МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “ МЕХАНІЗМИ ПРОТИДІЇ КІБЕРТЕРОРИЗМУ ЯК СКЛАДОВА СИСТЕМИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ ”

на здобуття освітнього ступеня магістра
зі спеціальності 125 Кібербезпека та захист інформації
освітньо-професійної програми Управління інформаційною та кібернетичною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ *Владислав* СКОЛОТА

(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБДМ-61
Владислав СКОЛОТА

Керівник:
к.т.н., доцент Юрій ЩАВІНСЬКИЙ

Рецензент:
к.т.н., доцент Юрій ПЕПА

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра Управління кібербезпекою та захистом інформації

Ступінь вищої освіти магістр

Спеціальність 125 Кібербезпека та захист інформації

Освітньо-професійна програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ

Завідувач кафедрою УКБЗІ
_____ Світлана ЛЕГОМІНОВА
"____"_____2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Сколоті Владиславу

1. Тема кваліфікаційної роботи: «Механізми протидії кібертероризму як складова система національної безпеки України»

керівник кваліфікаційної роботи Юрій ЩАВІНСЬКИЙ, к.т.н., доцент
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від "30" жовтня 2025 р. № 467.

2. Строк подання кваліфікаційної роботи "11" грудня 2025 р.

3. Вихідні дані до кваліфікаційної роботи: *нормативно-правові акти України та міжнародні стандарти у сфері кібербезпеки, аналітичні звіти профільних органів, наукова та технічна література.*

4. Перелік питань, які потрібно розробити:

1. Проаналізувати сутність і форми кібертероризму, його місце у системі національної безпеки та вплив на критичну інформаційну інфраструктуру України.
2. Дослідити сучасний стан кібертерористичних загроз і механізмів протидії в Україні та за кордоном, зокрема структуру загроз для об'єктів критичної інфраструктури та практики їх класифікації..
3. Визначити та обґрунтувати комплексні технічні, організаційні й правові механізми протидії кібертероризму та напрями підвищення ефективності захисту критичної інформаційної інфраструктури України.

5. Перелік ілюстративного матеріалу: *презентація*

6. Дата видачі завдання "02" жовтня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення об’єкта, предмета, мети та завдань дослідження	10.10.2025	
2.	Збір та аналіз наукових джерел, нормативно-правових актів і стандартів у сфері кібербезпеки та протидії кібертероризму	23.10.2025	
3.	Аналіз сутності кібертероризму, його форм та місця в системі національної безпеки України	27.10.2025	
4.	Дослідження сучасного стану кібертерористичних загроз і механізмів протидії в Україні та за кордоном, узагальнення результатів анкетування й контент-аналізу	10.11.2025	
5.	Розроблення моделі комплексних механізмів протидії кібертероризму та практичних рекомендацій щодо захисту критичної інформаційної інфраструктури	15.11.2025	
6.	Формулювання висновків за результатами проведеного дослідження	22.11.2025	
7.	Оформлення кваліфікаційної роботи	04.12.2025	
8.	Підготовка та оформлення презентації до захисту	14.12.2025	
9.	Отримання рецензії на роботу	18.12.2025	
10.	Захист кваліфікаційної роботи в ЕК	__.01.2026	

Здобувачка вищої освіти _____ Владислав СКОЛОТА_
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Юрій ЩАВІНСЬКИЙ_
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Сколоті В.В. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека та захист інформації
(код, найменування спеціальності)
Освітньо-професійної програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Механізми протидії кібертероризму як складова система національної безпеки України "
Кваліфікаційна робота і рецензія додаються.

Директор ННІКБЗІ _____ Євгенія ІВАНЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач **СКОЛОТА Владислав** у кваліфікаційній роботі проаналізував сутність і форми кібертероризму, його місце у системі національної безпеки та вплив на критичну інформаційну інфраструктуру України, дослідив сучасний стан кібертерористичних загроз і механізмів протидії в Україні та за кордоном, зокрема структуру загроз для об'єктів критичної інфраструктури та практики їх класифікації, визначив та обґрунтував комплексні технічні, організаційні й правові механізми протидії кібертероризму та напрями підвищення ефективності захисту критичної інформаційної інфраструктури України.

СКОЛОТА Владислав показав високу теоретичну і практичну підготовку, володіння науково-дослідницькими методами, вміння самостійно знаходити шляхи вирішення проблеми дослідження. Результати дослідження апробовані на конференції "Стратегії кіберстійкості: управління ризиками та безперервність бізнесу" 27 лютого 2025 року.

Все це дозволяє оцінити кваліфікаційну роботу здобувача **СКОЛОТИ Владислава** на оцінку "відмінно" та присвоїти йому кваліфікацію "Магістр з кібербезпеки та захисту інформації за освітньо-професійною програмою Управління інформаційною та кібернетичною безпекою".

Керівник кваліфікаційної роботи _____ Юрій ЩАВІНСЬКИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____"_____2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Сколота В.В. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедрою
Управління кібербезпекою та захистом
інформації _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну магістерську роботу

здобувача вищої освіти Сколоти Владислава Вікторовича
на тему “ Механізми протидії кібертероризму як складова система національної безпеки України ”

Актуальність Цілеспрямовані кібератаки на державні інформаційні ресурси, об’єкти критичної інфраструктури та системи управління можуть призводити до масштабних соціально-економічних наслідків і дестабілізації функціонування держави. У зв’язку з цим актуальним є дослідження та вдосконалення механізмів протидії кібертероризму як складової системи національної безпеки України з урахуванням сучасних технологічних, організаційно-правових та інформаційних аспектів.

Позитивні сторони

Автор здійснив ґрунтовний аналіз сутності та форм кібертероризму, його місця у системі національної безпеки та впливу на об’єкти критичної інформаційної інфраструктури України, що забезпечило цілісне розуміння досліджуваної проблематики.

У роботі детально досліджено сучасний стан кібертерористичних загроз, зокрема структуру загроз для об’єктів критичної інфраструктури, а також проаналізовано існуючі підходи до їх класифікації та оцінювання.

Значною перевагою роботи є зіставлення українських та зарубіжних практик протидії кібертероризму, що дозволило визначити сильні сторони та проблемні аспекти національної системи кібербезпеки.

Недоліки

1. Доцільно також окремо дослідити координацію дій між державними органами, військовими структурами, приватним сектором та операторами критичної інфраструктури у процесі запобігання та реагування на кібертерористичні загрози.

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує позитивної оцінки, а здобувач Сколота Владислав Вікторович заслуговує присвоєння кваліфікації “Магістр кібербезпеки за освітньо-професійною програмою “Управління інформаційною безпекою”.

Рецензент: доцент кафедри
Технічних систем кіберзахисту

к.т.н, доцент _____ Юрій ПЕПА

підпис

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 89 стор., 6 рис., 31 табл., 67 джерел.

Метою роботи є розроблення комплексних механізмів протидії кібертероризму для забезпечення національної безпеки України, які включають взаємопов'язані технічні, організаційні та правові заходи.

Об'єктом дослідження є процеси забезпечення захисту критичної інформаційної інфраструктури України від кібертерористичних загроз.

Предметом дослідження виступають механізми, методи та моделі протидії кібертероризму як складова системи національної безпеки, що поєднує державні інституції, операторів критичної інфраструктури та спеціалізовані структури кіберзахисту.

Методи дослідження. У роботі використано аналіз і синтез наукових джерел та нормативних актів, порівняльний аналіз моделей протидії кібертероризму, аналіз кейсів атак, опитування експертів, контент-аналіз внутрішніх політик, моделювання, методи оцінювання ризиків і візуалізацію результатів у вигляді схем, діаграм і карт ризиків.

Короткий зміст роботи. Як результат у роботі уточнено сутність кібертероризму, його місце в системі національної безпеки та підходи до класифікації загроз; проаналізовано сучасні технічні, організаційні, правові та етичні механізми протидії кібертероризму в Україні та за кордоном, результати анкетування експертів і контент-аналізу внутрішніх політик захисту критичної інфраструктури; розроблено модель комплексної системи протидії кібертероризму, запропоновано етапи її впровадження, ресурсні параметри та проведено апробацію на умовному кейсі оператора енергетичної мережі.

Галузь застосування. Результати роботи можуть бути використані органами державної влади, профільними регуляторами та операторами об'єктів критичної інфраструктури під час формування політики кібербезпеки, розроблення стратегій, програм і регламентів захисту від кібертерористичних загроз.

КЛЮЧОВІ СЛОВА: КІБЕРТЕРОРИЗМ, КІБЕРБЕЗПЕКА, КРИТИЧНА ІНФОРМАЦІЙНА ІНФРАСТРУКТУРА, НАЦІОНАЛЬНА БЕЗПЕКА, МЕХАНІЗМИ ПРОТИДІЇ.

ABSTRACT

Text part of the master's qualification thesis: 89 pages, 6 figures, 31 tables, 67 references.

The purpose of the thesis is to develop comprehensive mechanisms for countering cyberterrorism to ensure the national security of Ukraine, which include interrelated technical, organizational, and legal measures.

The object of the study is the processes of ensuring the protection of the critical information infrastructure of Ukraine against cyberterrorist threats.

The subject of the study comprises mechanisms, methods, and models for countering cyberterrorism as a component of the national security system, integrating state institutions, operators of critical infrastructure, and specialized cyber protection structures.

Research methods. The study employs analysis and synthesis of scientific sources and regulatory acts, comparative analysis of cyberterrorism countermeasures models, case analysis of cyber attacks, expert surveys, content analysis of internal security policies, modeling, risk assessment methods, and visualization of results in the form of schemes, diagrams, and risk maps.

Brief content of the thesis. As a result, the research уточнено the essence of cyberterrorism, its place within the national security system, and approaches to threat classification; analyzed contemporary technical, organizational, legal, and ethical mechanisms for countering cyberterrorism in Ukraine and abroad, including expert survey results and content analysis of internal policies for protecting critical infrastructure; developed a model of a comprehensive cyberterrorism counteraction system, proposed stages of its implementation and resource parameters, and conducted its testing using a conditional case of an energy network operator.

Field of application. The results of the thesis may be applied by public authorities, sectoral regulators, and operators of critical infrastructure facilities in forming cybersecurity policy and developing strategies, programs, and regulations for protection against cyberterrorist threats.

KEYWORDS: CYBERTERRORISM, CYBERSECURITY, CRITICAL INFORMATION INFRASTRUCTURE, NATIONAL SECURITY, COUNTERMEASURE MECHANISMS.

ЗМІСТ

ВСТУП

Актуальність теми. Механізми протидії кібертероризму формують один з ключових напрямів сучасної системи національної безпеки України, оскільки кібертерористичні впливи безпосередньо загрожують критичній інформаційній інфраструктурі, енергетиці, транспортним і фінансовим системам, органам державного управління та життєзабезпеченню населення. Повномасштабна збройна агресія проти України супроводжується інтенсивними кібератаками, комбінованими з інформаційно-психологічними операціями, що різко підвищує вимоги до стійкості національних інституцій, безперервності функціонування критичної інфраструктури та узгодженості технічних, організаційних і правових заходів кіберзахисту. Це обумовлює потребу у поглибленому дослідженні механізмів протидії кібертероризму саме як складової інтегрованої системи національної безпеки України, а не лише як сукупності окремих технічних рішень.

У наукових працях останніх років сформовано ключові теоретичні та прикладні підходи до аналізу кіберзагроз і кібертероризму. Левченко О. В. та Охрімчук В. В. висвітлюють антиукраїнський інформаційний і кібернетичний вплив як інструмент дестабілізації та підриву довіри до держави [1], Мельник Д. С. уточнює зміст, форми кібертероризму і напрями протидії на рівні державної політики [5], а Мазур Я. П. пов’язує основні кіберзагрози з воєнно-політичними цілями противника [6]. Галушко П. П. розкриває соціально-правову природу кіберзлочинності [7], Богдан Б. В. деталізує статус критичної інформаційної інфраструктури як об’єкта кібербезпеки [11], а Зінченко О. І. досліджує політичні аспекти розвитку кібертероризму в сучасному міжнародному порядку [17]. Комплексні механізми протидії кібертероризму, інтегровані в систему національної безпеки України та орієнтовані на захист критичної інформаційної інфраструктури в умовах війни, залишаються розробленими неповною мірою і потребують подальшого наукового опрацювання.

Метою дослідження є розроблення комплексних механізмів протидії кібертероризму для забезпечення національної безпеки України, які включають взаємопов'язані технічні, організаційні та правові заходи.

Для досягнення мети необхідно виконати наступні завдання*:*

– охарактеризувати поняття кібертероризму та його вплив на національну безпеку;

– розглянути класифікацію кібертерористичних загроз та атак;

– дослідити міжнародні стандарти та нормативно-правову базу щодо протидії кібертероризму (NIST, ENISA, законодавство України);

– розглянути роль державних та приватних структур у системі протидії кібертероризму;

– проаналізувати технічні методи захисту критичної інфраструктури (IDS/IPS, SIEM, SOC, AI/ML);

– встановити організаційні та адміністративні заходи протидії кібертероризму;

– сформувати правові та етичні аспекти забезпечення національної безпеки в кіберсфері;

– провести порівняльний аналіз ефективності існуючих підходів та технологій;

– обґрунтувати постановку завдань та принципи системного підходу до протидії кібертероризму;

– сформувати модель комплексної системи захисту критичної інфраструктури від кібертерористичних загроз;

– розробити рекомендації щодо впровадження механізмів протидії на практиці;

– дослідити апробацію моделі на умовному або реальному кейсі.

Об'єктом дослідження є процеси забезпечення захисту критичної інформаційної інфраструктури України від кібертерористичних загроз.

Предметом дослідження виступають механізми, методи та моделі протидії кібертероризму як складова системи національної безпеки, що поєднує державні інституції, операторів критичної інфраструктури та спеціалізовані структури кіберзахисту.

Методологічну основу роботи становить поєднання теоретичних, емпіричних, прикладних і візуалізаційних методів. Теоретичні методи охоплюють аналіз і синтез наукових джерел та нормативних актів, порівняння підходів до протидії кібертероризму, систематизацію і класифікацію кіберзагроз і заходів захисту. Емпіричні методи включають аналіз кейсів атак, опитування та інтерв'ю експертів, контент-аналіз політик захисту критичної інфраструктури. Прикладні та візуалізаційні методи передбачають моделювання механізмів протидії, оцінку ризиків, діаграми, карти ризиків і структурно-функціональні моделі.

Наукова новизна одержаних результатів полягає у розробленні системної моделі комплексних механізмів протидії кібертероризму, що інтегрує технічні, організаційні та правові заходи в багаторівневу систему національної безпеки. Удосконалено підходи до оцінювання ризиків і пріоритизації заходів кіберзахисту через поєднання кількісних індикаторів, інтегральних показників ризику та сценарного аналізу впливу атак на стійкість критичної інформаційної інфраструктури в умовах війни.

Практичне значення одержаних результатів полягає у можливості застосування запропонованих механізмів, моделей і рекомендацій органами державної влади, регуляторами та операторами критичної інфраструктури під час розроблення стратегій кібербезпеки, внутрішніх політик, регламентів реагування і планів безперервності діяльності. Розроблена модель може бути основою галузевих методичних документів, програм підготовки фахівців і алгоритмів оцінки ризиків та пріоритизації інвестицій, що сприяє підвищенню стійкості національної системи безпеки України до кібертерористичних загроз.

Апробація результатів. Сколота В. В. Гейміфікація навчальних програм з виявлення фішингових загроз: матеріали Всеукраїнської науково-практичної конференції / В. В. Сколота; Міністерство освіти і науки України, Державний університет інформаційно-комунікаційних технологій, Кафедра управління кібербезпекою та захистом інформації**;** Стратегії кіберстійкості: управління ризиками та безперервність бізнесу. – Київ, 27 лют. 2025. – С. 268-271.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСНОВИ ПРОТИДІЇ КІБЕРТЕРОРИЗМУ

1.1 Поняття кібертероризму та його вплив на національну безпеку

Кібертероризм сформувався як одна з ключових загроз національній безпеці в умовах гібридних війн, де поєднуються воєнні, інформаційні, економічні та політичні інструменти тиску. Для України, яка перебуває в умовах тривалої збройної агресії, кібертерористичні дії доповнюють інформаційно-психологічні операції, спрямовані на дестабілізацію суспільства, підрив довіри до органів влади та створення панічних настроїв. Наукові дослідження фіксують зростання спектра кіберзагроз, що охоплюють втручання в роботу державних інформаційних систем, енергетичної, транспортної, фінансової інфраструктури, а також використання кібератак як інструменту політичного тиску [1, 2].

У сучасних підходах до забезпечення національної безпеки кібертероризм розглядають як перетин інформаційної, воєнної, економічної, енергетичної та техногенної безпеки. Нормативно-правові акти України визначають кібертероризм як сукупність протиправних діянь із використанням комп'ютерних і телекомунікаційних технологій, що створюють загрозу життю і здоров'ю людей, стійкості функціонування критичної інфраструктури, обороноздатності держави, провокують надзвичайні ситуації та конфлікти з метою досягнення злочинних або політичних цілей [2, 3].

Стратегія кібербезпеки України закріплює кібертероризм у переліку пріоритетних загроз і підкреслює системний зв'язок між захищеністю державних інформаційних ресурсів, стійкістю сектору безпеки й оборони та загальним рівнем національної безпеки [4].

Сучасні дослідження кібертероризму формуються на перетині кримінального права, кримінології, безпекознавства та теорії міжнародної безпеки. Юридична школа, представлена, передусім, Д. С. Мельником, розглядає

кібертероризм як форму терористичної діяльності у цифровому середовищі, що поєднує ознаки тероризму і кіберзагроз та спрямована на дестабілізацію публічної влади, залякування населення і вплив на прийняття політичних рішень [5]. Підхід Я. П. Мазура акцентує на тому, що кібертероризм є одним із ключових видів кіберзагроз поряд з кіберзлочинністю, кібершпигунством і кібервійною, але виділяється саме політично мотивованим характером і орієнтацією на життєво важливі національні інтереси [6].

Кримінологічна школа, яку представляє П. П. Галушко, трактує кібертероризм у межах ширшого феномену кіберзлочинності, але наголошує, що терористична мета і створення стану масового страху в суспільстві відмежовують його від типових корисливих кіберзлочинів [7]. Частина авторів у сфері публічного управління та права кібербезпеки (В. В. Топчій, О. М. Бодунова) підкреслює, що кібертероризм слід розглядати не лише як окремий вид протиправної діяльності, а як системний фактор, який впливає на політику держави у сфері кібербезпеки, побудову національної системи реагування і взаємодію з міжнародними партнерами [8].

Відмежування кібертероризму від кіберзлочинності ґрунтується насамперед на мотивації, характері цілей і масштабі наслідків. Кіберзлочинність, за підходом П. П. Галушка, переважно має корисливий характер, орієнтована на отримання економічної вигоди або незаконний доступ до інформації, а обрані об’єкти не завжди мають стратегічне значення для держави [7]. Кібертероризм, навпаки, спрямований на завдання шкоди критичній інфраструктурі, органам влади чи об’єктам, які забезпечують життєдіяльність суспільства, а кінцевою метою є політичний вплив, дестабілізація або примушення держави до певних дій.

