії забезпечується через залучення міжнародних компаній кібербезпеки до Сінгапуру, підтримку локальних стартапів через гранти та субсидії, створення Cybersecurity Centre of Excellence. Зміцнення міжнародного партнерства включає двосторонні угоди з провідними країнами, участь у регіональних ініціативах ASEAN, прийом міжнародних конференцій та форумів. Брюс Шнайєр, порівнюючи різні моделі, зазначає: "Сінгапурська модель демонструє, що жорстка централізація та детальний регуляторний контроль можуть бути ефективними у невеликій країні з сильною централізованою владою. Проте ця модель важко масштабується на великі країни і може стримувати інновації через надмірне регулювання [31].

Для України сінгапурський досвід має обмежену застосовність через фундаментальні відмінності у політичних системах та масштабах. Проте окремі елементи можуть бути корисними: ефективність централізованої моделі для забезпечення швидкості прийняття рішень, важливість чітких та обов'язкових вимог до критичної інфраструктури з реальними санкціями за недотримання, цінність автоматизованого моніторингу всіх об'єктів КІ через єдину платформу, необхідність систематичних програм підвищення кіберграмотності для різних аудиторій. Водночас, надмірна централізація влади та детальний контроль можуть бути неприйнятними для України та суперечити демократичним цінностям [37; 40; 47].

National Cyber Directorate координує цивільну сферу, IDF Cyber Division – військові аспекти. Існує тісна координація через обмін персоналом (офіцери переходять у NCD після служби), спільні навчання, єдину систему моніторингу, узгоджену доктрину. Приватний сектор є партнером – компанії отримують контракти на захист КІ, беруть участь у розробці рішень, мають доступ до класифікованої інформації через систему security clearance. Уроки включають можливість ефективної інтеграції військових та цивільних структур, цінність залучення приватного сектору як рівноправного партнера, ефективність "обертових дверей" між секторами [30].

Аналіз виявляє, що кожна модель має свої переваги та недоліки, які відображають національний контекст. Американська модель є найбільш ресурсомісткою та складною, ефективною для великої федеративної держави, проте може бути надмірно складною для України. Британська модель забезпечує оптимальний баланс між централізацією експертизи та гнучкістю, може служити основою для української моделі з урахуванням необхідності адаптації. Естонська модель є найбільш релевантною для України через схожість викликів (загроза з боку Росії, обмежені ресурси), демонструє можливість досягнення високої ефективності при обмежених ресурсах. Сінгапурська модель є найменш придатною для України через фундаментальні відмінності у політичних системах, проте окремі елементи (чіткі вимоги, ефективні санкції) можуть бути корисними. Ізраїльська модель пропонує цінні уроки щодо інтеграції військового та цивільного секторів, розвитку кіберіндустрії (таблиця 3.1).

Таблиця 3.1

Спільні елементи успішних моделей координації

Елемент	США	Великобританія	Естонія	Сінгапур	Ізраїль
Єдиний центр координації	UCG	NCSC	Кіберкомандування	CSA	NCD
Автоматизація обміну	AIS	CiSP	X-Road	Централізована	Єдина платформа
Чіткі ролі	Так	Так	Так	Так	Так
Регулярні навчання	Cyber Storm	Щоквартальні	Постійні	Щомісячні	Постійні
Участь бізнесу	ISACs	CiSP	Партнерство	Обов’язкова	Інтегрована
Міжнародна інтеграція	Five Eyes	Five Eyes	НАТО	ASEAN	Двостороння

Для України оптимальною була б гібридна модель, що поєднує: британський підхід до централізації експертизи у єдиному центрі компетенцій (на зразок NCSC); естонський досвід залучення громадських ресурсів та резервування даних за кордоном; ізраїльську модель інтеграції військових та цивільних можливостей, розвитку кіберіндустрії; американські механізми державно-приватного партнерства через галузеві центри обміну інформацією;

сінгапурські елементи чітких вимог до критичної інфраструктури з ефективними санкціями.

3.3. Пріоритетні заходи щодо покращення міжвідомчої координації

Створення Національного центру координації кібербезпеки (НЦКК) при РНБО з функціями стратегічної координації (розробка та моніторинг стратегічних документів), оперативної координації (цілодобова координація реагування на значні інциденти), управління обміном інформацією (національна платформа обміну), міжнародної співпраці (координація взаємодії з партнерами), аналітики (стратегічний аналіз загроз). НЦКК має бути укомплектований 50-70 фахівцями з конкурентними зарплатами, бюджет близько 200 млн грн щорічно.