Кіберрозвідка, яку в літературі пов’язують із інтересами державних структур або спеціальних служб, спрямована на приховане збирання інформації, моделювання поведінки противника і підтримку прийняття рішень у сфері безпеки [6]. Вона може використовувати схожі технічні інструменти (спеціалізоване програмне забезпечення, експлойти, соціальну інженерію), проте

не має прямої мети залякування населення чи створення масштабних руйнівних наслідків, а її результати, як правило, залишаються латентними. Саме відсутність терористичної мети і демонстративного характеру дій є ключовою ознакою, що відмежовує кіберрозвідку від кібертероризму.

Відмежування кібертероризму від інформаційних операцій і кібервоєнних дій пов'язане з правовим статусом суб'єктів, режимом конфлікту та масштабом застосування сили. Д. С. Мельник зазначає, що інформаційні операції і кібератаки у ході збройного конфлікту здійснюються, як правило, державою або від її імені, мають воєнно-політичний характер і регулюються нормами міжнародного гуманітарного права [5]. Кібертероризм може здійснюватися як транснаціональними терористичними організаціями, так і малими групами чи окремими особами, формально не пов'язаними з державою, а сфера його дії не завжди обмежена періодом відкритого збройного конфлікту.

На основі критичного аналізу зазначених підходів кібертероризм можна узагальнено визначити як умисну, політично чи ідеологічно вмотивовану діяльність з використанням інформаційно-комунікаційних технологій, комп'ютерних систем і мереж, спрямовану на здійснення або підтримку терористичних актів, порушення функціонування критичної інфраструктури, створення стану страху і дестабілізації суспільства чи вплив на рішення органів публічної влади.

Таке визначення поєднує правові, кримінологічні та безпекові аспекти поняття, відображає центральну роль політичної мети, публічного резонансу та спрямованості на життєво важливі інтереси держави.

Для більш чіткого розмежування поняття кібертероризму від суміжних категорій доцільно зіставити його з кіберзлочинністю та кібервоєнними діями за ключовими критеріями. Порівняльний аналіз дає змогу показати відмінності у мотивації суб'єктів, характері об'єктів посягання, масштабі наслідків і правовому статусі дій, що є важливим для побудови системи криміналізації та протидії (табл. 1.1).

Таблиця 1.1

Порівняльна характеристика кібертероризму, кіберзлочинності та кібервоєнних дій

Критерій порівняння	Кібертероризм	Кіберзлочинність	Кібервоєнні дії
Основна мета	Політичний або ідеологічний вплив, дестабілізація, залякування населення	Отримання економічної вигоди, незаконний доступ до інформації	Досягнення воєнно-політичних цілей у збройному конфлікті
Типові об'єкти посягання	Критична інфраструктура, органи влади, системи життєзабезпечення	Банківські системи, комерційні ресурси, персональні дані	Військова інфраструктура, урядові мережі, комунікаційні та енергетичні системи
Характер суб'єктів	Терористичні організації, екстремістські групи, радикалізовані індивіди	Окремі злочинці, організовані кримінальні групи	Держава, її збройні сили, уповноважені структури, інколи проксі-формації
Правовий режим кваліфікації	Терористичні злочини з використанням комп'ютерних технологій	Злочини у сфері використання комп'ютерних систем	Акти застосування сили у кіберпросторі у межах міжнародного збройного конфлікту
Масштаб і характер наслідків	Масові соціальні, економічні та політичні наслідки, широке суспільне резонансне сприйняття	Переважно локальні матеріальні збитки, порушення конфіденційності	Стратегічні наслідки для обороноздатності, управління військовими та державними системами
Публічність і комунікаційний аспект	Демонстративний характер, прагнення до медійного резонансу та інформаційного впливу	Може мати латентний характер, орієнтація на прихованість	Може поєднувати відкриті і приховані дії, підпорядковані воєнному плануванню

Джерело: складено автором на основі [5, 7, 8]

Порівняльний аналіз показує, що кібертероризм займає проміжне, але концептуально відокремлене місце між кіберзлочинністю і кібервоєнними діями. Він поєднує нелегітимні засоби інформаційного впливу з політичною метою та націлюванням на критичні об'єкти, проте здійснюється недержавними суб'єктами і не завжди в умовах формально визнаного збройного конфлікту. Таке розуміння є підґрунтям для побудови спеціалізованих кримінально-правових норм і комплексної системи протидії кібертерористичним загрозам.

Цілі кібертерористичних дій у сучасних умовах гібридних конфліктів пов'язані з політичним тиском на уряди, нав'язуванням рішень у сфері безпеки та демонстрацією сили терористичних угруповань перед національною і міжнародною аудиторією [9]. Кібертерористи використовують інформаційні ресурси та цифрові платформи для залякування населення, підриву довіри до державних інституцій, провокування міжетнічних і міжрелігійних протистоянь і формування тривалої нестабільності, що обмежує спроможність держави ухвалювати стратегічні оборонні та безпекові рішення [9, 12].

В економічному вимірі кібертероризм спрямований на дестабілізацію фінансових ринків, руйнування ланцюгів постачання та блокування розрахункових систем, що провокує кризові явища у банківському секторі, енергетиці, транспорті та інших критично важливих галузях [11].

Об'єкти кібертерористичних атак концентруються навколо критичної інфраструктури, яка забезпечує безперервність функціонування енергетики, транспорту, зв'язку, водопостачання, охорони здоров'я, фінансових послуг та державного управління [11]. До пріоритетних мішеней належать інформаційні системи органів державної влади, оборонного сектору, розгалужені платіжні та клірингові платформи, а також сегменти телекомунікаційних мереж, від роботи яких залежить надання електронних адміністративних послуг та сервісів безпеки [9, 11].

Огляди подій у сфері кібербезпеки демонструють, що у реальних інцидентах кібертерористичні групи часто комбінують атаки на державні реєстри, вебресурси органів влади, інформаційні системи об'єктів енергетики та транспортної логістики, що створює синергетичний ефект у вигляді перебоїв у роботі базових функцій держави і критичних сервісів для населення [12].

Типові інструменти кібертерористичної діяльності включають застосування шкідливого програмного забезпечення, у тому числі вірусів-вимагачів, програм-стирачів, модулів віддаленого доступу, які інтегруються у мережеву інфраструктуру з метою прихованого контролю, модифікації чи знищення даних [10]. Важливу роль відіграють атаки типу відмови в

обслуговуванні та розподіленої відмови в обслуговуванні, що здійснюються через ботнети та інші форми масового генерування трафіку, які виводять з ладу вебресурси державних органів, електронні сервіси критичної інфраструктури та фінансові платформи [10, 12].

Окрему групу становлять фішингові кампанії та атакувальні операції проти промислових систем керування, зокрема SCADA-компонентів енергетичних, транспортних і водогосподарських об'єктів, які дають змогу кібертерористам не лише отримувати доступ до конфіденційної інформації, а й здійснювати фізичний вплив на технологічні процеси, що створює ризики аварій, масштабних перебоїв у постачанні послуг життєзабезпечення і формує атмосферу тривалої небезпеки в суспільстві [11, 12].

Вплив кібертероризму на політичну стабільність держави пов'язаний з кібератаками проти органів публічної влади, виборчої інфраструктури, офіційних каналів комунікації та засобів масової інформації, що веде до делегітимації рішень, недовіри до результатів виборів і урядової політики, а також до посилення поляризації суспільства [5, 9]. Скоординовані інформаційно-технічні операції, які поєднують компрометацію державних електронних сервісів з масованими кампаніями дезінформації, формують у громадян відчуття беззахисності, провокують політичні кризи, протестну активність, блокування інституційних каналів врегулювання конфліктів і знижують стійкість політичної системи до шоків [13].

У сфері економічної безпеки, обороноздатності та суспільної безпеки кібертероризм проявляється через атаки проти критичної інформаційної інфраструктури, фінансових систем, логістичних мереж, систем управління військовими ресурсами й об'єктами енергетики [13]. Порушення роботи платіжних систем, електронних торгівельних майданчиків, енергетичних і транспортних операторів спричиняє простій підприємств, збої у постачанні товарів і послуг, зниження інвестиційної привабливості та загрозу економічній безпеці. Атаки на інформаційні системи сектору безпеки і оборони обмежують можливості оперативного планування, координації дій і захисту населення, а

інциденти у сфері охорони здоров'я, зв'язку чи житлово-комунального господарства посилюють відчуття небезпеки, підривають довіру до інституцій держави і стимулюють радикалізацію частини населення.

Для систематизації впливу кібертероризму на різні компоненти національної безпеки доцільно виділити типові наслідки і запропонувати орієнтовні індикатори, що можуть застосовуватися у процесі моніторингу та оцінювання ризиків (табл. 1.2).

Таблиця 1.2

Компоненти національної безпеки та можливі наслідки кібертероризму

Компонент національної безпеки	Типові наслідки кібертерористичних дій	Потенційні індикатори оцінювання
Політична безпека	Делегітимація органів влади, зрив виборчих процесів, посилення політичної поляризації, зростання протестної активності	Частота інцидентів з втручанням у інформаційні ресурси органів влади, рівень довіри до інституцій, індекс політичної стабільності
Економічна безпека	Порушення функціонування фінансових ринків, збої у роботі банківських і платіжних систем, розрив ланцюгів постачання	Обсяги економічних збитків від кібератак, кількість порушень роботи фінансових та логістичних систем, зміни інвестиційної активності
Військова безпека та оборона	Зниження ефективності управління військами, компрометація інформації про оборонні об'єкти, порушення систем зв'язку	Кількість інцидентів у системах управління оборонними структурами, тривалість порушень зв'язку, показники готовності сил оборони
Безпека критичної інфраструктури	Перебої в енергопостачанні, транспорті, зв'язку, водопостачанні, зростання ризику техногенних аварій	Кількість кібератак на об'єкти критичної інфраструктури, тривалість простоїв, масштаби порушення надання послуг населенню
Суспільна безпека і довіра	Зростання відчуття небезпеки у населення, поширення панічних настроїв, радикалізація частини громадян	Соціологічні показники відчуття безпеки, рівень довіри до державних і безпекових інституцій, індикатори радикалізації та протестної активності

Джерело: складено автором на основі [4, 9, 11, 13]

Підсумовуючи наведені положення, слід зазначити, що кібертероризм модифікує традиційні уявлення про загрози національній безпеці, оскільки

поєднує технічні інструменти впливу з політичними, економічними та соціальними цілями. Визначення компонентів національної безпеки, найбільш чутливих до кібертерористичних дій, та побудова системи індикаторів для їх оцінювання створюють методологічне підґрунтя для формування скоординованої політики кібербезпеки, орієнтованої на превенцію, своєчасне виявлення і мінімізацію наслідків таких загроз.

Отже, кібертероризм формується як політично або ідеологічно мотивована діяльність, що застосовує інформаційно-комунікаційні технології для завдання шкоди критичній інфраструктурі, дестабілізації державного управління та створення суспільної напруженості. Його вплив поширюється на політичну стабільність, економічну та оборонну безпеку, а також на рівень довіри громадян до державних інституцій. Сукупність цих факторів перетворює кібертероризм на комплексну загрозу національній безпеці, яка потребує системного аналізу й інтегрованих механізмів протидії.

1.2 Класифікація кібертерористичних загроз та атак

Побудова ефективної системи протидії кібертероризму передбачає не тільки фіксацію окремих інцидентів, але і впорядкування загроз за чіткими критеріями. Класифікація кіберзагроз є необхідною умовою для пріоритизації ресурсів, вибору адекватних моделей ризику та визначення критичних елементів інфраструктури, які потребують першочергового захисту [14]. Це стосується насамперед загроз кібертерористичного характеру, які поєднують технологічні, політичні та психологічні фактори впливу на державу, бізнес та населення [17].

Методологічні підходи до класифікації кібертерористичних загроз ґрунтуються на виділенні кількох базових критеріїв. По-перше, у працях А. Шкітова, Д. Світличного та інших дослідників сформовано підхід, за якого відправною точкою є джерело походження загрози: державні актори, недержавні терористичні угруповання, змішані або проксі-структури, що діють за підтримки іноземних спецслужб [14]. По-друге, окремо розглядається об’єкт впливу: органи

державної влади, критична інфраструктура, фінансовий сектор, інформаційно-комунікаційні мережі, суспільні інститути, які через залежність від цифрових сервісів набувають вразливості до кібертерористичних атак [16].

По-третє, важливим критерієм є масштаб і рівень координації дій. У роботах Я. Мазур та В. Машталіра простежується підхід, за якого загрози ранжуються від локальних, малокоординованих атак до комплексних кампаній, що комбінують кіберудари, інформаційно-психологічні впливи і фізичні дії проти об'єктів критичної інфраструктури [6, 14, 17].

Така багатовимірна класифікація дає змогу не тільки описувати спектр можливих кібертерористичних дій, але і співвідносити їх з конкретними індикаторами ризику, інструментами моніторингу та процедурами реагування, які закріплюються у доктринальних і програмних документах з кібербезпеки.

Узагальнення наукових підходів дає змогу виокремити три основні групи кібертерористичних загроз. Перша група – стратегічні загрози, спрямовані на завдання масштабної шкоди критичній інфраструктурі та підрив довгострокової спроможності держави забезпечувати базові публічні послуги й реалізовувати оборонну політику [9, 14].

Друга група – операційні загрози, що проявляються у прицільних кібератаках на окремі органи державної влади, бізнес-структури чи військові об'єкти з метою порушення процесів управління, логістики та фінансів. Третя група – інформаційно-психологічні загрози, у межах яких кіберзасоби застосовуються для поширення дезінформації, дискредитації державних інститутів, провокування панічних настроїв і послаблення суспільної стійкості [17].

У таблиці 1.3 класифікація кібертерористичних загроз представлена за поєднанням критеріїв джерела походження, об'єктів впливу, рівня координації та очікуваних ефектів. Класифікація кібертерористичних загроз за джерелом, об'єктами впливу та масштабом дій створює підґрунтя для диференціації заходів протидії.

Таблиця 1.3

Класифікація кібертерористичних загроз за основними критеріями

Група загроз	Джерело походження	Основні об’єкти впливу	Рівень координації та масштаб	Типові очікувані ефекти
Стратегічні кібертерористичні загрози	Державні актори, транснаціональні терористичні мережі, гібридні структури	Критична інфраструктура, системи енергетики, транспорту, зв’язку, оборонні інформаційні системи	Висока координація, міжсекторальні та міждержавні кампанії	Порушення функціонування держави, довготривалі збої послуг, системні економічні втрати
Операційні кібертерористичні загрози	Терористичні організації, радикалізовані групи, окремі угруповання хактивістів	Окремі державні органи, військові підрозділи, фінансові установи, великі компанії	Середній рівень координації, локальні або галузеві атаки	Порушення процесів управління, локальні кризи, фінансові втрати, витік конфіденційних даних
Інформаційно-психологічні кібертерористичні загрози	Терористичні мережі, інформаційні підрозділи недержавних акторів, мережеві спільноти	Населення, медіапростір, органи публічної влади, політичні інститути	Від низької до високої координації, тривалі кампанії у цифровому середовищі	Дестабілізація суспільної думки, підрив довіри до інституцій, посилення поляризації та панічних настроїв

Джерело: складено автором на основі [6, 10, 14–17]

Для стратегічних загроз пріоритетними стають інструменти захисту критичної інфраструктури і міжвідомча координація, для операційних – побудова галузевих механізмів кіберстійкості, тоді як для інформаційно-психологічних загроз ключового значення набувають системи моніторингу інформаційного простору, медіаграмотність та кризові комунікації.

У системі класифікації кіберзагроз виокремлюються технічні й організаційні типи атак, які за мотивацією суб’єктів та спрямованістю на об’єкти критичної інфраструктури можуть набувати ознак кібертероризму. До них належать розподілені атаки відмови в обслуговуванні (DDoS-атаки), орієнтовані

на блокування електронних сервісів органів державної влади, порталів електронного урядування та інших критично важливих онлайн-платформ [18]. Застосування таких атак має подвійний ефект: поряд із технічним порушенням функціонування інформаційних систем воно формує публічне уявлення про вразливість держави, індукує панічні настрої серед населення та сприяє делегітимації владних інститутів [18, 19].

Окрему групу становлять кібератаки на промислові системи керування (SCADA, промислові та логічні програмовані контролери), що забезпечують функціонування енергетичних, транспортних, комунальних та інших критично важливих об'єктів [21]. Їх компрометація, включно із зламом урядових інформаційних ресурсів, створює ризики техногенних аварій, тривалих збоїв у постачанні базових послуг і спотворення чи блокування доступу до даних, які можуть використовуватися для подальших деструктивних впливів [19].

Вагому групу становлять кібертерористичні впливи на фінансові системи, засоби масової інформації та платформи соціальних мереж. У фінансовому секторі це проявляється у компрометації платіжних і банківських інформаційних систем, порушенні оброблення транзакцій, що зумовлює ризики значних економічних втрат, ерозії довіри до фінансових інститутів і порушення макрофінансової стабільності держави [20].

У медійному та комунікаційному просторі такі дії полягають у зламі редакційних систем, маніпуляції контентом і цілеспрямованому поширенні дезінформації через соціальні мережі з метою деморалізації населення, індукування панічних настроїв і посилення суспільної поляризації [22]. Політична, ідеологічна чи релігійна мотивація та орієнтація на публічний резонанс і залякування населення або органів влади дають підстави відносити такі атаки до кібертерористичних, а не лише кіберзлочинних [4, 18].

У таблиці 1.4 наведено ключові характеристики базових типів кібертерористичних атак, що дає змогу пов'язати тип об'єкта, основну мету нападника, застосовані методи та очікувані наслідки для системи національної безпеки. Кібертерористичні атаки відрізняються не лише технічними

параметрами, а передусім поєднанням об’єкта, мети та очікуваного суспільно-політичного ефекту.

Таблиця 1.4

Типи кібертерористичних атак та їх ключові характеристики

Тип атаки	Основний об’єкт	Головна мета	Ключові методи реалізації	Ймовірні наслідки
1	2	3	4	5
DDoS-атака проти державних та сервісних ресурсів	Веб-сайти органів державної влади, портали електронних послуг, інформаційні ресурси критичної інфраструктури	Порушення доступності послуг, дестабілізація роботи органів влади, демонстрація їх вразливості	Генерування надмірного трафіку з розподілених бот-мереж, експлуатація вразливостей протоколів та сервісів	Блокування електронних сервісів, зрив комунікації з громадянами, репутаційні втрати, панічні настрої
Атака на промислові системи керування та SCADA	Енергетичні об’єкти, транспортні системи, об’єкти житлово-комунального господарства, промислові підприємства	Фізичне пошкодження обладнання, припинення технологічних процесів, створення аварійних ситуацій	Несанкціонований віддалений доступ до контролерів, модифікація конфігурацій, шкідливе програмне забезпечення для промислових систем	Аварії та пошкодження інфраструктури, тривалі відключення послуг, економічні збитки, ризики для життя і здоров’я населення
Злам урядових інформаційних ресурсів	Державні реєстри, системи документообігу, інформаційно-аналітичні системи органів влади	Дезорганізація державного управління, компрометація даних, підрив довіри до влади	Використання вразливостей прикладного програмного забезпечення, фішинг для отримання облікових даних, експлуатація слабких механізмів автентифікації	Витік або знищення даних, блокування управлінських процесів, ускладнення роботи органів влади, підвищення вразливості до інших атак
Компрометація фінансових систем	Банківські інформаційні системи, платіжні платформи, міжбанківські розрахункові системи	Порушення фінансової стабільності, завдання економічної шкоди, підрив довіри до фінансового сектору	Викрадення облікових даних, шкідливе програмне забезпечення для доступу до платіжних систем, атаки на інфраструктуру розрахунків	Зрив платежів і розрахунків, прямі фінансові втрати, масовий витік фінансових даних, зниження довіри до фінансових установ

Продовження табл. 1.4

1	2	3	4	5
Атакування засобів масової інформації та платформ соціальних мереж	Редакційні системи засобів масової інформації, облікові записи в соціальних мережах, платформи масової комунікації	Поширення дезінформації, посилення суспільної напруженості, делегітимація державних інститутів	Злам облікових записів, розміщення фальшивого контенту, автоматизоване поширення повідомлень через бот-мережі, таргетовані інформаційні кампанії	Формування викривленої картини реальності, падіння довіри до офіційних джерел інформації, підвищення конфліктності у суспільстві

Джерело: складено автором на основі [18,19,20,21,22]

Систематизація наведених у таблиці 1.4 характеристик типів кібертерористичних атак дає змогу чітко відмежовувати кібертероризм від суто кримінальних кібератак, а також обґрунтовувати пріоритетні напрями посилення кіберзахисту в системі державного управління, сегментах критичної інфраструктури, фінансовому секторі та інформаційному просторі держави.

Ескалація кібертерористичних атак має поетапний характер і охоплює підготовку, первинне проникнення, закріплення у скомпрометованому середовищі, масштабування, реалізацію деструктивного впливу та приховування слідів. На початкових стадіях здійснюються розвідка, підбір інструментів, експлуатація вразливостей і отримання облікових даних, далі – встановлення прихованих засобів віддаленого доступу й розширення присутності в мережі, у тому числі через поширення шкідливого програмного забезпечення на критичні сегменти інфраструктури [18]. Завершальний етап передбачає запуск деструктивних сценаріїв з політичними, економічними або психологічними цілями та модифікацію журналів подій і цифрових артефактів для ускладнення розслідування інциденту [20].

Виділення послідовних стадій розвитку кібертерористичної атаки є важливим для побудови системи раннього виявлення загроз, оскільки дає змогу пов’язати індикатори компрометації з етапами ескалації та сформувати поетапні

заходи протидії – від превентивних дій і фіксації аномалій доступу до цілеспрямованого реагування й відновлення. Це переводить систему кібербезпеки від пасивного реагування до проактивного управління життєвим циклом атаки, що є критично важливим за умов кібертерористичних загроз [16].

На рисунку 1.1 відображено послідовність етапів, базові індикатори, що можуть фіксуватися на кожній стадії, а також орієнтовні заходи протидії, які реалізуються у межах системи національної кібербезпеки.

Рис. 1.1 Схема ескалації кібертерористичної атаки

Джерело: побудовано автором на основі [18,20]

Схематичне подання етапів ескалації кібертерористичної атаки показує, що кожна стадія генерує власний набір індикаторів, які можуть бути використані системою кібермоніторингу для раннього виявлення загроз. Поетапний підхід дозволяє поєднати технічні засоби контролю, організаційні процедури і правові механізми реагування та формує методологічну основу для проєктування інтегрованих систем кіберзахисту, орієнтованих на превенцію і мінімізацію наслідків кібертероризму.

Отже, класифікація кібертерористичних загроз і атак формує структуроване уявлення про типи загроз, мотиви їх реалізації, об'єкти впливу та масштаби можливих наслідків. Виокремлення груп загроз, рівнів ескалації і базових технічних форм атак забезпечує можливість побудови проєктних рішень для превенції, раннього виявлення та реагування. Такий підхід створює методологічну основу для системного зміцнення національної кібербезпеки та визначення пріоритетів державної політики протидії кібертероризму.

1.3 Міжнародні стандарти та нормативно-правова база щодо протидії кібертероризму (NIST, ENISA, законодавство України)

Міжнародні підходи до протидії кібертероризму ґрунтуються на діяльності кількох провідних інституцій, серед яких особливе місце посідають NIST та ENISA. NIST формує комплекс рамкових документів з кібербезпеки, у тому числі рамку кібербезпеки версії 2.0, які задають ризик орієнтовану модель управління загрозами, послідовність процесів ідентифікації, захисту, виявлення, реагування та відновлення, а також вимоги до безперервного моніторингу стану захищеності [27, 29].

ENISA, як агенція Європейського Союзу з питань кібербезпеки, підтримує розроблення та впровадження європейських стандартів управління ризиками, інцидент менеджменту та кіберстійкості, зокрема через аналітичні огляди загроз і рекомендації щодо побудови національних стратегій кібербезпеки [28]. Спільними принципами для цих підходів є управління ризиками як основа

політики протидії кіберзагрозам, безперервний моніторинг стану інформаційної інфраструктури та інституціоналізований процес оброблення інцидентів, що безпосередньо формує методологічний фундамент системи протидії кібертероризму.

У протидії кібертероризму NIST Cybersecurity Framework розглядається як еталонна модель організації кіберзахисту для критичної інфраструктури та державних органів. Її базові функції – ідентифікація, захист, виявлення, реагування та відновлення – формують замкнений цикл управління кіберризиками, що охоплює інвентаризацію активів і вразливостей, впровадження захисних заходів, моніторинг аномалій, інцидент-менеджмент і планування безперервності діяльності [27, 29].

Для протидії кібертероризму це означає можливість проєктувати спеціальні профілі кібербезпеки для об’єктів енергетики, транспорту, фінансового сектору та органів влади, інтегруючи вимоги щодо захисту критичної інфраструктури, забезпечення стійкості до складних цільових атак і швидкого відновлення після реалізації деструктивних сценаріїв [27, 30].

Підходи ENISA до забезпечення стійкості кіберпростору зосереджені на аналітичному супроводі політики Європейського Союзу у сфері кібербезпеки, підтримці впровадження стандартів управління ризиками, розбудові спроможностей національних команд реагування на інциденти та розвитку культури кіберстійкості в державному і приватному секторах [28, 31].

У контексті протидії кібертероризму ENISA розробляє рекомендації щодо захисту критичної інфраструктури, готує огляди загроз і методичні матеріали для секторів енергетики, транспорту, фінансів, а також координує обмін інформацією про кібератаки між державами Європейського Союзу та партнерами [28, 31]. Національні стратегії кібербезпеки та секторіальні стандарти спираються на ці рекомендації, що забезпечує узгодження підходів до протидії кібертерористичним загрозам на міждержавному рівні.

Нормативно правова база України у сфері протидії кібертероризму ґрунтується на поєднанні спеціального законодавства про кібербезпеку,

антитерористичного законодавства, актів щодо захисту критичної інфраструктури та стратегічних документів у сфері національної безпеки. Закон України «Про основні засади забезпечення кібербезпеки України» закріплює суб'єктів національної системи кібербезпеки, визначає принципи кіберзахисту та пріоритети захисту критичної інфраструктури, у тому числі від терористичних загроз у кіберпросторі [32].

Закон «Про боротьбу з тероризмом» встановлює правові основи протидії терористичній діяльності, повноваження суб'єктів боротьби з тероризмом та порядок проведення антитерористичних операцій, що поширюється і на дії у кіберпросторі [33]. Закон України «Про критичну інфраструктуру», постанова Кабінету Міністрів України № 1109 «Деякі питання об'єктів критичної інфраструктури» та пов'язані підзаконні акти формують рамку ідентифікації, категоризації та моніторингу безпеки об'єктів, які є пріоритетними мішенями кібертерористичних атак [34, 35]. Стратегія кібербезпеки України, затверджена Указом Президента № 447/2021, визначає кібертероризм однією з ключових загроз національній безпеці та орієнтує на побудову стійкої системи кіберзахисту у тісній взаємодії державних органів і приватного сектору [36].

У таблиці 1.5 зіставлено основні міжнародні стандарти і ключові нормативні акти України, їх зміст, релевантність для протидії кібертероризму та особливості імплементації.

Таблиця 1.5

Ключові міжнародні стандарти та нормативні акти України у сфері протидії кібертероризму

Документ / стандарт	Орган, що прийняв	Короткий зміст	Релевантність для протидії кібертероризму	Особливості імплементації в Україні
1	2	3	4	5
Рамка NIST Cybersecurity Framework	Національний інститут стандартів і технологій (США)	Модель управління кіберризиками з функціями ідентифікації, захисту, виявлення, реагування та відновлення	Орієнтир для побудови систем кіберзахисту критичної інфраструктури, розроблення профілів безпеки для об'єктів підвищеного ризику	Використовується як методична основа у відомчих документах та підзаконних актах щодо кіберзахисту критичної інфраструктури

Продовження табл. 1.5

1	2	3	4	5
Аналітичні та методичні документи ENISA	Агенція Європейського Союзу з питань кібербезпеки	Огляди загроз, рекомендації з управління ризиками	Формують підходи до оцінювання і протидії складним кібератакам,	Використовуються як орієнтир під час розроблення стратегічних документів.
Закон України «Про основні засади забезпечення кібербезпеки України»	Верховна Рада України	Визначає правові та організаційні засади кібербезпеки, суб'єктів системи, принципи захисту кіберпростору	Створює правову основу діяльності державних органів і взаємодії з приватним сектором у протидії кібертерористичним загрозам	Імплементується через підзаконні акти, секторальні вимоги до кіберзахисту та створення уповноважених органів кібербезпеки
Закон України «Про боротьбу з тероризмом»	Верховна Рада України	Визначає правові основи, суб'єктів, принципи та порядок здійснення боротьби з тероризмом	Надає загальну рамку для кваліфікації кібертерористичних діянь і організації антитерористичних заходів	Застосовується з урахуванням специфіки кіберпростору через підзаконні акти, доктринальні документи та практику залучення кіберпідрозділів
Закон України «Про критичну інфраструктуру»	Верховна Рада України	Визначає правові засади функціонування системи захисту критичної інфраструктури, її суб'єктів та об'єктів	Фокусує увагу на найбільш вразливих до кібертероризму об'єктах та визначає вимоги до їх захисту	Реалізується через секторальні переліки об'єктів, моніторинг рівня безпеки та механізми міжвідомчої координації
Постанова Кабінету Міністрів України № 1109 «Деякі питання об'єктів критичної інфраструктури»	Кабінет Міністрів України	Встановлює порядок віднесення об'єктів до критичної інфраструктури, критерії та організаційні процедури	Дає змогу ідентифікувати об'єкти, які є потенційними мішенями кібертерористичних атак, і визначити пріоритети захисту	Забезпечує практичну реалізацію вимог законів у частині обліку, категоризації та паспортизації об'єктів критичної інфраструктури
Указ Президента України № 447/2021 «Про Стратегію кібербезпеки України»	Президент України, Рада національної безпеки і оборони України	Визначає пріоритети, цілі та завдання державної політики у сфері кібербезпеки, у тому числі у протидії кібертероризму	Закріплює кібертероризм як одну з ключових загроз, орієнтує на розвиток національної системи кібербезпеки та зміцнення міжнародної співпраці	Імплементується через секторальні стратегії, державні програми, плани заходів і діяльність уповноважених органів безпеки

Джерело: складено автором на основі [27, 28, 29, 31, 32, 33, 34, 35, 36]

Протидія кібертероризму спирається на поєднання міжнародних стандартів управління кіберризиками з національними законами, підзаконними актами та стратегічними документами. Узгодженість цих рівнів забезпечує можливість адаптувати найкращі світові практики до українського правового поля, посилювати захист критичної інфраструктури та формувати цілісну систему взаємодії державних органів і приватного сектору у сфері кібербезпеки.

Порівняльний аналіз показує, що українське законодавство загалом узгоджується з міжнародними підходами NIST та ENISA за принципами ризик орієнтованого управління, роллю критичної інфраструктури та пріоритетом інцидент менеджменту, однак залишається менш деталізованим щодо практичних процедур оцінювання кіберризиків, секторальних профілів безпеки та формалізованих вимог до кіберстійкості об’єктів.

Сильні сторони національної системи пов’язані з наявністю базових законів і стратегій, тоді як ключовими прогалинами є нерівномірна імплементація норм, обмежена стандартизація вимог для різних секторів і недостатня регламентація механізмів взаємодії державних органів з приватним сектором у форматі, який відповідав би найкращим практикам NIST та ENISA.

1.4 Роль державних та приватних структур у системі протидії кібертероризму

Національна система протидії кібертероризму включає сукупність суб’єктів, серед яких виокремлюють органи, відповідальні за формування державної політики і нормативно правове регулювання у сфері кібербезпеки, спеціалізовані структури оперативного реагування та розвідки, правоохоронні органи, координаційні центри, а також суб’єктів секторального нагляду за критичною інфраструктурою [23, 24, 32].

У межах цієї системи розподіляються функції нормотворчості, вироблення стратегічних рішень, виявлення і припинення кібертерористичних загроз, аналітичного супроводу та ситуаційної обізнаності, міжнародної взаємодії з

партнерами і участі в кіберальянсах [32, 36]. Координаційні механізми національної кібербезпеки орієнтовані на інтеграцію зусиль різних органів, побудову єдиного простору обміну інформацією про інциденти і забезпечення узгоджених дій у разі реалізації загроз кібертерористичного характеру [24, 26].

Приватний сектор і оператори критичної інфраструктури розглядаються як повноцінні суб'єкти протидії кібертероризму, оскільки саме на їхніх інформаційних системах зосереджено значну частину технологічних, фінансових і комунікаційних ресурсів держави [18, 20].

Для таких суб'єктів законодавчо встановлюються обов'язки з упровадження засобів кіберзахисту, створення систем управління інформаційною безпекою, виконання вимог до захисту критичної інфраструктури та своєчасного повідомлення про інциденти [32, 34, 35]. Рівень стійкості держави до кіберзагроз істотно залежить від зрілості систем безпеки у корпоративному секторі та готовності приватних компаній інвестувати у кіберзахист, резервування потужностей, безперервність бізнес-процесів [12, 20].

Система державно приватної взаємодії у сфері кібербезпеки включає обмін інформацією про кібератаки, спільні науково дослідні проєкти, участь бізнесу у національних кластерах кібербезпеки, а також регулярні спільні навчання та тренінги [25, 37].

Такі механізми дозволяють поєднати ресурси державних органів і приватних компаній, узгодити практичні стандарти реагування, прискорити адаптацію міжнародних підходів до національного середовища та створити більш стійку до кібертерористичних дій екосистему критичної інфраструктури.

Механізми публічно приватного партнерства у сфері протидії кібертероризму охоплюють створення спільних робочих груп, галузевих центрів обміну інформацією про інциденти, платформ для оперативного попередження про загрози, а також узгоджених протоколів реагування, у межах яких державні органи і приватні компанії координують дії під час складних кібератак проти критичної інфраструктури [41].

Такі формати взаємодії забезпечують поєднання регуляторних повноважень і розвідувально аналітичних ресурсів держави з технологічною експертизою, інноваційним потенціалом і операційними можливостями бізнесу, що підвищує швидкість виявлення атак, якість обміну оперативною інформацією, узгодженість заходів реагування і створює більш стійке до кібертерористичних загроз середовище.

Міжнародна координація протидії кібертероризму ґрунтується на участі держави у діяльності міжнародних організацій і форматів співпраці з кібербезпеки, де важливу роль відіграють платформи обміну інформацією про загрози, спільні навчання та міжнародні форуми [42].

Участь у таких ініціативах забезпечує доступ до актуальних даних про кіберзагрози, методичної підтримки з боку міжнародних експертних структур, включаючи установи, пов'язані з Організацією Об'єднаних Націй, Північноатлантичним альянсом, Європейським Союзом та спеціалізованими центрами кібероборони [43]. Обмін досвідом, інформацією про індикатори компрометації, сценаріями атак і найкращими практиками дає змогу державним і приватним суб'єктам підвищувати рівень готовності до складних багаторівневих кібератак, адаптувати власні стратегії кіберзахисту до глобальних тенденцій і посилювати спроможність протидії кібертероризму.

Отже, ефективна протидія кібертероризму спирається на узгоджену взаємодію державних органів, приватного сектору та операторів критичної інфраструктури, які виконують різні, але взаємодоповнювальні функції. Розподіл повноважень між нормотворчими, координаційними, оперативними та аналітичними структурами і розвиток публічно приватного партнерства створюють умови для своєчасного виявлення кібертерористичних загроз, підвищення кіберстійкості ключових об'єктів та посилення інтеграції у міжнародні ініціативи кібербезпеки.

Таким чином, теоретико-методологічні основи протидії кібертероризму охоплюють цілісну систему понять, класифікацій та інституційних підходів, які забезпечують наукове підґрунтя для формування державної політики

кібербезпеки. Розкрито зміст кібертероризму як специфічної загрози національній безпеці, обґрунтовано класифікацію кібертерористичних загроз і атак, проаналізовано міжнародні стандарти та національне нормативно-правове регулювання, а також окреслено роль державних і приватних суб'єктів у побудові стійкої системи протидії. Сукупність цих положень формує методологічну базу для подальшого аналітичного дослідження стану протидії кібертероризму та розроблення практичних заходів його нейтралізації.

Висновки до Розділу 1

Кібертероризм постає як системний чинник дестабілізації національної безпеки, оскільки поєднує політичну або ідеологічну мотивацію з технологічно складними кібератаками. Його особливість полягає в спрямованості на критичну інфраструктуру, органи публічної влади, фінансовий сектор і суспільну свідомість, що формує багаторівневий ризик для політичної, економічної, оборонної та інформаційної безпеки держави.

Класифікація кібертерористичних загроз і атак демонструє, що реальна небезпека виникає не тільки від масштабних стратегічних кампаній, а й від операційних та інформаційно психологічних дій, які можуть мати кумулятивний ефект. Розмежування загроз за джерелами, об'єктами впливу, рівнем координації та етапами ескалації створює підґрунтя для адресного управління ризиками, пріоритизації захисту й проєктування систем раннього виявлення.

Порівняння міжнародних стандартів NIST і ENISA з українським правовим полем показує часткову відповідність за принципами ризик орієнтованого підходу, інцидент менеджменту та акцентом на критичній інфраструктурі. Разом з тим виявляється потреба посилити нормування секторальних вимог, конкретизувати процедури оцінювання кіберризиків, підвищити рівень практичної імплементації стратегічних документів і узгодити їх із міжнародними профілями кіберстійкості.

Аналіз ролі державних і приватних структур підтверджує, що без активної участі операторів критичної інфраструктури, бізнесу та розвинених механізмів публічно приватного партнерства формування дієвої системи протидії кібертероризму є неможливим. Синхронізація правового регулювання, організаційних моделей управління безпекою, інформаційного обміну та міжнародної координації виступає ключовою умовою підвищення стійкості національного кіберпростору до кібертерористичних загроз.