Реформування CERT-UA передбачає розширення штату до 100-120 фахівців, створення регіональних відділень у 5-7 обласних центрах, надання повноважень видавати обов'язкові технічні директиви для КІ в кризових ситуаціях, інтеграцію з Національним центром координації. Створення Міжвідомчого координаційного комітету на рівні заступників керівників ключових відомств для щомісячних зустрічей, узгодження позицій, вирішення конфліктів юрисдикції, планування спільних заходів [2].

Національна платформа обміну інформацією (НПОІ) має базуватися на розподіленій архітектурі з вузлами у кожного суб'єкта, використовувати міжнародні протоколи (STIX/TAXII) для сумісності, забезпечувати диференційований доступ залежно від рівня довіри, автоматично поширювати IoC на захисні системи учасників, містити вбудовані інструменти аналізу та візуалізації. Орієнтовна вартість розробки 50 млн грн, експлуатації 15 млн грн щорічно. Система ситуаційного центру включає модернізацію Ситуаційного центру РНБО з великим екраном для відображення кіберситуації в реальному часі, інтеграцію з моніторинговими системами відомств, систему відеоконференц-зв'язку, захищені канали зв'язку. Мобільний додаток

координації для уповноважених осіб забезпечує миттєві повідомлення про критичні події, швидке скликання віртуальних нарад, обмін файлами, функцію «червоної кнопки» для екстрених ситуацій.

Протокол реагування на масштабні інциденти має визначати критерії класифікації інцидентів (5 рівнів від локального до національного), чітке розподілення ролей для кожного рівня, процедури ескалації та деескалації, терміни повідомлення та реагування, формати звітності, процедури залучення міжнародної допомоги. Система планування та звітності передбачає узгодження річних планів через НЦКК, квартальну звітність за єдиною формою, оприлюднення публічної частини звітів, аналіз виконання НЦКК з рекомендаціями. Регулярні міжвідомчі навчання включають щорічні масштабні кіберучення за участю всіх суб'єктів (за аналогією з Cyber Europe), квартальні настільні учення для відпрацювання координації, місячні тренінги для контактних осіб відомств [45;50].

Внесення змін до Закону про кібербезпеку з доповненням розділом про координацію, який чітко визначає повноваження Національного центру, обов'язки щодо обміну інформацією, відповідальність за невиконання рішень, процедури розв'язання конфліктів. Постанова КМУ про Національну платформу обміну інформацією встановлює правила участі, категорії інформації для обміну, гарантії конфіденційності, відповідальність за зловживання, технічні вимоги. Наказ про стандарти звітності встановлює єдині стандарти звітності про кіберінциденти для всіх суб'єктів.

Програма підготовки координаторів включає курс тривалістю 3 місяці для працівників відомств, технічні, правові, управлінські аспекти, міжнародні стажування, обов'язкову сертифікацію. Secondment програма передбачає обмін персоналом між відомствами на 6-12 місяців для отримання досвіду, формування міжособистісних зв'язків, збереження зарплати та гарантій. Створення комунікаційних мереж через професійну асоціацію фахівців державного сектору, щоквартальні форуми, онлайн-платформу, спільні дослідницькі проєкти.

Для подолання бар'єрів у комунікації між відомствами та формування міжособистісних зв'язків доцільно запровадити програму тимчасового обміну персоналом. Механізм програми включає відрядження фахівців з одного відомства до іншого на строк від 6 до 12 місяців, збереження зарплати та всіх соціальних гарантій за основним місцем роботи, додаткова компенсація приймаючою стороною (якщо необхідно), гарантія повернення на попередню посаду або еквівалентну після завершення. Цілі програми включають отримання досвіду роботи іншого відомства, розуміння його специфіки та обмежень; формування особистих зв'язків між фахівцями різних відомств для полегшення майбутньої координації; обмін кращими практиками та методологіями; виявлення можливостей для покращення міжвідомчої взаємодії.

Пріоритетні напрямки обміну: між CERT-UA та кіберпідрозділами СБУ/ЗСУ для обміну технічною експертизою; між НЦКК та відомствами для розуміння координаційних потреб; між українськими структурами та міжнародними партнерами (NCSC, CISA) для трансферу досвіду. Критерії відбору учасників включають досвід роботи у сфері кібербезпеки не менше 2 років, відповідний рівень допуску до секретної інформації, рекомендацію керівництва, успішне проходження співбесіди. Очікувані результати: щорічно 20-30 фахівців беруть участь у програмі обміну, формується мережа міжособистісних зв'язків між відомствами, покращується взаєморозуміння та координація, виявляються та усуваються організаційні бар'єри. Бюджет програми близько 15 млн грн щорічно (додаткові витрати на компенсації, логістику, адміністрування).

Для підтримки неформальної комунікації між фахівцями з кібербезпеки державного сектору доцільно створити професійну асоціацію. Мета асоціації полягає у сприянні професійному розвитку фахівців, обміну досвідом та кращими практиками, формуванні професійних стандартів, адвокації інтересів професійної спільноти. Діяльність асоціації включає щоквартальні професійні форуми (конференції, круглі столи) з обговоренням актуальних тем; онлайн-платформу для професійного спілкування (форум, чат, база знань); спільні

дослідницькі проєкти з актуальних питань кібербезпеки; публікацію професійного журналу або бюлетеня; організацію професійних конкурсів та нагородження кращих фахівців.

Членство в асоціації є добровільним та відкритим для всіх фахівців з кібербезпеки державного сектору. Асоціація функціонує на некомерційній основі з можливістю отримання грантів від міжнародних партнерів. Керівні органи обираються на загальних зборах членів терміном на 2 роки. Бюджет асоціації формується з членських внесків (символічних), грантів міжнародних партнерів, підтримки держави (субсидії на організацію форумів). Орієнтовний щорічний бюджет 5-7 млн грн забезпечить організацію 4 форумів, підтримку онлайн-платформи, публікацію матеріалів (таблиця 3.2).

Таблиця 3.2

Фінансові потреби реалізації заходів

Захід	Одноразово (млн грн)	Щорічно (млн грн)
Національний центр координації	100	200
Розширення CERT-UA	50	150
Національна платформа обміну	50	15
Модернізація Ситуаційного центру	80	20
Програми навчання та обміну	20	40
Кіберучення та тренінги	15	60
Інше	35	15
ЗАГАЛОМ	350	500

Реалізація нової системи координації кібербезпеки потребує поетапного підходу з чітким розмежуванням завдань, відповідальних структур, часових рамок та необхідного фінансування. Такий підхід забезпечує поступове нарощування спроможностей, зниження ризиків імплементації та можливість адаптації на основі результатів проміжних етапів. Нижче подано узагальнену таблицю 3.3 з графіком реалізації, ключовими заходами, очікуваними результатами та обсягами фінансування.

Таблиця 3.3

Етапи впровадження, терміни, заходи, бюджет і результати

Етап	Терміни	Ключові заходи	Бюджет (млн грн)	Очікувані результати
Підготовчий	Місяці 1–6	Розробка нормативної бази (зміни до Закону, постанова КМУ, стандарти звітності) Створення НЦКК (положення, персонал, технічне оснащення) Формування Міжвідомчого координаційного комітету Розробка протоколів реагування, технічних специфікацій НПОІ, навчальних програм	150	Запущено НЦКК Прийнято ключові нормативні акти Розроблено технічні та процедурні документи Оголошено набір координаторів
Розгортання	Місяці 7–18	Розробка та тестування НПОІ (пілот з 10–15 організаціями) Модернізація Ситуаційного центру Розробка мобільного додатку Розширення CERT-UA (найм, інфраструктура) Створення трьох регіональних відділень Підготовка координаторів, перші стажування Настільні та міжвідомчі навчання	300	НПОІ у тестовому режимі (30–50 учасників) Оновлений Ситуаційний центр Три регіональні відділення CERT-UA Підготовлена перша група координаторів Проведено перші міжвідомчі навчання
Функціонування	Місяці 19–36	Повноцінний запуск НПОІ (державний та приватний сектори) Впровадження мобільного додатку для всіх користувачів Відкриття ще трьох регіональних відділень CERT-UA Створення ISAC у пріоритетних секторах Масштабні навчання Оцінка ефективності та коригування системи	350	Повнофункціональна система координації Національне покриття CERT-UA Інтегрований приватний сектор Регулярні навчання всіх типів Система довела ефективність у кризових ситуаціях

Запропонований графік реалізації передбачає логічну послідовність дій: від створення інституційної та нормативної основи – до впровадження технологічних рішень, регіонального охоплення та повномасштабного функціонування. Такий підхід дозволяє забезпечити контроль за результатами на

кожному етапі, мінімізувати ризики провалу, а також адаптуватися до змін у безпековому середовищі. Передбачене фінансування у 800 млн грн на трирічний період є збалансованим і реалістичним у співвідношенні «вартість – результат», забезпечуючи сталу національну спроможність у сфері кіберкоординації.