РОЗДІЛ 2
АНАЛІЗ СУЧАСНИХ МЕХАНІЗМІВ ПРОТИДІЇ КІБЕРТЕРОРИЗМУ

2.1 Технічні методи захисту критичної інфраструктури (IDS/IPS, SIEM, SOC, AI/ML)

Критична інфраструктура охоплює енергетичний, транспортний, фінансовий, комунальний, медичний та державний сектори, у яких функціонують взаємопов'язані технічні й інформаційні системи управління технологічними процесами, обліку та комунікацій [44, 45]. Вразливість цих систем зумовлена використанням застарілих технологій, розгалуженими мережами доступу, наявністю віддалених підключень, інтерфейсів SCADA та великою кількістю користувачів, що створює значний простір для кібератак із істотним впливом на національну безпеку (табл. 2.1).

Таблиця 2.1

Об'єкти критичної інфраструктури та основні вектори кібератак

Сектор критичної інфраструктури	Тип об'єкта	Ключові інформаційні системи	Типові вектори кібератак	Потенційні наслідки для безпеки
1	2	3	4	5
Енергетика	Електростанції, підстанції, газо- та нафтотранспортні системи	Автоматизовані системи диспетчерського керування, SCADA, системи комерційного обліку енергоносіїв	Несанкціонований доступ до систем управління, шкідливе програмне забезпечення, маніпуляція параметрами, криптовірусні атаки	Порушення енергопостачання, масштабні відключення, збої в роботі інших секторів
Транспорт	Залізничні вузли, морські порти, аеропорти, автомагістралі	Інформаційні системи управління рухом, логістичні платформи, системи бронювання та диспетчеризації	Компрометація облікових записів, атаки на сервери управління, підміна маршрутних даних, DDoS	Зрив перевезень, логістичні колапси, підвищення ризику аварій

Продовження табл. 2.1

1	2	3	4	5
Фінансовий сектор	Банки, платіжні системи, фондові та клірингові структури	Банківські автоматизовані системи, платіжні шлюзи, системи дистанційного обслуговування	Викрадення облікових даних, атакування платіжних систем, втручання в розрахункові операції, шкідливе програмне забезпечення	Викрадення коштів, дестабілізація розрахунків, підрив довіри до фінансової системи
Охорона здоров'я	Лікарні, центри екстреної медичної допомоги, лабораторії	Медичні інформаційні системи, реєстри пацієнтів, системи телемедицини, мережеві пристрої медичного обладнання	Несанкціонований доступ до персональних даних, шифрування медичних баз, атакування мережевого обладнання	Блокування медичних послуг, витік чутливої інформації, ризики для життя пацієнтів
Державне управління	Органи центральної та місцевої влади, органи сектору безпеки	Інформаційно-аналітичні системи, реєстри, електронний документообіг, системи електронних послуг	Злам інформаційних ресурсів, підміна інформації, DDoS, атакування сервісів надання електронних послуг	Порушення роботи органів влади, делегітимізація рішень, зниження довіри до державних інституцій

Джерело: складено автором на основі [44, 46, 47]

Узагальнена характеристика секторів критичної інфраструктури демонструє, що технічні вразливості інформаційних систем безпосередньо трансформуються у ризики для життєво важливих послуг, економічної стабільності та суспільної безпеки, а тому потребують пріоритизації при плануванні системи протидії кібертероризму.

Застосування IDS/IPS, SIEM і SOC у захисті критичної інфраструктури полягає у побудові багаторівневої системи виявлення та блокування вторгнень, кореляції подій безпеки та безперервного моніторингу стану інформаційних систем. IDS/IPS фіксують і блокує мережеві та хостові атаки, SIEM агрегує журнали подій із різнорідних джерел, виконує кореляцію та формує інциденти, а центри моніторингу безпеки SOC організовують цілодобовий аналіз подій,

реагування і координацію дій технічних та організаційних підрозділів, що особливо важливо для об’єктів критичної інфраструктури [46].

У таблиці 2.2 відображено аналітичні відмінності між класами рішень за призначенням, типами виявлюваних загроз, рівнем автоматизації та ключовими обмеженнями, що дозволяє обґрунтувати необхідність їх спільного застосування, а не взаємної заміни.

Таблиця 2.2

Порівняльна характеристика технічних засобів виявлення та реагування на інциденти

Основне призначення	Типи виявлюваних загроз	Рівень автоматизації процесів	Основні обмеження застосування
1	2	3	4
IDS (системи виявлення вторгнень)			
Пасивне або напівпасивне виявлення підозрілої активності у мережевому трафіку та на хостах, формування сповіщень для аналітиків	Відомі сигнатурні атаки, аномальний трафік, спроби сканування, базові експлойти та підозрілі з’єднання	Середній: автоматизоване виявлення і генерація сповіщень, реагування здебільшого ініціюється персоналом	Обмежена ефективність проти невідомих і складно маскованих атак, високий рівень хибно позитивних спрацювань, потреба у постійному оновленні сигнатур і баз правил
IPS (системи запобігання вторгненням)			
Активне блокування атак у реальному часі з можливістю модифікації трафіку та відсікання шкідливих дій	Сигнатурні та частина аномальних атак, експлойти відомих вразливостей, спроби несанкціонованого доступу, деякі типи DDoS	Вищий за середній: автоматичне блокування за налаштованими правилами і політиками, інтеграція з міжмережевими екранами	Ризик блокування легітимного трафіку, складність налаштування політик для критичних сервісів, обмежена видимість за межами мережевого периметра, потреба у ретельному тестуванні змін
SIEM (системи управління інформацією та подіями безпеки)			
Централізований збір, зберігання та кореляція журналів подій безпеки з різних систем, формування інцидентів та аналітичних звітів	Комплексні багатоступеневі атаки, повільні проникнення, внутрішні загрози, послідовності подій, що окремо не виглядають критичними	Високий: автоматизована кореляція подій, створення правил виявлення, формування інцидентів, підтримка робочих процесів реагування	Високі вимоги до якості журналів і налаштування кореляційних правил, значні витрати на впровадження та супровід, ризик перевантаження аналітиків великою кількістю сповіщень

Продовження табл. 2.2

1	2	3	4
SOC (центр моніторингу безпеки)			
Організація безперервного моніторингу, аналізу інцидентів, реагування та координації заходів кіберзахисту на рівні організації або сектору	Комплексний спектр загроз: зовнішні та внутрішні атаки, кібершпигунство, кібертерористичні кампанії, інциденти у взаємопов'язаних системах	Змішаний: поєднання автоматизованих інструментів (IDS/IPS, SIEM, SOAR) з роботою аналітиків, розроблення сценаріїв реагування і процедур ескалації	Залежність від кваліфікації персоналу, значні організаційні й фінансові витрати, потреба у чіткому регламенті взаємодії з підрозділами і зовнішніми партнерами, складність масштабування для багатосекторних об'єктів критичної інфраструктури

Джерело: складено автором на основі [44,45,46,47]

Аналітичне порівняння показує, що системи виявлення та запобігання вторгненням (IDS та IPS) забезпечують переважно периметровий і мережевий рівень захисту, SIEM формує цілісну картину подій безпеки та дає змогу виявляти складні тривалі атаки, а SOC інтегрує технічні засоби і людські ресурси в безперервний процес моніторингу та реагування. Поєднання цих рішень у єдиній архітектурі кіберзахисту критичної інфраструктури скорочує час виявлення інцидентів, підвищує якість реагування та забезпечує пріоритизацію ресурсів щодо загроз кібертерористичного характеру.

Застосування методів штучного інтелекту і машинного навчання у протидії кібертероризму ґрунтується на аналізі аномалій у мережевому трафіку, журналах подій, поведінці користувачів та роботі прикладних систем. Такі підходи дають змогу виявляти нетипові послідовності дій, повільні багатоетапні атаки, приховані спроби закріплення у мережі, які часто залишаються поза полем зору класичних сигнатурних засобів захисту [44, 45].

Переваги полягають у здатності обробляти великі обсяги даних у реальному часі, виявляти раніше невідомі патерни загроз і скорочувати час виявлення інцидентів, однак існують суттєві ризики: чутливість моделей до якості навчальних вибірок, імовірність зміщень і хибних спрацювань, складність

інтерпретації рішень і можливість цілеспрямованого обходу алгоритмів з боку зловмисників [46, 47].

У таблиці 2.3 наведено основні сфери застосування, типи даних, які використовуються для аналізу, очікуваний ефект для зниження кіберризиків та потенційні ризики впровадження на об’єктах критичної інфраструктури.

Таблиця 2.3

Ключові напрямки застосування методів штучного інтелекту та машинного навчання у кіберзахисті

Напрям застосування	Тип даних	Основна мета аналізу	Очікуваний ефект для зниження кіберризиків	Потенційні ризики впровадження
1	2	3	4	5
Аналіз аномалій у мережевому трафіку	Мережеві потоки, заголовки пакетів, статистика з’єднань	Виявлення нетипових з’єднань, сканування, прихованих каналів обміну даними	Раннє виявлення невідомих атак, зменшення часу перебування зловмисника у мережі	Хибні спрацювання, залежність від репрезентативності навчальних даних, складність налаштування порогів
Поведінковий аналіз користувачів і облікових записів	Логи автентифікації, дії користувачів у системах, часові патерни	Виявлення відхилень від звичайної поведінки, захоплення облікових записів, внутрішніх загроз	Зменшення ризику компрометації привілейованих доступів, виявлення інсайдерської активності	Порушення приватності, небезпека неправильної інтерпретації поведінки, ризик дискримінаційних рішень
Автоматизований аналіз шкідливого програмного забезпечення	Файли, сигнатури, динамічні і статичні характеристики виконання	Класифікація шкідливого програмного забезпечення, виявлення нових сімейств і варіантів	Підвищення швидкості класифікації загроз, скорочення навантаження на аналітиків, оперативне оновлення правил захисту	Можливість обходу моделей через модифікацію шкідливого коду, потреба у постійному донавчанні
Інтелектуальний аналіз подій безпеки (кореляція інцидентів)	Журнали подій з мережевих, серверних, прикладних систем, дані SIEM	Виявлення складних багатоступеневих сценаріїв атак, пріоритизація інцидентів	Зниження кількості нерелевантних сповіщень, фокусування ресурсів SOC на критичних загрозах	Непрозорість логіки прийняття рішень, ризик надмірної автоматизації без належного контролю з боку фахівців

Продовження табл. 2.3

1	2	3	4	5
Прогнозування кіберризиків та підтримка прийняття рішень	Історичні дані про інциденти, технічні й організаційні показники, зовнішні індикатори загроз	Оцінювання імовірності інцидентів, моделювання сценаріїв атак, підтримка планування заходів захисту	Оптимізація розподілу ресурсів кіберзахисту, підвищення обґрунтованості управлінських рішень щодо пріоритетів захисту	Ризик хибних прогнозів, надмірна довіра до моделей, можливість використання застарілих або упереджених даних

Джерело: складено автором на основі [44, 46, 47]

Отже, методи штучного інтелекту і машинного навчання доповнюють традиційні засоби кіберзахисту, дозволяючи виявляти складні та раніше невідомі загрози, однак їх застосування вимагає зрілого управління моделями, прозорих процедур валідації, контролю якості даних і чіткого розподілу відповідальності між автоматизованими системами та фахівцями, особливо у контексті захисту критичної інфраструктури.

2.2 Організаційні та адміністративні заходи протидії кібертероризму

Національна система управління ризиками кібертероризму ґрунтується на багаторівневій моделі, у межах якої державний рівень відповідає за формування політики, законодавства та загальної координації, галузевий рівень – за адаптацію вимог до особливостей конкретних секторів критичної інфраструктури, а рівень окремих організацій – за впровадження процедур управління ризиками у виробничі й інформаційні процеси [37]. Ключовими управлінськими функціями у цій системі є оцінювання ризиків, планування заходів протидії кібертероризму, розподіл відповідальності між суб'єктами, організація обміну інформацією про інциденти, контроль виконання вимог безпеки та коригування заходів з урахуванням змін загрозового середовища [34].

У таблиці 2.4 показано, як основні функції у системі протидії кібертероризму реалізуються центральними органами державної влади,

спеціалізованими службами безпеки, операторами критичної інфраструктури та іншими суб’єктами, які забезпечують експертну, наукову й комунікаційну підтримку.

Таблиця 2.4

Розподіл функцій і відповідальності суб’єктів протидії кібертероризму

Функція у системі протидії кібертероризму	Центральні органи державної влади	Спеціалізовані служби безпеки	Оператори критичної інфра-структури	Інші суб’єкти
1	2	3	4	5
Формування політики і нормативно правової бази	Розроблення законів, стратегій, концепцій, стандартів захисту кіберпростору, затвердження вимог до критичної інфраструктури	Участь у підготовці доктрин і концепцій з урахуванням оперативного досвіду	Надання пропозицій щодо секторальних вимог, участь у консультаціях щодо технічних стандартів	Наукова експертиза проєктів актів, підготовка аналітичних висновків, участь у громадських обговореннях
Стратегічне оцінювання і координація управління ризиками	Визначення пріоритетів, затвердження загальнодержавних програм, координація міжгалузевих заходів	Надання аналітичної інформації про загрози, участь у міжвідомчих координаційних органах	Формування секторальних карт ризиків, узгодження планів заходів із державними органами	Розроблення методик оцінювання ризиків, проведення досліджень щодо тенденцій кібертероризму
Оперативне виявлення та нейтралізація кібертерористичних загроз	Політичне і правове забезпечення проведення спеціальних заходів, міжнародна координація на рівні угод	Виявлення, документування, розслідування та припинення кібертерористичних дій, участь в антитерористичних операціях	Впровадження систем моніторингу, оперативне реагування на інциденти, взаємодія зі службами безпеки	Надання експертної підтримки при інцидентах, участь у розробленні рекомендацій щодо удосконалення практик реагування
Управління технічними й організаційними заходами кіберзахисту	Встановлення мінімальних обов’язкових вимог і контроль їх виконання на рівні держави та секторів	Розроблення рекомендацій щодо тактик протидії, участь у перевірках готовності об’єктів	Організація систем управління інформаційною безпекою, впровадження технічних і процедурних заходів	Адаптація міжнародних стандартів, підготовка методичних матеріалів і програм навчання

Продовження табл. 2.4

1	2	3	4	5
Інформаційна взаємодія, обмін даними про інциденти та просвіта	Створення державних платформ обміну інформацією, комунікація з міжнародними партнерами	Збір, аналіз і передання інформації про кібертерористичні загрози, попередження суб'єктів	Надання даних про інциденти, участь у спільних навчаннях і тренуваннях	Проведення освітніх програм, підвищення обізнаності, сприяння формуванню культури кібербезпеки

Джерело: складено автором на основі [32, 34, 39]

Представлений розподіл функцій показує, що керування ризиками кібертероризму неможливо звести до діяльності одного центру відповідальності: результативність системи визначається узгодженістю політичних, оперативних, технічних та науково експертних компонентів. Чітке окреслення ролей суб'єктів дозволяє знизити дублювання повноважень, підвищити керованість процесів протидії кібертероризму та забезпечити більш повне охоплення ризиків на державному, галузевому й організаційному рівнях.

Внутрішні політики, процедури і стандарти організаційної безпеки формують управлінський каркас протидії кібертероризму на рівні окремої організації, у тому числі оператора критичної інфраструктури. До ключових належать політики управління доступом, резервного копіювання та відновлення, реагування на інциденти, а також регламенти взаємодії підрозділів під час кіберінциденту, які визначають ролі, порядок ескалації, канали комунікації й відповідальність посадових осіб [32, 37, 44–47]. Їх наявність недостатня без регулярного оновлення, практичної перевірки через навчання та аудити, а також прив'язки до вимірюваних показників ефективності.

У таблиці 2.5 наведено аналітичну характеристику основних організаційних заходів протидії кібертероризму на рівні організації з урахуванням цілей, очікуваних результатів, показників оцінювання та типових проблем реалізації.

Таблиця 2.5

Основні організаційні заходи протидії кібертероризму на рівні організації

Організаційний захід	Мета впровадження	Очікуваний результат	Показники оцінювання ефективності	Поточний стан реалізації
1	2	3	4	5
Політика управління доступом	Обмеження доступу до ресурсів за принципом мінімально необхідних повноважень	Зменшення ймовірності несанкціонованого доступу до критичних систем і даних	Частка облікових записів з надлишковими правами; кількість інцидентів, пов'язаних з доступом; результати аудиту прав доступу	Часто формально затверджена, потребує регулярного перегляду, скорочення привілейованих доступів і автоматизації контролю
Політика резервного копіювання та відновлення	Забезпечення збереження даних і відновлення функцій після кібератак і збоїв	Своєчасне відновлення ключових сервісів і критичних даних до прийнятного рівня	Наявність і актуальність планів відновлення; час відновлення; частота тестових відновлень	Наявні базові процедури резервного копіювання, проте тестування відновлення проводиться нерегулярно, документація часто фрагментарна
План реагування на кіберінциденти	Встановлення узгодженого порядку дій підрозділів під час кіберінциденту	Скорочення часу виявлення і локалізації інцидентів, зменшення масштабу наслідків	Час від виявлення до початку реагування; число інцидентів з неконтрольованою ескалацією; результати навчань і тренувань	У більшості організацій існує базовий план, який потребує деталізації сценаріїв, регулярних навчань та перегляду після реальних інцидентів
Регламенти взаємодії підрозділів і ескалації подій	Координація дій IT, підрозділів безпеки, керівництва, юридичної та комунікаційної служб	Зменшення організаційних затримок, узгодженість рішень, контроль наслідків для репутації та юридичного статусу	Чіткість маршрутів ескалації; кількість випадків порушення регламентів; результати післяінцидентного аналізу	Регламенти часто описані загально, потребують конкретизації відповідальності і каналів комунікації, відпрацювання на практичних сценаріях

Продовження табл. 2.5

1	2	3	4	5
Програма підготовки персоналу та підвищення обізнаності	Формування культури кібербезпеки та зниження ризику помилок користувачів	Зменшення випадків фішингових інцидентів, некоректних дій персоналу, що полегшують роботу зловмисників	Частота навчань; результати тестування знань; частка успішних імітацій фішингових атак	Навчання проводиться епізодично, не завжди охоплює всі категорії персоналу, потребує систематизації та актуалізації матеріалів
Впровадження систем управління інформаційною безпекою (на основі стандартів)	Інтеграція технічних і організаційних заходів у єдину систему управління	Структуроване планування заходів, наявність замкненого циклу поліпшення, відповідність стандартам	Наявність сертифікації; результати внутрішніх і зовнішніх аудитів; кількість виявлених і усунених невідповідностей	Частково реалізовано у великих організаціях, у малих суб'єктів практика фрагментарна, переважає реактивний підхід

Джерело: складено автором на основі [44,45,46,47].