Висновки до розділу 3

Аналіз системи координації у сфері кібербезпеки України виявив серйозні проблеми: дублювання функцій, слабку центральну координацію, запізнілу реакцію, інформаційну ізоляцію та брак контролю. Міжнародні моделі демонструють ефективність через наявність єдиного центру, автоматизований обмін, чіткий розподіл ролей і партнерство з приватним сектором. Для України пріоритетом є створення Національного центру координації при РНБО, посилення CERT-UA, запуск платформи обміну інформацією, модернізація Ситуаційного центру та міжвідомча інтеграція. Орієнтовні витрати — 350 млн грн одноразово та 500 млн грн щорічно. Впровадження протягом 3 років дозволить створити дієву систему, за умови політичної волі й підтримки всіх стейкхолдерів.

ВИСНОВКИ

Проведене дослідження дозволило всебічно розкрити механізми публічного управління у сфері кібербезпеки в Україні, виявити їх сильні та слабкі сторони, оцінити регіональний вимір, нормативно-правову базу, міжнародний досвід та міжвідомчу взаємодію. Встановлено, що сучасна кібербезпека вийшла за межі технічної проблематики і стала міждисциплінарним явищем, яке потребує інтегрованого управлінського підходу на основі багаторівневого та багатосекторального врядування. Теоретико-методологічні підходи до аналізу кібербезпеки демонструють перехід від технократичної до системної парадигми, що охоплює політичний, правовий, економічний і соціальний контексти.

У рамках дослідження регіонального виміру кібербезпеки на прикладі Вінницької області виявлено істотні розриви між рівнем цифровізації та розвитком інституційної спроможності. Відсутність спеціалізованих структур, обмежене фінансування, недосконалий моніторинг та слабка регіональна координація свідчать про потребу у формуванні нових інструментів регіонального управління кібербезпекою. Аналіз міжнародних моделей (Естонії, Великобританії, Ізраїлю, США, Сінгапуру) підтвердив ефективність централізованої або чітко координованої архітектури з автоматизованими механізмами обміну інформацією, формалізованими процедурами взаємодії та високим рівнем залучення приватного сектору. Ці підходи можуть бути адаптовані до українських реалій у формі комбінованої моделі, що враховує наявні ресурси, загрози та інституційні обмеження.

Нормативно-правова база України має фундамент, але залишається фрагментарною, частково застарілою, з низьким рівнем гармонізації з європейськими директивами (зокрема NIS2, GDPR) та відсутністю дієвих механізмів контролю й санкцій. Оцінка правового забезпечення на рівні 5,7/10 вказує на необхідність системного оновлення законодавства з урахуванням міжнародних стандартів. Організаційна структура управління кібербезпекою

включає велику кількість суб’єктів із розмитими повноваженнями та слабкою координацією, що призводить до дублювання зусиль, неефективного використання ресурсів і повільного реагування на інциденти. Найгостріші проблеми — нестача кадрів, обмежене фінансування (лише 0,15% держбюджету) та слабкий рівень цифрової грамотності населення. Інтегральна оцінка ефективності моделі управління (5,29/10) підтверджує середній рівень розвитку, з найбільшими проблемами в організаційному та кадровому вимірах.

Особливої уваги потребує сфера міжвідомчої координації. Система координації кібербезпеки в Україні є надмірно фрагментованою, без єдиного центру оперативного управління, технічної платформи для обміну інформацією та чітких регламентів взаємодії. Міжнародний досвід демонструє, що саме централізовані або синхронізовані моделі координації дозволяють досягати найкращих результатів. В Україні ж, через організаційні дисбаланси та відсутність чіткої відповідальності, до 30% ресурсів витрачається неефективно, а реакція на загрози може затримуватись на 24–48 годин. Наукова новизна роботи полягає у розробці системи критеріїв оцінки ефективності моделі управління кібербезпекою з урахуванням гібридного характеру загроз, аналізі регіонального виміру на прикладі конкретного регіону (Вінницької області) та формуванні адаптованої до українських умов моделі вдосконалення міжвідомчої координації на основі кращих міжнародних практик.

Практична значущість дослідження полягає в тому, що запропоновані інституційні, правові, технологічні, організаційні та освітні рекомендації є конкретними, реалістичними й фінансово обґрунтованими (350 млн грн одноразово та 500 млн грн щорічно — 0,03% бюджету). Їх впровадження протягом 3 років дозволить суттєво зміцнити національну кібербезпеку навіть за умов війни та обмежених ресурсів. Результати відповідають меті дослідження та можуть лягти в основу державної політики, регіональних стратегій і загального підвищення кіберстійкості України.

СПИСОК ДЖЕРЕЛ І ЛІТЕРАТУРИ

1. Боярчук Р. М., Савченко В. А., Мацько О. Й., Новікова І. В. Модель трансформації національної системи кібербезпеки в умовах дії гібридних загроз. *Сучасний захист інформації*. 2020. № (1). С. 6-10.

2. Вівчар І., Постельжук О., Валюх Л. Кібербезпека як сфера міжнародного співробітництва у період глобальної кризи безпеки. "Вісник НЮУ імені Ярослава Мудрого". *Серія: Філософія, філософія права, політологія, соціологія*, 2025. № 2(65).

3. Горбулін В. П. Кібербезпека в Україні: глобальні тенденції та національні виклики. *Стратегічна панорама*. 2016. № 2. С. 7-18.

4. Грищенко С. М. Правове регулювання кібербезпеки в умовах цифрової трансформації суспільства // *Інформація і право*. — 2025. — № 2 (53). — С. 45–52.

5. Даник Ю. Г. Система забезпечення кібербезпеки України: концептуальні засади. *Інформація і право*. 2018. № 3(26). С. 82-94.

6. Довгань О. Д. Державна політика у сфері кібербезпеки: теорія і практика. *Аспекти публічного управління*. 2019. Т. 7. № 4. С. 25-36.

7. Іщенко К. Ф. Роль публічного управління у формуванні національної кібербезпеки: механізми координації та контролю // *Вісник студентського наукового товариства Донецького національного університету імені Василя Стуса*. — Вінниця: ДонНУ імені Василя Стуса, 2025. — Вип. 17, т. 1. — С. 69.

8. Закон України «Про основні засади забезпечення кібербезпеки України». URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 15.10.2025).

9. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». URL: https://zakon.rada.gov.ua/go/80/94-%D0%B2%D1%80/ed20140302 (дата звернення 15.10.2025).

10. Кібератаки в Україні за 2023 рік. URL: https://am-bits.com/uk/novosti-i-stati/kiberataky-v-ukrayini-za-2023-rik/ (дата звернення 15.10.2025).

11. Ліпкан В., Діордіца І. Національна система кібербезпеки як складова частина системи забезпечення національної безпеки України. *Підприємництво, господарство і право.* 2017. №(5). С. 174-180.

12. Лучик С.Д., Лучик В.Є. Кібербезпека в умовах війни: соціальні аспекти. Наука і техніка сьогодні. 2024. № 7(35). С. 857-870.

13. Мануілов Я. Європейський досвід забезпечення кібербезпеки. *Інформація і право. 2025 №(2 (53)).* С. 147-154.

14. Наказ ДССЗЗІ «Про затвердження Порядку інформування про кіберінциденти» від 22 лютого 2019. URL: https://cip.gov.ua/ua/filter?tagId=49656 (дата звернення 15.10.2025).

15. Постанова КМУ «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» від 19 червня 2019 року №518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text (дата звернення 15.10.2025).

16. Петров В. В. Правове забезпечення кібербезпеки в Україні: стан та перспективи. *Право і безпека*. 2017. № 4 (67). С. 100–107.

17. Поляков О. М. Активізація міжнародної співпраці у сфері забезпечення кібербезпеки: шляхи удосконалення в реаліях сьогодення. *Інформація і право. 2021. №(2).* С. 129-138.

18. Федієнко О. П. Міжнародні стандарти оцінки кіберстійкості. Інформація і право.2024. № 3 (50).С. 124-135.

19. У застосунку «Армія+» стартував курс з кібербезпеки. URL: https://www.ukrinform.ua/rubric-society/3943259-u-zastosunku-armia-startuvav-kurs-z-kiberbezpeki.html (дата звернення 15.10.2025).