Організаційні заходи протидії кібертероризму ефективні лише тоді, коли вони не обмежуються формальними документами, а підкріплені вимірюваними показниками, регулярним аудитом, навчанням персоналу і реальною інтеграцією у щоденну діяльність організації, передусім у секторах критичної інфраструктури.

Підготовка персоналу та формування культури кібербезпеки є ключовою умовою протидії кібертероризму, оскільки значна частина успішних атак реалізується через помилки користувачів, слабку обізнаність та відсутність відпрацьованих алгоритмів дій у разі інциденту. Регулярні навчання, тренінги, моделювання інцидентів і перевірка готовності співробітників до дій у кризових ситуаціях дають змогу зменшити ймовірність реалізації соціотехнічних атак, підвищити якість взаємодії підрозділів та скоротити час реагування на кібертерористичні загрози [37, 39].

Найбільш уразливими залишаються категорії адміністративного та нового персоналу, для яких соціотехнічні атаки та порушення базових правил безпеки є найбільш характерним (табл. 2.6).

Таблиця 2.6

Оцінювання готовності персоналу до дій у разі кібертерористичних загроз

Рівень обізнаності у сфері кібербезпеки	Частота проходження навчань	Типові помилки, виявлені під час тестування	Необхідні коригувальні заходи
Керівництво			
Середній (близько 65% правильних відповідей у тестах)	1 раз на рік	Недооцінка часу реакції на інциденти, плутанина у процедурах ескалації	Цільові сесії щодо управління інцидентами, відпрацювання сценаріїв прийняття рішень
Підрозділи IT та інформаційної безпеки			
Високий (80–85% правильних відповідей)	2–4 рази на рік, участь у спеціалізованих тренінгах	Надмірна технічна зосередженість без достатнього документування дій, перевантаження фахівців	Розвиток навичок документування, розподіл ролей у групах реагування, впровадження ротації обов'язків
Операційний персонал (чергові, диспетчери, оператори систем)			
Середній (55–60% правильних відповідей)	1–2 рази на рік, участь у навчаннях з моделювання інцидентів	Запізніла передача інформації про підозрілі події, неповне заповнення журналів подій	Додаткові тренінги з виявлення аномалій, спрощення інструкцій, чіткі схеми повідомлення
Адміністративний та офісний персонал			
Низький–середній (45–50% правильних відповідей)	Епізодично, переважно онлайн-курси	Високий відсоток переходів за фішинговими посиланнями, використання слабких паролів	Регулярні симуляції фішингових кампаній, обов'язкові курси, політика складних паролів і двофакторної автентифікації
Нові співробітники			
Низький (до 40% правильних відповідей до проходження навчання)	Початковий інструктаж під час прийняття на роботу	Відсутність розуміння процедур повідомлення про інциденти, нехтування правилами використання робочих пристроїв	Введення обов'язкової програми вступного курсу з кібербезпеки, контроль засвоєння матеріалу, наставництво з боку досвідчених співробітників

Джерело: складено автором на основі [45,46,47]

Концентрація зусиль на систематизації навчання, регулярних симуляціях атак і чіткому контролі засвоєння матеріалу дає змогу істотно зменшити ризики кібертерористичних дій, спрямованих на використання людського чинника у структурах, що забезпечують функціонування критичної інфраструктури.

Отже, організаційні та адміністративні заходи протидії кібертероризму формують керовану рамку для інтеграції технічних рішень у практику функціонування державних органів і операторів критичної інфраструктури. Багаторівнева система управління ризиками, чіткий розподіл функцій між суб'єктами, наявність внутрішніх політик і процедур, які реально застосовуються та вимірюються за показниками ефективності, у поєднанні з систематичною підготовкою персоналу і побудовою культури кібербезпеки зменшує вразливість організацій до кібертерористичних дій і підвищує їх здатність до своєчасного виявлення, локалізації та подолання наслідків інцидентів.

2.3 Правові та етичні аспекти забезпечення національної безпеки в кіберсфері

Нормативно правове регулювання протидії кібертероризму формується як багаторівнева система, що включає спеціальні закони у сфері кібербезпеки, акти про боротьбу з тероризмом, стратегії кібербезпеки та підзаконні документи, які конкретизують вимоги до об'єктів критичної інфраструктури. У межах цієї системи визначаються повноваження центральних органів влади, спеціалізованих служб безпеки та регуляторів, а також механізми координації з міжнародними стандартами, насамперед вимогами Європейського Союзу, Сполучених Штатів Америки й Республіки Корея [48, 49].

У таблиці 2.7 подано узагальнену характеристику базових документів України та провідних держав у сфері розвитку інформаційних технологій, із виділенням їхніх положень щодо кібербезпеки, специфічних аспектів кібертероризму та компетентних органів виконання.

Таблиця 2.7

Нормативно правові акти у сфері протидії кібертероризму

Назва акта	Рівень акта	Ключові положення у сфері кібербезпеки	Аспекти, що стосуються кібертероризму	Компетентні органи виконання
1	2	3	4	5
Закон України «Про основні засади забезпечення кібербезпеки України» № 2163 VIII від 05.10.2017	Закон	Визначає суб'єктів національної системи кібербезпеки, порядок захисту критичної інфраструктури, вимоги до кіберзахисту державних інформаційних ресурсів; закріплює механізми обміну інформацією про кіберінциденти	Надає повноваження державним органам щодо виявлення, попередження і нейтралізації дій, що мають ознаки кібертероризму, включаючи атаки на об'єкти критичної інфраструктури	Центральні органи виконавчої влади у сфері кібербезпеки, сектор безпеки і оборони, органи, що координують захист критичної інфраструктури [48; 49]
Закон України «Про боротьбу з тероризмом» № 638 IV від 20.03.2003	Закон	Встановлює правові та організаційні засади протидії тероризму, визначає види терористичної діяльності, повноваження суб'єктів боротьби з тероризмом, процедури проведення антитерористичних операцій	Дозволяє кваліфікувати окремі дії у кіберпросторі як терористичні за умови спрямованості на заподіяння істотної шкоди безпеці держави, життю та здоров'ю населення, об'єктам критичної інфраструктури	Спеціальні служби безпеки, правоохоронні органи, координаційні центри з питань боротьби з тероризмом [49]
Стратегія кібербезпеки України та План її реалізації (Указ Президента № 447/2021, Указ Президента № 37/2022)	Стратегія та акт глави держави	Визначає стратегічні цілі розвитку національної системи кібербезпеки до 2025 року, пріоритети підвищення стійкості державних органів і критичної інфраструктури, завдання щодо розвитку спроможностей реагування	Містить орієнтири щодо протидії кібертероризму через підвищення готовності сектору безпеки і оборони, розбудову національної кіберстійкості та розширення міжнародної кооперації	Рада національної безпеки і оборони України, Кабінет Міністрів України, Національний координаційний центр кібербезпеки, галузеві органи виконавчої влади [48; 53]

Продовження табл. 2.7

1	2	3	4	5
Директива ЄС NIS2 2022/2555 про забезпечення високого рівня кібербезпеки в державах – членах ЄС	Надна-ціональний акт ЄС	Встановлює уніфіковану рамку кібербезпеки для 18 критичних секторів, зобов'язання щодо управління ризиками, вимоги до звітування про інциденти, можливість накладення значних штрафів (до кількох відсотків річного обороту) за невиконання вимог	Передбачає запровадження розширених вимог до стійкості критичної інфраструктури та ланцюгів постачання, що створює додаткові правові механізми для попередження і мінімізації кібертерористичних атак у країнах ЄС і партнерських державах	Європейська комісія, національні компетентні органи кібербезпеки держав – членів ЄС, галузеві регулятори [50]
Законодавчі акти США у сфері кібербезпеки (зокрема Cybersecurity and Infrastructure Security Agency Act, FISMA)	Федеральні закони	Формують правову основу діяльності Агентства з кібербезпеки та безпеки інфраструктури, встановлюють вимоги до захисту федеральних інформаційних систем, інформаційного обміну з приватним сектором і критичною інфраструктурою	Опосередковано регулюють протидію кібертероризму через створення механізмів обміну відомостями про загрози, обов'язкові мінімальні вимоги до захисту об'єктів критичної інфраструктури, спільні заходи реагування	Агентство з кібербезпеки та безпеки інфраструктури, федеральні відомства, регулятори галузей, оператори важливих об'єктів [51]
Акти Республіки Корея у сфері захисту інформаційно комунікаційної інфраструктури (зокрема Act on the Protection of Information and Communications Infrastructure)	Закон та підзаконні акти	Визначають критичну інформаційно комунікаційну інфраструктуру, встановлюють вимоги до її захисту, процедури оцінювання ризиків, аудит безпеки та обов'язки операторів щодо впровадження технічних і організаційних заходів	Охоплюють не тільки загальні кіберзагрози, а й дії, що створюють загрозу національній безпеці, включаючи кібертерористичні атаки проти державних систем та ключових сервісів електронного урядування	Уповноважені органи у сфері цифрової політики, національні регулятори телекомунікацій, оператори критичної інформаційної інфраструктури [52]

Джерело: складено автором на основі [48,49,50,51,52,53]

Українська нормативно правова база вже інтегрує базові міжнародні підходи до протидії кібертероризму, однак порівняння із рамками Європейського Союзу, Сполучених Штатів Америки та Республіки Корея виявляє необхідність подальшої деталізації вимог для окремих секторів критичної інфраструктури, посилення механізмів нагляду й відповідальності, а також розширення інструментів практичної імплементації стратегічних документів у щоденну діяльність компетентних органів і приватних операторів.

Міжнародні стандарти та правові підходи до протидії кібертероризму демонструють, що Україна рухається в єдиному векторі з Європейським Союзом, Сполученими Штатами Америки та Республікою Корея, але різниться ступенем деталізації визначення кібертероризму, секторальною конкретизацією вимог до критичної інфраструктури та рівнем імплементації міжнародних зобов'язань [50].

Для Європейського Союзу характерне комплексне регулювання через NIS2 і CER, що поєднують кібербезпеку і стійкість критичних об'єктів, у США акцент зроблено на широких повноваженнях федеральних органів у межах антитерористичного законодавства, у Південній Кореї – на жорсткій регламентації критичної інформаційно-комунікаційної інфраструктури, тоді як українська модель поєднує спеціальний закон про кібербезпеку, антитерористичне законодавство і стратегії, які поступово наближаються до стандартів Європейського Союзу [55]. Міжнародні зобов'язання, зокрема імплементація вимог NIS2, участь у відповідних конвенціях і партнерських форматах, відіграють роль каталізатора поглиблення правового регулювання протидії кібертероризму та гармонізації національної моделі з практиками провідних держав [56].

У таблиці 2.8 наведено узагальнену характеристику базових актів, підходів до визначення кібертероризму, повноважень компетентних органів і механізмів міжнародної взаємодії, з урахуванням кількісних параметрів там, де вони закріплені (строки повідомлення про інциденти, рівень штрафних санкцій тощо).

Таблиця 2.8

Порівняльна характеристика правових підходів до протидії кібертероризму

Базовий нормативний акт	Підхід до визначення кібертероризму	Повноваження компетентних органів	Механізми міжнародної взаємодії
1	2	3	4
Україна			
Закон України «Про основні засади забезпечення кібербезпеки України»; Закон України «Про боротьбу з тероризмом»; Стратегія кібербезпеки України до 2025 року	Кібертероризм не виділяється як окрема категорія у спеціальному законі, проте дії у кіберпросторі можуть бути кваліфіковані як терористичні, якщо спрямовані на заподіяння значної шкоди національній безпеці, життю та здоров'ю населення або критичній інфраструктурі; у стратегії кібербезпеки окреслено потребу посилення протидії таким діям	Суб'єкти національної системи кібербезпеки та суб'єкти боротьби з тероризмом мають повноваження щодо виявлення, документування, припинення кіберінцидентів, зокрема з ознаками терористичної діяльності; передбачено створення національного центру координації та галузевих центрів; вводиться обов'язок операторів критичної інфраструктури повідомляти про інциденти у визначені строки	Участь у структурах Європейського Союзу та міжнародних ініціативах, імплементація стандартів NIS2, співпраця з НАТО та іншими партнерами у сфері обміну інформацією про загрози і проведення спільних навчань
Європейський Союз			
Директива ЄС 2022/2555 (NIS2); Директива щодо стійкості критичних суб'єктів (CER)	NIS2 не вводить окреме визначення кібертероризму, проте закріплює вимоги щодо управління ризиками для критичних і важливих суб'єктів у 18 секторах, зокрема щодо загроз, які можуть мати терористичний характер; CER прямо фокусується на протидії масштабним загрозам, включаючи терористичні атаки проти критичних суб'єктів	Національні компетентні органи мають повноваження встановлювати обов'язкові вимоги до управління ризиками, проводити нагляд, вимагати усунення порушень і накладати значні штрафи (до 2% річного обороту або фіксовані суми до 10 млн євро для окремих категорій організацій)	Механізми координації в межах Європейського Союзу, мережі компетентних органів, обмін інформацією про інциденти та загрози, спільні практичні навчання, розроблення керівних документів Європейською агенцією з кібербезпеки ENISA

Продовження табл. 2.8

1	2	3	4
Сполучені Штати Америки			
Patriot Act, акти у сфері кібербезпеки, включаючи Cybersecurity and Infrastructure Security Agency Act, інші спеціальні закони	Поняття кібертероризму зазвичай виводиться через розширене тлумачення терористичної діяльності, якщо кіберзасоби застосовуються для спричинення серйозних наслідків; пряма дефініція рідко закріплюється у законодавстві, натомість регулювання здійснюється через комбінацію антитерористичних і кібербезпекових норм	Федеральні органи, включаючи Агентство з кібербезпеки та безпеки інфраструктури, службу безпеки і розвідувальні структури, мають широкі повноваження щодо збору інформації, реагування на загрози, координації захисту критичної інфраструктури; законодавство передбачає обов'язкову співпрацю приватних операторів та державних органів	Розвинуті механізми двосторонньої та багатосторонньої співпраці, участь у міжнародних групах з протидії кіберзлочинності і кібертероризму, обмін технічною інформацією через спеціалізовані платформи, підтримка партнерів у зміцненні кіберстійкості
Республіка Корея			
Act on the Protection of Information and Communications Infrastructure та пов'язане законодавство щодо кібербезпеки	Регулювання зосереджене на захисті критичної інформаційно-комунікаційної інфраструктури, де електронні вторгнення, які ставлять під загрозу стійкість державних сервісів і базових функцій, розглядаються як загроза безпеці держави; питання кібертероризму інтегроване в ширший контекст національної безпеки і захисту критичних інфраструктур	Уповноважені органи мають чітко визначені повноваження щодо класифікації критичних об'єктів, проведення аудитів безпеки, затвердження планів захисту та реагування; оператори зобов'язані регулярно звітувати про стан безпеки та інциденти, виконувати вимоги державних органів, проводити навчання персоналу	Активна участь у регіональних і глобальних ініціативах з кібербезпеки, двосторонні програми з обміну досвідом, участь у міжнародних дослідженнях і розробленні стандартів, спрямованих на захист критичних інформаційних систем

Джерело: складено автором на основі [48–53, 55–57]

Порівняльний аналіз, узагальнений у таблиці 2.8, показує, що, попри різницю у формальних дефініціях і акцентах, правові підходи провідних держав і Європейського Союзу до протидії кібертероризму збігаються у визнанні критичної інфраструктури основним об'єктом захисту, необхідності широких повноважень компетентних органів і важливості інституційованих механізмів

міжнародної взаємодії. Для України стратегічним завданням є не лише подальша гармонізація законодавства з рамками Європейського Союзу, Сполучених Штатів Америки та Республіки Корея, а й підвищення рівня практичної реалізації закріплених норм, у тому числі через чіткі обов'язки операторів, ефективний нагляд і реальне використання міжнародних інструментів співпраці.

Етичні ризики у сфері протидії кібертероризму пов'язані передусім із практиками моніторингу трафіку, тривалого зберігання даних і розширеного доступу до інформації, які, з одного боку, підвищують ефективність виявлення загроз, а з іншого – створюють ризики непропорційного втручання у приватне життя, свободу вираження поглядів та інші права людини [61]. У демократичній правовій державі застосування інструментів кіберзахисту має ґрунтуватися на принципах законності, необхідності й пропорційності, чітких процедурних гарантіях, незалежному нагляді та можливості оскарження рішень, що обмежують права особи [62].

У таблиці 2.9 узагальнено ключові інструменти, потенційні ризики, типові механізми їх зниження та орієнтовну оцінку прийнятності для демократичної правової держави, з урахуванням практики України, Європейського Союзу, Сполучених Штатів Америки та інших держав з розвинутими системами кібербезпеки.

Таблиця 2.9

Етичні ризики застосування інструментів кіберзахисту та можливі запобіжники

Інструмент кіберзахисту	Потенційні ризики для прав людини	Можливі механізми зниження етичних ризиків	Оцінка прийнятності для демократичної правової держави
1	2	3	4
Масштабний моніторинг мережевого трафіку	Розширений нагляд за комунікаціями великої кількості користувачів; ризик перегляду вмісту, що не стосується загроз; імовірність зловживань та профілювання окремих груп населення	Чітке визначення підстав і меж моніторингу в законі; судовий або незалежний дозвільний механізм; технічні обмеження доступу до змісту; регулярний зовнішній аудит	Умовно прийнятний за умови суворого дотримання принципів законності, необхідності та пропорційності, наявності дієвого контролю

Продовження табл. 2.9

1	2	3	4
Зберігання телекому-нікаційних метаданих	Тривале зберігання даних про зв'язки, місцезнаходження і тривалість комунікацій; ризик створення детального профілю поведінки користувачів; можливі витоки або несанкціонований доступ	Скорочення строків зберігання до мінімально необхідних; диференціація строків для різних категорій даних; захист метаданих шифруванням; обмеження доступу для вузького кола уповноважених суб'єктів; обов'язок повідомлення про витоки	Обмежено прийнятний; потребує чіткого обґрунтування необхідності та постійної переоцінки пропорційності, з урахуванням рішень судових інстанцій щодо надмірного зберігання даних
Системи глибокого аналізу пакетів (DPI)	Можливість повного аналізу вмісту трафіку; загроза конфіденційності листування; ризик блокування законного контенту; потенціал для політично мотивованого нагляду	Точкове застосування за виняткових умов; суворі процесуальні гарантії; технічні фільтри для мінімізації обробки надлишкових даних; прозорі звіти про використання DPI у знеособленій формі	Високоризикований інструмент, допустимий лише у вузько окреслених випадках із максимально жорсткими гарантіями та контролем з боку незалежних органів
Централізовані платформи аналізу журналів (SIEM з розширеною кореляцією подій)	Концентрація великого обсягу логів про дії користувачів і адміністраторів; можливість відстеження поведінки конкретних осіб; ризик використання даних поза заявленими цілями	Мінімізація обсягу персональних даних у журналах; застосування псевдонімізації; обмеження доступу до повних профілів; розмежування ролей операторів і аудиторів; чітка фіксація цілей обробки в політиках організації	Загалом прийнятний інструмент за умови дотримання принципів мінімізації даних, прозорості та внутрішнього і зовнішнього аудиту
Автоматизовані системи виявлення аномалій та поведінкової аналітики (з елементами штучного інтелекту)	Ризик упередженості алгоритмів; помилкове віднесення осіб або груп до «підозрілих»; частка хибно позитивних спрацювань може перевищувати 10–15%, що створює додаткові обмеження прав доброчесних осіб	Регулярна оцінка впливу на права людини; тестування моделей на наявність упередженості; встановлення допустимого порогу хибно позитивних спрацьовувань; обов'язкова участь людини в ухваленні рішень із високим впливом	Потенційно прийнятний інструмент за умови поєднання з людським наглядом і проведення постійних етичних та технічних аудитів
Обов'язкове зберігання даних автентифікації та журналів доступу до критичних систем	Ризик несанкціонованого доступу до облікових даних; можливість використання журналів для неконтрольованого спостереження за працівниками; підвищення чутливості до витоків	Шифрування облікових даних і журналів; обмеження строків зберігання; чіткі внутрішні регламенти використання журналів; інформування працівників про обсяг і мету контролю; застосування принципу «need-to-know»	Прийнятний за умови технічного захисту та прозорості щодо обсягу й мети контролю, наявності ефективних засобів оскарження зловживань

Джерело: складено автором на основі [58–64]

Систематизація, подана у таблиці 2.9, показує, що жоден з інструментів кіберзахисту не є нейтральним щодо прав людини: кожен потребує чіткого нормативного врегулювання, технічних обмежень і багаторівневого контролю, які дають змогу зменшити ризики надмірного нагляду, дискримінації та порушення приватності, зберігаючи при цьому спроможність держави та приватних суб'єктів ефективно протидіяти кібертероризму.

Отже, правові та етичні аспекти забезпечення національної безпеки в кіберсфері демонструють, що ефективна протидія кібертероризму неможлива без збалансованого поєднання жорстких вимог до кіберзахисту, чіткої регламентації повноважень компетентних органів і реальних гарантій прав людини. Гармонізація національного законодавства з міжнародними стандартами, прозорі механізми міжнародної взаємодії, процедурні запобіжники від зловживань у сфері моніторингу та зберігання даних, а також етична оцінка застосування технологій на основі штучного інтелекту формують основу моделі, у якій держава посилює спроможність протидіяти кібертероризму без підриву довіри суспільства до інститутів влади.

2.4 Порівняльний аналіз ефективності існуючих підходів та технологій

Критерії оцінювання ефективності механізмів протидії кібертероризму повинні відображати результативність технічних засобів, організаційних рішень і правового регулювання у вимірюваній формі. Доцільно поєднувати кількісні показники (час виявлення і реагування, частка заблокованих інцидентів, охоплення навчанням персоналу, рівень імплементації нормативних вимог) з якісними індикаторами зрілості процесів, що дозволяє порівнювати практику України з підходами Європейського Союзу, Сполучених Штатів Америки і Республіки Корея.

Сформована система критеріїв має бути уніфікованою для різних груп механізмів, але з урахуванням їх специфіки. У таблиці 2.10 наведено приклад структурованої системи оцінювання, де для технічних, організаційних і правових

механізмів визначено критерії, одиниці виміру та орієнтовні бажані й допустимі рівні, які можуть використовуватися для порівняльного аналізу ефективності механізмів протидії кібертероризму в Україні та державах з розвинутими системами кібербезпеки.

Таблиця 2.10

Критерії оцінювання ефективності механізмів протидії кібертероризму

Група механізмів	Критерій оцінювання	Одиниця виміру	Бажаний рівень	Допустимий рівень
1	2	3	4	5
Технічні	Середній час виявлення інциденту	Години	Не більше 1 години	Не більше 24 годин
	Частка інцидентів, заблокованих на ранній стадії	Відсотки	Не менше 80%	Не менше 60%
	Охоплення критичних систем централізованим моніторингом (SIEM, SOC)	Відсотки	Не менше 95%	Не менше 80%
	Частка систем з актуальними оновленнями безпеки	Відсотки	Не менше 95%	Не менше 85%
Організаційні	Частота навчань і тренінгів з кібербезпеки	Рази на рік	Не менше 2	Не менше 1
	Частка персоналу, який пройшов навчання за останні 12 місяців	Відсотки	Не менше 95%	Не менше 80%
	Покриття ключових процесів документованими процедурами реагування	Відсотки	100%	Не менше 85%
	Середній час ескалації інформації про інцидент до керівництва	Хвилини	Не більше 30 хвилин	Не більше 120 хвилин
Правові	Частка секторів критичної інфраструктури з визначеним статусом і вимогами кіберзахисту	Відсотки	100%	Не менше 80%
	Час обов'язкового повідомлення про значущий кіберінцидент компетентним органам	Години	Не більше 24 годин	Не більше 72 годин
	Рівень наближеності національного регулювання до міжнародних стандартів (NIS2, рекомендації ENISA, NIST)	Індекс (0–1)	Не менше 0,8	Не менше 0,6
	Частка перевірених об'єктів критичної інфраструктури, для яких виконано приписи наглядових органів	Відсотки	Не менше 90%	Не менше 70%

Джерело: складено автором на основі [65,66,67]

Структурування критеріїв у таблиці 2.10 показує, що ефективність протидії кібертероризму може бути об’єктивно оцінена лише за умови поєднання технічних, організаційних і правових показників, де кожна група механізмів має чіткі цільові орієнтири та допустимі порогові значення, які дозволяють виявляти відставання, планувати удосконалення та порівнювати національну практику з підходами провідних держав.

Порівняльний аналіз технічних, організаційних і правових механізмів показує, що рівень їхньої ефективності є нерівномірним: технічні засоби у провідних державах демонструють вищу результативність за рахунок розвиненої інфраструктури моніторингу і автоматизації, організаційні механізми істотно залежать від зрілості процесів управління ризиками і культури кібербезпеки, а правові підходи визначають рамкові можливості для координації, нагляду та міжнародної взаємодії. Для України актуальним завданням є поступове наближення фактичних показників до орієнтирів, які вже реалізовано в Європейському Союзі, Сполучених Штатах Америки та Республіці Корея, з урахуванням національних ресурсних обмежень та структури загроз.

У таблиці 2.11 наведено узагальнену характеристику технічних, організаційних і правових механізмів протидії кібертероризму, де інтегральна оцінка подається у вигляді відносного індексу (від 0 до 1) для поточного стану України порівняно з практиками провідних держав.

Таблиця 2.11

Інтегральна оцінка ефективності груп механізмів протидії кібертероризму

Показник	Технічні механізми	Організаційні механізми	Правові механізми
1	2	3	4
Сильні сторони	Базовий захист периметра, системи моніторингу подій безпеки в ключових секторах, розвиток центрів моніторингу безпеки, орієнтація на підходи Європейського Союзу та NIST	Формалізовані структури кібербезпеки у великих організаціях, наявність політик і процедур реагування, висока частка навченого персоналу у критичних секторах	Наявність спеціального закону про кібербезпеку, антитерористичного законодавства, стратегії кібербезпеки, початок гармонізації з NIS2 і практиками Європейського Союзу, формування координаційних інституцій

Продовження табл. 2.11

1	2	3	4
Основні обмеження	Нерівномірне покриття критичної інфраструктури, частка застарілих систем понад 15–20 %, обмежені інвестиції, залежність від імпортних технологій	Наявність повного набору процедур лише у частини суб'єктів, епізодичний характер навчань, слабка культура фіксації та аналізу інцидентів, відмінності між секторами	Неповна імплементація вимог для всіх секторів критичної інфраструктури, обмежені наглядові спроможності, нерівномірне виконання норм, недостатня регламентація кібертероризму як окремого явища
Інтегральна оцінка ефективності (0–1)	0,65	0,55	0,50
Ключові напрями посилення	Прискорення модернізації інфраструктури, розширення автоматизованого виявлення загроз, скорочення часу реагування до рівня практик Європейського Союзу та Сполучених Штатів Америки	Поширення стандартів організаційної безпеки на всі категорії операторів, систематичне й обов'язкове навчання, запровадження вимірюваних показників ефективності управлінських заходів	Розширення секторального регулювання, посилення повноважень і спроможностей наглядових органів, конкретизація вимог щодо протидії кібертероризму та відповідальності операторів

Джерело: складено автором на основі [50,65,66,67]

Технічні механізми вже досягають відносно вищого рівня ефективності порівняно з організаційними та правовими, однак не реалізують потенціал без належної управлінської та нормативної підтримки. Підвищення результативності протидії кібертероризму потребує синхронного посилення всіх трьох груп механізмів, з пріоритетом розвитку організаційної зрілості та поглиблення правового регулювання відповідно до стандартів провідних держав.

Виявлення проблемних зон у сфері протидії кібертероризму показує, що технічні, організаційні та правові механізми розвиваються нерівномірно: частка критичних систем, охоплених сучасним моніторингом, залишається нижчою порівняно з провідними державами, рівень організаційної зрілості та культури

кібербезпеки є неоднорідним між секторами, а імплементація правових вимог і гармонізація з європейськими стандартами все ще не досягають цільових орієнтирів [67]. Для формування рекомендацій у подальшому розділі доцільно запропонувати структурований перелік пріоритетних напрямів посилення системи протидії кібертероризму з оцінкою очікуваного ефекту для національної безпеки та рівня пріоритетності впровадження.

Узагальнення проблемних зон подано у таблиці 2.12, де для ключових технічних, організаційних та правових аспектів відображено поточний стан, рекомендовані напрями удосконалення, очікуваний вплив на стійкість держави до кібертерористичних загроз та орієнтовний рівень пріоритетності у коротко- та середньостроковій перспективі.

Таблиця 2.12

Пріоритетні напрями посилення системи протидії кібертероризму

Проблемна зона	Поточний стан	Рекомендований напрям удосконалення	Очікуваний ефект для національної безпеки	Пріорітет реалізації (1 – найвища, 3 – відкладена)
1	2	3	4	5
Нерівномірне покриття критичної інфраструктури засобами моніторингу та виявлення інцидентів	Охоплення централізованими системами моніторингу оцінюється орієнтовно на рівні 70–80% критичних об'єктів, тоді як у провідних державах цей показник перевищує 90–95%	Розширення інфраструктури центрів моніторингу безпеки, інтеграція додаткових об'єктів, прискорення переходу до цілодобового моніторингу з високим рівнем автоматизації	Зменшення ймовірності непомічених кібертерористичних атак, скорочення часу виявлення інцидентів до рівня менше 1 години для більшості критичних систем	1
Недостатня системність організаційних процедур реагування та ескалації	Документовані процедури реагування повністю охоплюють приблизно 60–70% ключових процесів, навчання персоналу має нерегулярний характер у значній частині організацій	Стандартизація процедур реагування для всіх операторів критичної інфраструктури, запровадження обов'язкових щорічних тренінгів та навчань з моделювання інцидентів для не менше 90–95% персоналу	Підвищення готовності персоналу до дій у разі кібертерористичних загроз, скорочення масштабів наслідків інцидентів завдяки швидкій та узгодженій реакції	1

Продовження табл. 2.12

1	2	3	4	5
Часткова імплементація вимог до кіберзахисту у всіх секторах критичної інфраструктури	Формалізовані вимоги до кіберзахисту повною мірою охоплюють не всі сектори; рівень виконання приписів наглядових органів оцінюється нижче 80%	Розширення секторального регулювання з урахуванням NIS2, посилення механізмів нагляду, встановлення чітких строків усунення порушень і стимулів для виконання вимог	Підвищення загальної стійкості критичної інфраструктури, наближення практик до рівня Європейського Союзу та інших провідних держав, зниження системних ризиків масштабних атак	2
Обмежена інтеграція результатів аналізу ризиків у стратегічне та бюджетне планування	Рішення щодо інвестицій у кібербезпеку не завжди спираються на формалізовані результати оцінювання ризиків, частка проєктів, де ризик-аналіз використовується як основа для обґрунтування, залишається нижчою 50–60%	Інституціалізація ризик-орієнтованого підходу, включення показників кіберризику до стратегічних документів, бюджетних рішень та ключових показників ефективності для керівництва	Оптимізація розподілу ресурсів, зосередження інвестицій на найбільш ризикових ділянках, зниження ймовірності критичних інцидентів при обмежених ресурсах	2
Недостатньо розвинуті механізми міжнародної практичної взаємодії у сфері протидії кібертероризму	Участь у міжнародних ініціативах зростає, проте частка спільних навчань, обмінів технічною інформацією та спільних проєктів ще не відповідає рівню провідних держав	Активізація участі у міжнародних платформах обміну інформацією про загрози, розширення практики спільних навчань та тренувань, розвиток двосторонніх проєктів з профільними агентствами інших держав	Зменшення часу отримання інформації про нові методи кібертероризму, доступ до найкращих практик, підвищення стійкості завдяки колективній безпеці	3

Джерело: складено автором на основі [50, 65, 66, 67]

Отже, першочерговими є завдання розширення технічної інфраструктури моніторингу та підвищення організаційної готовності персоналу, тоді як правові та міжнародні аспекти потребують послідовного посилення у середньостроковій перспективі, що створить основу для комплексної системи протидії кібертероризму з узгодженим розвитком усіх складових.

Для отримання експертної оцінки використано метод анкетування. Проведено анкетування 35 експертів з кібербезпеки, які працюють у підрозділах інформаційної безпеки операторів критичної інфраструктури енергетичного та телекомунікаційного секторів України, в акціонерному товаристві «НЕК «Укренерго» та суміжних організаціях (табл. 2.13). Анкета містила 15 запитань, об'єднаних у три блоки: оцінювання рівня загроз і готовності, організаційно-правові механізми протидії та технічні й ресурсні аспекти захисту. Відповіді подавалися за трибальною шкалою (1 – низький або незадовільний стан, 2 – середній, 3 – високий рівень зрілості), що дало змогу розрахувати середні оцінки та частку експертів, які обрали домінуючу відповідь (Додаток А).

Таблиця 2.13

Результати анкетування експертів з кібербезпеки

Коротке формулювання питання	Домінуюча відповідь (якісна оцінка)	Частка респондентів, %	Середній бал (1–3)	Опис
1	2	3	4	5
Блок І. Загрози і готовність				
Актуальність кібертерористичних загроз	Висока, з тенденцією до зростання	71,4	2,71	Експерти очікують посилення загроз у найближчі роки.
Відповідність стану кіберзахисту умовам війни	Часткова відповідність, значні прогалини	62,9	2,03	Система захисту не встигає за динамікою загроз.
Узгодженість дій операторів	Взаємодія переважно ситуативна	57,1	1,86	Відсутність сталих процедур спільного реагування.
Готовність керівництва до кризових рішень	Обмежена, з елементами імпровізації	60,0	1,94	Потреба в залученні керівництва до навчань і тренувань.
Вплив загроз на безперервність послуг	Ймовірні тривалі збої при складних атаках	54,3	2,11	Ризик порушення безперервності залишається підвищеним.

Продовження табл. 2.13

1	2	3	4	5
Блок II. Організаційні та правові механізми				
Чіткість розподілу відповідальності	Ролі визначені частково	65,7	2,09	Формалізація відповідальності неповна, існують «сірі зони».
Якість внутрішніх політик	Частково оновлені, є застарілі елементи	68,6	2,00	Оновлення документів відстає від зміни загроз.
Достатність національної нормативної бази	Основи є, проте з прогалинами	74,3	2,03	Потрібна деталізація вимог та механізмів контролю.
Інтеграція кібертероризму у ризик-менеджмент	Враховується нерегулярно	60,0	1,97	Немає системної переоцінки ризиків з урахуванням війни.
Формалізація взаємодії з державними органами	Частково регламентована	62,9	2,06	Взаємодія опирається на поєднання протоколів і неформальних контактів.
Блок III. Технічні та ресурсні аспекти				
Захищеність АСУ ТП	Захист частковий, з уразливими каналами доступу	71,4	1,97	АСУ ТП залишаються одним з найуразливіших сегментів.
Повнота моніторингу подій безпеки	Моніторинг охоплює не всі сегменти	68,6	2,00	Недостатня повнота охоплення критичних зон.
Підготовка персоналу	Тренінги епізодичні, навички нерівномірні	77,1	1,89	Персонал потребує системної підготовки за сценаріями атак.
Достатність фінансування	Переважно базовий рівень без запасу	65,7	1,80	Фінансування обмежує можливості модернізації.
Якість технічної інфраструктури	Частково модернізована, наявні застарілі елементи	71,4	1,94	Структурні обмеження уповільнюють впровадження сучасних рішень.

Джерело: складено автором

Отримані результати свідчать, що експерти розглядають кібертероризм як загрозу з тенденцією до посилення, тоді як поточний рівень готовності критичної інфраструктури оцінюється лише як частково відповідний умовам війни.

Найнижчі середні оцінки отримав блок технічних і ресурсних аспектів, що відображає системний дефіцит фінансування, підготовки персоналу та модернізації АСУ ТП (рис. 2.1).

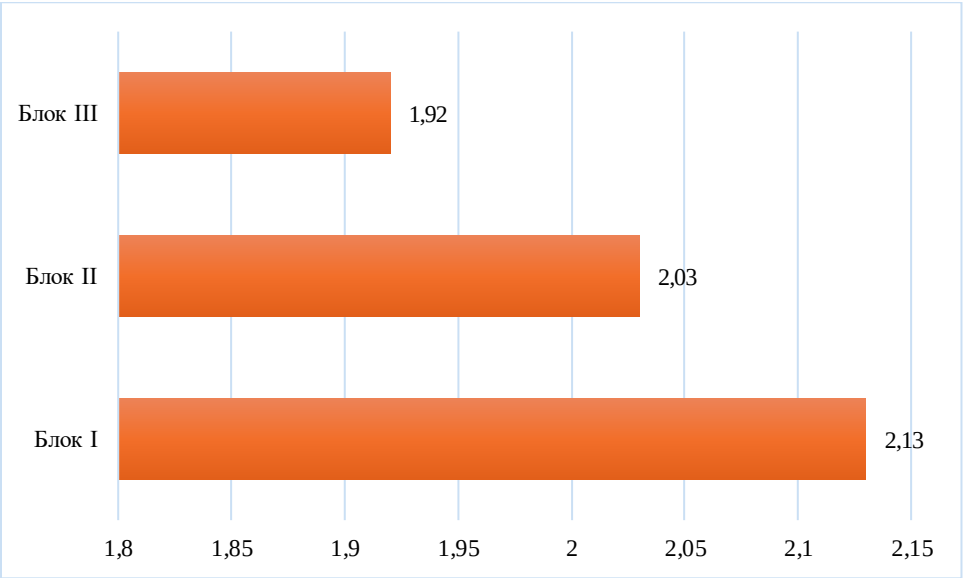

Рис. 2.1 Діаграма результатів анкетування експертів (бали)

Джерело: побудовано автором

Організаційно-правові механізми протидії загалом сформовані, проте мають прогалини у деталізації ролей, процедур взаємодії та інтеграції кібертероризму у ризик-менеджмент. Найбільш проблемними сферами є технічний стан АСУ ТП, повнота моніторингу, системність навчання та достатність фінансування, що підтверджує потребу у пріоритетному інвестуванні саме в ці елементи комплексної системи протидії.