20. Урядова команда CERT-UA в 2023 році опрацювала 2543 кіберінциденти. URL: https://cip.gov.ua/ua/news/uryadova-komanda-cert-ua-v-2023-roci-opracyuvala-2543-kiberincidenti (дата звернення 15.10.2025).

21. Шульга В. П., Іванченко Є. В., Вишневська Н. С. Дослідження методів та моделей оцінювання кіберзахисту критичної інфраструктури держави. *Сучасний захист інформації*. 2024. №(3).С. 6-19.

22. Bondarenko, S., Nagornyak, T., Polovyi, M. Modern information models of the national interests' protection policy of the world countries. *European journal of transformation studies*. 2018. Vol. 6, Iss. 2.44-54.

23. Bondarenko S., Nagornyak T., Polovyi M. Institutional mechanisms to ensure national security in the information space of the United States, the United Kingdom and the Russian Federation. *Przegląd Strategiczny* 2020, Issue 13, P. 265-279. DOI : 10.14746/ps.2020.1.16

24. Deibert R. J. Black Code: Surveillance, Privacy, and the Dark Side of the Internet. Toronto: McClelland & Stewart. 2013. 320 p.

25. Dunayev I., Lugovenko N. The State and Personal Data in the Post-GDPR World: Towards a Global Consensus or Regulatory Fragmentation?. *Theory and Practice of Public Administration,* 2024. № 2(79). С. 28-62.

26. Cyber Security Agency of Singapore. URL: https://www.csa.gov.sg/ (дата звернення 15.10.2025).

27. Jiow H. J. Efforts to Get People Involved in Cyber-Physical Security: Case Studies of Australia and Singapore. In*: Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level*, 2016. P. 221-232.

28. Libicki M. C. Cyberdeterrence and Cyberwar. Santa Monica: RAND Corporation, 2009. 240 p.

29. Libicki M. C. Cyberspace in Peace and War. Annapolis: Naval Institute Press, 2016. 456 p..

30. Miller J., Butler R. Making the National Cyber Director Operational With a National Cyber Defense Center. Lawfare. 2023.

31. Moskal E. J. A model for establishing a cybersecurity center of excellence. *Information systems education journal*, 2015. №13(6). P. 97-108.

32. Nye J. S. Nuclear Lessons for Cyber Security? *Strategic Studies Quarterly*. 2011. Vol. 5, No. 4. P. 18-38.

33. Nye J. S. The Regime Complex for Managing Global Cyber Activities. *Global Commission on Internet Governance Paper Series*. 2014. No. 1. – P. 1-20.

34. Schneier B. The Security Implications of the EU's NIS2 Directive. *IEEE Security & Privacy*. 2023. Vol. 21. No. 2. P. 88-91.

35. The National Cyber Security Centre. URL: https://www.ncsc.gov.uk/ (дата звернення 15.10.2025).

36. The National Security Strategy of the United States of America. Washington, 2006. 54 p.

37. Clarke R. A., Knake R. K. Cyber War: The Next Threat to National Security and What to Do About It. New York: Ecco. 2010. 290 p.

38. Healey J. (ed.). A Fierce Domain: Conflict in Cyberspace, 1986–2012. Washington, DC: Cyber Conflict Studies Association, 2013. 347 p.

39. Rid T. Cyber War Will Not Take Place. Oxford: Oxford University Press, 2013. 218 p.

40. Singer P. W., Friedman A. Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford: Oxford University Press. 2014. 320 p.

41. Zetter K. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. New York: Crown, 2014. 448 p.

42. United States Government Accountability Office. Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electricity Grid. GAO-19-332, 2019.

43. World Economic Forum. Global Cybersecurity Outlook 2024. Geneva: WEF, 2024.

44. ETSI. Cyber Security Threats and Solutions for Critical Infrastructure. ETSI TR 103 445 V2.1.1, 2022.

45. Kello L. The Virtual Weapon and International Order. New Haven: Yale University Press, 2017. 337 p.

46. Dragos Inc. Industrial Cybersecurity Year in Review 2023. Dragos Report, 2024.

47. Shackelford S. Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace. Cambridge University Press, 2014. 448 p.

48. Slay J., Miller M. Cybersecurity for Industrial Control Systems. CRC Press, 2017. 340 p.

49. Baezner M., Robin P. Cyber Conflicts in 2022: Trends and Analysis. Center for Security Studies, ETH Zurich, 2023.

50. Department of Homeland Security. Cybersecurity Strategy. Washington, DC: DHS, 2018.