Контент-аналіз проведено для 18 внутрішніх політик та регламентів кібербезпеки семи операторів критичної інфраструктури України (енергетика, телекомунікації, транспорт і фінансовий сектор). Оцінювалися ключові напрями регулювання: класифікація активів і критичності, управління ризиками, моніторинг і реєстрація подій, управління інцидентами, безперервність діяльності, взаємодія з державними органами та підготовка персоналу. Для кожного напряму визначена частка документів, у яких вимога відображена повністю, частково або відсутня (табл. 2.14).

Таблиця 2.14

Результати контент-аналізу внутрішніх політик і регламентів захисту критичної інфраструктури

Напрям регулювання	Повне відображення вимоги, %	Часткове відображення, %	Відсутність відображення, %	Аналітичний висновок
Класифікація активів та рівнів критичності	44,4	38,9	16,7	Класифікація активів є наявною, але не у всіх операторів формалізована до рівня, необхідного для пріоритизації захисту.
Управління ризиками кібертероризму	33,3	44,4	22,3	Ризик-менеджмент прописаний нерівномірно, кібертероризм часто розглядається у загальних формулюваннях без деталізованих процедур.
Моніторинг і реєстрація подій безпеки	55,6	33,3	11,1	Технічні аспекти моніторингу описані відносно краще, проте не завжди доповнені вимогами до зберігання та аналізу журналів подій.
Управління інцидентами та ескалація	38,9	44,4	16,7	Процедури реагування на інциденти здебільшого наявні, але механізми ескалації і взаємодії під час комплексних атак описані стисло.
Забезпечення безперервності діяльності	27,8	44,4	27,8	Питання безперервності часто винесені в окремі документи, однак не завжди інтегровані з регламентами кібербезпеки.
Взаємодія з державними органами і регуляторами	22,2	50,0	27,8	Формалізація каналів обміну інформацією та порядку повідомлення про інциденти є недостатньою, переважають загальні декларації.
Підготовка та навчання персоналу	16,7	50,0	33,3	Навчання здебільшого згадується формально, конкретні програми, періодичність і сценарії тренувань описані рідко.

Джерело: складено автором

Контент-аналіз демонструє, що внутрішні політики операторів критичної інфраструктури більшою мірою охоплюють технічні аспекти моніторингу та реєстрації подій, тоді як управління ризиками кібертероризму, безперервність діяльності та взаємодія з державними органами описані фрагментарно. Питання класифікації активів і критичності у частини операторів формалізовані, однак у значній кількості документів відсутні чіткі критерії, які можна використовувати для пріоритизації інвестицій у захист. Особливо слабкою виявилася регламентація системного навчання персоналу: третина документів взагалі не містить конкретних вимог до програм підготовки, а у половині випадків це обмежується загальними формулюваннями без визначеної періодичності та сценаріїв.

У підсумку результати контент-аналізу підтверджують висновки анкетування: внутрішня нормативна база операторів критичної інфраструктури створює загальний каркас захисту, проте не забезпечує достатньої глибини опрацювання ризиків кібертероризму, безперервності діяльності та підготовки персоналу. Це формує потребу у розробці типових регламентів, галузевих стандартів і методичних рекомендацій, які деталізують вимоги до класифікації активів, ризик-менеджменту, процедур реагування, взаємодії з державними органами та системної підготовки співробітників.

Висновки до Розділу 2

Результати аналізу сучасних технічних механізмів протидії кібертероризму показують, що IDS, IPS, SIEM, SOC та рішення на основі методів штучного інтелекту формують базовий каркас захисту критичної інфраструктури, але ефективність цих засобів обмежується нерівномірним охопленням об’єктів, збереженням частки застарілих систем і недостатнім рівнем автоматизації процесів виявлення й реагування. Технічний контур захисту демонструє потенціал наближення до практик провідних держав за умови цілеспрямованої

модернізації, інтеграції інструментів моніторингу та скорочення залежності від ручних операцій.

Організаційні та адміністративні заходи виявляються ключовим чинником, який визначає, чи перетворюються технічні можливості на реальну стійкість до кібертероризму. Наявність формалізованих політик, процедур реагування, системи розподілу функцій і відповідальності, регулярних навчань та перевірок готовності персоналу підвищує рівень захищеності, проте неповне охоплення суб'єктів, формальний характер частини документів і нерегулярність тренінгів знижують ефективність організаційної реакції на складні кіберінциденти.

Правові та етичні аспекти забезпечення національної безпеки в кіберсфері відображають потребу одночасно посилювати регуляторні вимоги до захисту критичної інфраструктури і підтримувати гарантії прав людини. Українська модель поступово наближається до підходів Європейського Союзу, Сполучених Штатів Америки та Республіки Корея, проте вимагає подальшої деталізації вимог до операторів критичної інфраструктури, зміцнення наглядових спроможностей компетентних органів та інституційних механізмів оцінювання етичних ризиків при застосуванні інструментів моніторингу, зберігання даних і систем аналізу поведінки.

Порівняльний аналіз існуючих підходів і технологій засвідчує, що реальна стійкість до кібертероризму формується лише за умови узгодженого розвитку технічних, організаційних і правових механізмів з виразним етичним компонентом. Результати анкетування 35 експертів з кібербезпеки засвідчили, що технічні засоби оцінюються ними відносно вище, ніж організаційні та ресурсні аспекти, проте залишаються суттєві прогалини у захищеності АСУ ТП, повноті моніторингу та підготовці персоналу. Контент-аналіз 18 внутрішніх політик і регламентів операторів критичної інфраструктури України виявив фрагментарність регулювання ризиків кібертероризму, безперервності діяльності, взаємодії з державними органами та системного навчання працівників. Отримані емпіричні результати підтвердили, що формальна наявність документів і технічних рішень не гарантує стійкості без глибокої

інтеграції вимог кібербезпеки у управлінські процеси. Технічні засоби отримують відносно вищі інтегральні оцінки, але не реалізують потенціал без зрілих управлінських процесів та цілісної правової рамки. Пріоритетними напрямами удосконалення стають розширення інфраструктури моніторингу критичної інфраструктури, стандартизація процедур управління інцидентами, систематичне навчання персоналу, поглиблення імплементації міжнародних стандартів і впровадження стійких механізмів етичного контролю за застосуванням інструментів кіберзахисту.

РОЗДІЛ 3
РОЗРОБКА КОМПЛЕКСНИХ МЕХАНІЗМІВ ПРОТИДІЇ КІБЕРТЕРОРИЗМУ

3.1 Постановка завдань та принципи системного підходу до протидії кібертероризму

Кібертероризм формує багаторівневу загрозу національній безпеці, оскільки поєднує руйнівний вплив на інформаційні ресурси, системи управління, фінансову та енергетичну інфраструктуру, а також на суспільну стабільність. У цих умовах система протидії кібертероризму має розглядатися як цілісна підсистема національної безпеки, орієнтована на попередження, виявлення, нейтралізацію та мінімізацію наслідків кібертерористичних впливів.

Стратегічною метою системи протидії кібертероризму є формування стійкої, скоординованої та ресурсно забезпеченої моделі захисту, яка гарантує безперервне функціонування критичної інфраструктури, збереження керованості держави та захист прав і свобод громадян від кібертерористичних загроз.

Така мета має бути узгоджена з базовими компонентами національної безпеки, включаючи інформаційну, військову, економічну, енергетичну, техногенну та соціальну безпеку, через чітко визначені цілі та вимірювані показники.

Формулювання стратегічної мети потребує її проєкції на окремі компоненти національної безпеки, для яких кібертероризм формує специфічні ризики й виклики. Відповідність цілей системи протидії кібертероризму структурним складовим національної безпеки подано в табл. 3.1. Наведена таблиця відображає, що стратегічна мета системи протидії кібертероризму набуває практичного змісту лише за умови її розкладання на цілі для окремих компонентів національної безпеки з чітко окресленими очікуваними результатами та вимірюваними показниками.

Таблиця 3.1

Відповідність цілей системи протидії кібертероризму компонентам національної безпеки

Компонент національної безпеки	Ціль системи протидії кібертероризму	Очікуваний результат реалізації цілі	Орієнтовні показники досягнення
Інформаційна безпека	Зниження вразливості державних інформаційних ресурсів та систем критичної інфраструктури до кібертерористичних атак	Стійке функціонування інформаційно-комунікаційних систем, своєчасне виявлення та блокування спроб кібертерористичного втручання	Частка інцидентів, що локалізуються на ранній стадії; середній час виявлення інцидентів; частка об'єктів з цілодобовим моніторингом подій безпеки
Військова безпека	Забезпечення захищеності систем управління оборонними ресурсами та військовою інфраструктурою від кібертерористичних впливів	Підтримання боєздатності та керованості сил оборони за умов масованих кібератак, збереження конфіденційності й цілісності інформації	Частота успішного проходження навчань з кіберзахисту; частка захищених сегментів військових мереж; кількість критичних збоїв, спричинених кібератаками
Економічна безпека	Захист платіжних систем, фінансових ринків та електронних сервісів від кібертерористичних посягань	Збереження стабільності фінансової системи, мінімізація економічних втрат від кібертерористичної діяльності	Обсяг прямих і непрямих збитків від кіберінцидентів; частота збоїв у роботі фінансових сервісів; рівень покриття сектору стандартизованими засобами кіберзахисту
Енергетична та техногенна безпека	Підвищення стійкості енергетичних об'єктів і техногенно небезпечних об'єктів до кібертерористичних загроз	Безперервність постачання енергоресурсів, запобігання аваріям техногенного характеру, спричиненим кібервпливами	Частка об'єктів енергетики з впровадженими системами кіберзахисту; кількість інцидентів, що призвели до переривання постачання; рівень готовності до реагування на кібератаки
Соціальна безпека та громадська безпека	Недопущення дестабілізації суспільства через кібертерористичні атаки на медіапростір, медичні системи, об'єкти життєзабезпечення	Підтримання суспільної стабільності, збереження доступу населення до ключових послуг, мінімізація панічних настроїв	Рівень доступності електронних публічних сервісів; кількість масових збоїв у системах охорони здоров'я та життєзабезпечення; оцінки довіри населення до цифрових сервісів держави

Джерело: складено автором

Такий підхід формує підґрунтя для подальшого планування завдань, вибору інструментів і побудови комплексної моделі протидії кібертерористичним загрозам.

Реалізація стратегічної мети протидії кібертероризму потребує її розкладання на узгоджені завдання для різних рівнів управління. Стратегічний рівень формує довгострокові орієнтири розвитку системи, оперативний рівень забезпечує координацію суб'єктів та організацію процесів, тактичний рівень відповідає за безпосереднє реагування, експлуатацію засобів захисту і підтримання готовності персоналу.

Визначення завдань на кожному рівні має спиратися на очікувані результати, які можуть бути виміряні через зміну стану захищеності інформаційних систем, критичної інфраструктури і рівня ризику кібертерористичних загроз.

Для впорядкування завдань на стратегічному, оперативному та тактичному рівнях, а також фіксації зв'язку між ними й очікуваними результатами формування комплексних механізмів протидії кібертероризму, доцільно використати структуроване подання (табл. 3.2).

Таблиця 3.2

Декомпозиція завдань системи протидії кібертероризму за рівнями управління

Рівень управління	Завдання	Інструменти реалізації	Відповідальні суб'єкти	Очікуваний результат
1	2	3	4	5
Стратегічний	Визначення довгострокової політики протидії кібертероризму, затвердження національної стратегії кібербезпеки, формування цільових програм захисту критичної інфраструктури	Стратегія кібербезпеки держави, державні цільові програми, концепції розвитку кіберзахисту, міжвідомчі координаційні органи, єдині стандарти і вимоги до захисту критичної інфраструктури	Законодавчий орган, уряд, Рада національної безпеки і оборони, центральні органи виконавчої влади у сфері безпеки та цифровізації	Зменшення системної вразливості держави до кібертероризму, формування інтегрованої системи управління ризиками, стабільне та прогнозоване ресурсне забезпечення заходів протидії

Продовження табл. 3.2

1	2	3	4	5
Оперативний	Організація галузевих систем моніторингу і реагування, запровадження процедур управління інцидентами, координація взаємодії суб'єктів у разі кібертерористичних загроз	Галузеві плани протидії кібертероризму, регламенти обміну інформацією про інциденти, ситуаційні та моніторингові центри, навчання і тренування міжвідомчих груп, внутрішні положення про реагування	Галузеві міністерства і відомства, національні регулятори, служби безпеки, керівництво суб'єктів критичної інфраструктури	Скорочення часу виявлення і реагування на кіберінциденти, підвищення частки локалізованих загроз, налагоджена взаємодія між державними органами, операторами критичної інфраструктури і силами безпеки
Тактичний	Налаштування і експлуатація засобів технічного захисту, ведення моніторингу подій безпеки, виконання процедур реагування та відновлення, підготовка і інструктаж персоналу	Комплекси технічного захисту інформації, системи виявлення і запобігання вторгненням, журнали подій, плани безперервності діяльності, інструкції та чек-листи реагування, навчальні програми і тренінги	Підрозділи інформаційної безпеки підприємств, адміністратори інформаційних систем, оператори центрів моніторингу, групи швидкого реагування на інциденти	Зменшення кількості успішних атак, скорочення тривалості простоїв систем, підвищення готовності персоналу до дій у разі кібертерористичних загроз, стабільне функціонування інформаційних і технологічних процесів

Джерело: складено автором

Узагальнення завдань за рівнями управління демонструє, що ефективна система протидії кібертероризму спирається на взаємодоповнювані рішення: стратегічні документи та програми, організаційні механізми координації і щоденну практику технічного та процедурного захисту.

Принципи системного підходу формують рамку для проєктування комплексних механізмів протидії кібертероризму. Принцип цілісності вимагає розглядати систему протидії як єдину конструкцію, де технічні, організаційні і

правові рішення взаємодіють, а не існують ізольовано. Принцип узгодженості передбачає чітке стикування повноважень, відповідальності і процедур між державними органами, суб'єктами критичної інфраструктури і структурами безпеки, що усуває дублювання функцій і прогалини у реагуванні.

Принцип безперервності орієнтує проєктування механізмів на постійний моніторинг, регулярне оновлення засобів захисту і підтримання готовності персоналу, а не на разові заходи. Принцип адаптивності вимагає включення у модель гнучких процедур оновлення політик, сценаріїв реагування і технічних конфігурацій відповідно до еволюції кібертерористичних загроз. Принцип ресурсної достатності означає, що проєктні рішення мають супроводжуватися реалістичними розрахунками фінансових, кадрових, технічних та інформаційних потреб, а також визначенням пріоритетів, щоб система була не лише концептуально коректною, а й виконуваною у практиці.

Отже, стратегічна мета системи протидії кібертероризму полягає у формуванні стійкої моделі захисту критичної інфраструктури через узгоджене виконання завдань на стратегічному, оперативному і тактичному рівнях на основі принципів цілісності, узгодженості, безперервності, адаптивності і ресурсної достатності, що забезпечує перехід від декларативних цілей до конкретних керованих змін у стані кіберзахищеності держави.

3.2 Модель комплексної системи захисту критичної інфраструктури від кібертерористичних загроз

Загальна архітектура моделі комплексної системи захисту критичної інфраструктури ґрунтується на трирівневій побудові. Національний рівень формує політику, нормативно-правові засади, єдині вимоги до кіберзахисту критичної інфраструктури, координує діяльність спеціалізованих органів, ситуаційних центрів та центрів реагування на комп'ютерні інциденти. Галузевий рівень відповідає за адаптацію національних рішень до умов конкретного сектору, організацію галузевих центрів моніторингу, розробку планів протидії

кібертероризму, методичну підтримку суб'єктів критичної інфраструктури у відповідній сфері. Рівень суб'єкта критичної інфраструктури охоплює внутрішні політики безпеки, системи моніторингу й реагування, технічні засоби захисту, процедури управління інцидентами та підготовку персоналу.

Взаємозв'язки між рівнями ґрунтуються на рухові керівних і інформаційних потоків у двох напрямках. Згори вниз передаються стратегічні цілі, обов'язкові вимоги, стандарти, регламенти взаємодії та ресурси підтримки, що визначають рамки функціонування галузевих структур і суб'єктів критичної інфраструктури. Знизу вгору надходить інформація про інциденти, вразливості, результати аудиту, показники ефективності заходів, що дозволяє коригувати політику, уточнювати пріоритети та оновлювати модель з урахуванням реальної динаміки кібертерористичних загроз.

У межах розробки моделі комплексної системи захисту критичної інфраструктури доцільно формалізувати функціональне наповнення кожного рівня. Це дає можливість чітко визначити роль учасників, характер інформаційних потоків і набір інструментів, які закладаються у проєктну архітектуру. Узгодженість цих елементів забезпечує керованість моделі і її придатність до практичної реалізації (табл. 3.3).

Таблиця 3.3

Структурні рівні моделі комплексної системи захисту критичної інфраструктури

Рівень моделі	Основні функції	Ключові суб'єкти	Інформаційні потоки	Інструменти реалізації
1	2	3	4	5
Національний	Формування політики протидії кібертероризму, визначення обов'язкових вимог до кіберзахисту критичної інфраструктури, координація діяльності органів безпеки і регуляторів, розподіл ресурсів	Вищі органи державної влади, органи сектора безпеки і оборони, центральні органи виконавчої влади, національні регулятори	Збір узагальненої інформації про інциденти, ризики і вразливості від галузевих структур; передача стратегічних рішень, стандартів, методик і ресурсів вниз	Національна стратегія кібербезпеки, державні цільові програми, міжвідомчі координаційні платформи, нормативно-правові акти, єдині стандарти кіберзахисту

Продовження табл. 3.3

1	2	3	4	5
Галузевий	Адаптація національної політики до особливостей конкретного сектору, організація галузевих центрів моніторингу, методичний супровід суб'єктів критичної інфраструктури, координація реагування у межах галузі	Профільні міністерства, галузеві регулятори, об'єднання операторів критичної інфраструктури, галузеві центри реагування на інциденти	Отримання від суб'єктів деталізованих даних про інциденти і стан захисту; передача галузевих планів реагування, методичних рекомендацій, консолідованих звітів на національний рівень	Галузеві плани протидії кібертероризму, регламенти інформаційного обміну, галузеві ситуаційні центри, методичні документи, програми галузевого навчання
Рівень суб'єкта критичної інфраструктури	Впровадження і експлуатація систем технічного та організаційного захисту, моніторинг подій безпеки, управління інцидентами, підготовка персоналу, забезпечення безперервності функціонування об'єкта	Керівництво суб'єкта, підрозділи інформаційної безпеки, технічні служби, служби експлуатації, внутрішні групи реагування на інциденти	Надання звітів про події, вразливості і ефективність заходів на галузевий рівень; отримання інструкцій, сценаріїв реагування, вимог до модернізації систем	Системи моніторингу і виявлення атак, засоби технічного захисту, внутрішні регламенти з кібербезпеки, плани безперервності діяльності, програми навчання персоналу, внутрішні аудити безпеки

Джерело: складено автором

Розроблена модель комплексної системи захисту критичної інфраструктури спирається на чіткий розподіл функцій та інструментів між національним, галузевим рівнем і рівнем суб'єкта критичної інфраструктури. Національний рівень концентрує нормативно-стратегічні рішення і ресурсну підтримку, галузевий рівень виконує роль проміжної ланки адаптації політики і координації, а рівень суб'єкта забезпечує практичну реалізацію захисних заходів та постійний моніторинг (рис. 3.1).

На рисунку відображено три рівні моделі (національний, галузевий, рівень суб'єкта критичної інфраструктури), між якими організовано вертикальні керівні та інформаційні потоки.

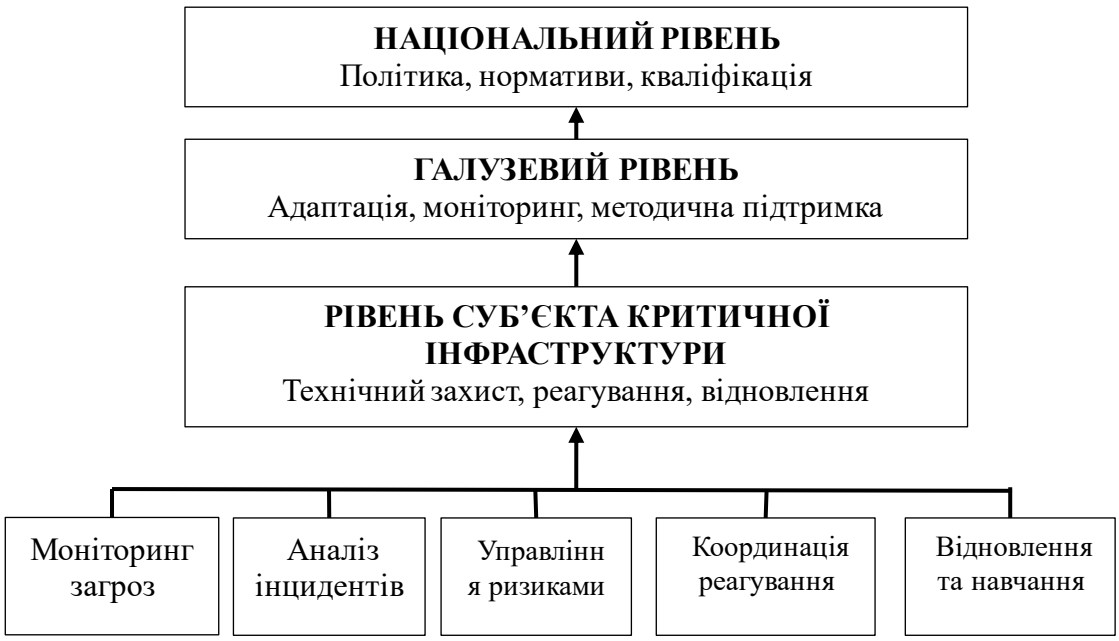

Рис. 3.1. Схема моделі комплексної системи протидії кібертероризму

Джерело: побудовано автором

Така побудова демонструє, що практична реалізація моделі ґрунтується на поєднанні управлінських рівнів та функціональних модулів у єдину конструкцію.

Функціональна архітектура розробленої моделі комплексної системи захисту критичної інфраструктури України передбачає виокремлення низки взаємопов'язаних модулів. Кожний модуль охоплює завершений цикл дій – від отримання вхідної інформації до формування керівних рішень та практичних результатів. Такий підхід особливо важливий в умовах війни, коли інтенсивність кібертерористичних атак зростає, а помилки у координації можуть мати критичні наслідки (табл. 3.4). Модель комплексної системи захисту критичної інфраструктури опирається на послідовний ланцюг модулів, де моніторинг загроз, аналіз інцидентів і управління ризиками формують інформаційну основу для координації реагування, а блок відновлення та навчання забезпечує замкнене коло постійного удосконалення.

Таблиця 3.4

Функціональні модулі комплексної системи захисту та їх характеристика

Назва модуля	Основні функції	Вхідна інформація	Вихідна інформація	Відповідальні виконавці
1	2	3	4	5
Моніторинг загроз	Безперервний збір, кореляція і фільтрація подій безпеки, раннє виявлення ознак кібертерористичних атак, формування сповіщень про інциденти	Журнали подій, телеметрія з об’єктів критичної інфраструктури, повідомлення від національних і галузевих центрів реагування на комп’ютерні інциденти, дані розвідки у кіберпросторі	Сповіщення про підозрілі події, попередні індикатори атак, аналітичні зведення про активність загроз	Національні і галузеві центри моніторингу, центри реагування на комп’ютерні інциденти, підрозділи інформаційної безпеки суб’єктів критичної інфраструктури
Аналіз інцидентів	Класифікація кіберінцидентів, встановлення причин і каналів атаки, оцінка масштабів наслідків, напрацювання технічних і організаційних висновків	Сповіщення з модуля моніторингу, технічні артефакти інцидентів, журнали доступу, свідчення персоналу, результати внутрішніх перевірок	Звіти про інциденти, висновки щодо використаних вразливостей, рекомендації з блокування і локалізації, індикатори компрометації для подальшого моніторингу	Аналітичні підрозділи центрів реагування на інциденти, служби інформаційної безпеки, технічні фахівці суб’єктів критичної інфраструктури
Управління ризиками	Ідентифікація і оцінювання ризиків кібертероризму, ранжування активів, визначення пріоритетів захисних заходів з урахуванням воєнного стану	Дані про активи і процеси, результати аналізу інцидентів, аудити безпеки, сценарії загроз, вимоги національних і галузевих регуляторів	Карти ризиків, переліки пріоритетних заходів, обґрунтування потреб у ресурсах, вимоги до модернізації інфраструктури	Підрозділи управління ризиками в державних органах і на об’єктах критичної інфраструктури, галузеві регулятори, служби безпеки
Координація реагування	Узгодження дій суб’єктів різних рівнів, формування і запуск сценаріїв реагування, управління кризовими ситуаціями, у тому числі за умов комбінованих воєнних та кібернетичних загроз	Оповіщення про інциденти, плани реагування, рішення кризових штабів, інформація від сил оборони і правоохоронних органів	Розпорядження і сигнали управління для виконавців, узгоджені сценарії дій, публічні та службові комунікаційні повідомлення	Координаційні органи національного рівня, галузеві ситуаційні центри, кризові штаби, керівництво суб’єктів критичної інфраструктури

Продовження таблиці 3.4

1	2	3	4	5
Відновлення та навчання	Відновлення працездатності систем, документування отриманого досвіду, оновлення регламентів, планування і проведення навчань та тренувань	Плани безперервності діяльності, журнали інцидентів, звіти аналізу, оцінки ефективності реагування, інформація про збої під час війни	Відновлені сервіси, оновлені процедури і інструкції, плани модернізації, програми підготовки персоналу, звіти про навчання	Керівництво об'єктів, служби експлуатації, підрозділи інформаційної безпеки, навчальні центри органів безпеки і галузевих структур

Джерело: складено автором

Інтеграція технічних, організаційних і правових механізмів у розробленій моделі комплексної системи захисту критичної інфраструктури передбачає, що технічні рішення (системи моніторингу, виявлення і блокування атак) проєктуються і впроваджуються у строгій відповідності до управлінських процедур і правових вимог, закріплених у національних стратегіях, законах та підзаконних актах України. Управлінські регламенти визначають порядок взаємодії суб'єктів, розподіл відповідальності, алгоритми реагування і відновлення, а правове підґрунтя фіксує обов'язковість виконання цих процедур, вимоги до захисту критичної інфраструктури, режим обміну інформацією про інциденти. З позицій практичної реалізації це створює в Україні цілісну рамку, у межах якої технічні засоби не існують як ізольовані рішення, а вбудовуються у керовані процеси, що можна масштабувати і перевіряти, що важливо для апробації моделі на реальних об'єктах у воєнних умовах.

3.3 Розробка рекомендацій щодо впровадження механізмів протидії на практиці

План впровадження розробленої комплексної системи протидії кібертероризму доцільно будувати як послідовність чотирьох етапів:

підготовчого, пілотного, етапу розгортання і етапу оптимізації. Підготовчий етап охоплює нормативно-організаційне налаштування системи, визначення відповідальних суб'єктів, формування ресурсної бази та уточнення пріоритетів, що особливо важливо для України в умовах війни, коли обсяг загроз і обмеження ресурсів є підвищеними. Пілотний етап передбачає апробацію моделі на обмеженій групі об'єктів критичної інфраструктури, відпрацювання процедур, перевірку працездатності модулів моніторингу, реагування та відновлення у реальних умовах.

Етап розгортання орієнтується на масштабування рішень, поширення напрацьованих підходів на інші об'єкти та галузі, поетапне підключення до національних і галузевих центрів моніторингу, формування стабільної практики обміну інформацією про кібертерористичні загрози. Етап оптимізації зосереджується на вдосконаленні процедур, уточненні ризиків, модернізації технічних засобів, системному аналізі інцидентів і результатів навчань, що дає можливість підтримувати працездатність моделі у довгостроковому періоді і коригувати її з урахуванням зміни характеру війни та кібертерористичних атак.

Для конкретизації логіки впровадження комплексної системи протидії кібертероризму пропонується план, структурований за ключовими етапами, змістом робіт та відповідальними суб'єктами (табл. 3.5).

Таблиця 3.5

Етапи впровадження комплексної системи протидії кібертероризму

Зміст робіт	Відповідальні суб'єкти	Орієнтовні строки реалізації	Очікуваний проміжний результат
1	2	3	4
Етап 1. Підготовчий			
Аналіз стану кіберзахисту критичної інфраструктури, деталізація моделі для умов України, розробка проєктів нормативно-правових актів, затвердження концепції впровадження, формування міжвідомчих координаційних механізмів, попереднє планування ресурсів	Вищі органи державної влади, Рада національної безпеки і оборони, профільні міністерства, національні регулятори, органи сектора безпеки і оборони	6–12 місяців	Затверджена концепція і план впровадження, визначені відповідальні органи і ролі, сформована нормативна та організаційна основа для запуску системи

Продовження табл. 3.5

1	2	3	4
Етап 2. Пілотний			
Вибір пріоритетних об’єктів критичної інфраструктури, впровадження модулів моніторингу, аналізу інцидентів і управління ризиками на пілотних об’єктах, налаштування інформаційних потоків з національними і галузевими центрами, проведення навчань і сценарних тренувань з урахуванням воєнних загроз	Галузеві міністерства, галузеві регулятори, керівництво відібраних об’єктів, центри реагування на комп’ютерні інциденти, підрозділи інформаційної безпеки	12–18 місяців	Перевірена на практиці модель взаємодії, відпрацьовані процедури реагування, отримані дані про ефективність рішень, скориговані регламенти та вимоги
Етап 3. Розгортання			
Поширення рішень, відпрацьованих на пілоті, на ширше коло об’єктів і галузей, поетапне підключення нових суб’єктів до систем моніторингу і обміну інформацією, розгортання інфраструктури підтримки, масштабні навчання, інтеграція з системами управління військовими та цивільними операціями	Профільні міністерства, галузеві об’єднання, керівництво суб’єктів критичної інфраструктури, національні та галузеві центри моніторингу, органи сектора безпеки і оборони	18–36 місяців	Створена функціонуюча мережа суб’єктів, що працюють за єдиними принципами, суттєве скорочення часу виявлення та реагування, підвищення стійкості критичної інфраструктури до кібертерористичних атак
Етап 4. Оптимізація			
Оцінювання результатів, поглиблений аналіз інцидентів, ревізія карт ризиків, модернізація технічних засобів, удосконалення регламентів і навчальних програм, закріплення сталих процедур у стандартних операційних регламентах, інтеграція нових технологічних рішень	Національні регулятори, галузеві органи управління, керівництво суб’єктів критичної інфраструктури, наукові й експертні установи, навчальні центри	Після 36 місяців, постійний процес	Стабільне функціонування комплексної системи, підвищення її адаптивності, формування культури кібербезпеки, можливість гнучкого реагування на нові форми кібертероризму у тривалому періоді

Джерело: складено автором

Запропонований план впровадження демонструє, що розроблена система протидії кібертероризму не є разовим проєктом, а розгортається як поетапний процес із чіткими проміжними результатами.

Ефективне впровадження розробленої комплексної системи протидії кібертероризму в Україні потребує збалансованого поєднання фінансових, кадрових, технічних та інформаційних ресурсів. В умовах війни особливого значення набуває раціональний розподіл обмежених ресурсів, концентрація інвестицій на об'єктах і процесах з найвищим рівнем ризику, а також поетапність фінансування. Оцінювання мінімально необхідних ресурсів має спиратися на реалістичні можливості державного бюджету, міжнародної підтримки та потенціал приватного сектору критичної інфраструктури.

Для практичної реалізації моделі потрібна формалізація основних видів ресурсів і їх очікуваного обсягу на етапах запуску та підтримання системи. Структурування ресурсних потреб дає можливість зіставити амбіції проєкту з наявними і потенційними джерелами фінансування, виявити «вузькі місця» та визначити пріоритети. У табл. 3.6 подано узагальнений перелік ключових ресурсів, орієнтовні витрати та характерні обмеження для українських умов воєнного часу.

Таблиця 3.6

Ресурсні потреби для впровадження комплексної системи протидії кібертероризму

Вид ресурсу	Необхідний обсяг	Джерело забезпечення	Орієнтовні витрати	Потенційні обмеження
1	2	3	4	5
Фінансові ресурси	Формування багаторічного бюджету на розробку, пілотне впровадження і розгортання системи, резервування коштів на модернізацію та аварійні потреби	Державний бюджет, цільові фонди безпеки, міжнародна технічна допомога, внесок операторів критичної інфраструктури	Високі початкові капітальні витрати, подальші щорічні експлуатаційні витрати	Обмеженість бюджетних ресурсів у воєнний період, конкуренція з іншими пріоритетами оборони і відновлення, залежність від зовнішнього фінансування

Продовження табл. 3.6

1	2	3	4	5
Кадрові ресурси	Команди аналітиків, фахівців з інформаційної безпеки, адміністраторів систем, інструкторів і науково-експертних груп для супроводу моделі	Підрозділи державних органів, спеціалізовані служби безпеки, IT-підрозділи операторів критичної інфраструктури, профільні заклади освіти	Витрати на підготовку, перепідготовку, заробітну плату та утримання високо-кваліфікованого персоналу	Дефіцит фахівців у воєнних умовах, кадрова міграція, ризик вигорання персоналу, конкуренція з приватним сектором і оборонною сферою
Технічні ресурси	Системи моніторингу, засоби виявлення і запобігання атакам, криптографічний захист, серверна і мережна інфраструктура, резервні майданчики	Інфраструктура державних органів, ресурси операторів критичної інфраструктури, спільні платформи, проєкти міжнародної допомоги	Значні капітальні витрати на закупівлю та інтеграцію, видатки на обслуговування, оновлення і ліцензування	Обмеження імпорту обладнання, залежність від іноземних постачальників, складність інтеграції з наявними системами, ризик фізичного ураження об’єктів
Інформаційні та аналітичні ресурси	Бази даних про активи і вразливості, сховища журналів подій, знання про загрози, типові сценарії атак, методичні матеріали	Державні реєстри, внутрішні системи обліку операторів, центри реагування на інциденти, наукові та експертні структури	Витрати на створення і підтримання репозитаріїв, аналітичних платформ, інструментів візуалізації і звітності	Обмеження доступу до чутливої інформації, нерівномірна якість даних, необхідність узгодження форматів і протоколів обміну
Організаційно-правові ресурси	Нормативні акти, стандарти, регламенти взаємодії, типові договори, механізми координації та контролю виконання вимог	Законодавчий орган, уряд, регулятори, міжвідомчі комісії, профільні експертні ради	Витрати на розробку і супровід нормативної бази, проведення консультацій, створення структур координації	Тривалість процедур ухвалення рішень, можливий опір окремих стейкхолдерів, потреба у постійному оновленні документів відповідно до умов війни і розвитку технологій

Джерело: складено автором

Поєднання високих витрат, дефіциту фахівців і технологічних залежностей формує ресурсний ризик, який вимагає пріоритизації інвестицій і активного залучення міжнародної підтримки.

Розроблені організаційні та методичні рекомендації передбачають створення у суб'єктів критичної інфраструктури внутрішніх регламентів, які детально описують порядок моніторингу, реагування, обміну інформацією та відновлення з урахуванням воєнних ризиків, а також запровадження навчальних програм і тренувань, інтегрованих у систему підготовки персоналу. Протоколи взаємодії мають встановлювати чіткі канали і часові рамки обміну даними між державними органами, галузевими структурами і операторами об'єктів, визначати відповідальних осіб та ескалаційні маршрути у разі кібертерористичних інцидентів.

Запропонована система організаційних та методичних заходів посилює координацію між учасниками системи протидії кібертероризму в Україні, забезпечує узгодженість дій у критичних ситуаціях і перетворює модель, що розробляється, на практичний інструмент управління безпекою в умовах війни.

3.4 Апробація моделі на умовному кейсі

У межах апробації моделі розглядається умовний, наближений до реального, оператор регіональної енергетичної мережі України, який забезпечує електропостачання для близько 1,2 млн споживачів і має розгалужену систему підстанцій та диспетчерських пунктів. Початковий стан кіберзахисту характеризується наявністю базових засобів технічного захисту і фрагментарно формалізованих процедур реагування, що не повністю відповідає вимогам воєнного часу, коли комбінуються фізичні ураження інфраструктури та цілеспрямовані кібератаки на автоматизовані системи управління.

Для подальшого моделювання доцільно формалізувати ключові параметри стану кіберзахисту об'єкта, його вразливості та рівні ризику кібертерористичних загроз. У табл. 3.7 подано вихідні характеристики, які використовуються як

вхідні дані для оцінювання ефективності розробленої моделі комплексної системи захисту.

Таблиця 3.7

Вихідні характеристики об’єкта для апробації моделі

Параметр об’єкта	Поточний стан	Ідентифіковані вразливості	Рівень ризику кібер-терористичних загроз	Опис
1	2	3	4	5
Організаційна система управління кібербезпекою	Відсутня окрема служба кібербезпеки, функції розподілені між IT-підрозділом та службою охорони праці	Нечіткий розподіл відповідальності, відсутність регулярних аудитів, нерегулярне оновлення внутрішніх регламентів	0,75 (високий)	Передбачити створення окремого підрозділу або принаймні виділення відповідальних осіб, запровадити регулярні аудити і оновлення документів
Мережна інфраструктура офісного сегмента	Часткова сегментація мережі, використання змішаних за віком і класом мережних пристроїв	Недостатня сегментація, застаріле обладнання, обмежені можливості журналювання і кореляції подій	0,70 (високий)	У моделі закласти посилення сегментації, оновлення обладнання та інтеграцію з модулем моніторингу загроз
Автоматизовані системи управління технологічними процесами (АСУ ТП)	Використання промислових контролерів, частина каналів дистанційного доступу налаштована без повноцінного моніторингу	Слабка ізоляція АСУ ТП від офісної мережі, можливість несанкціонованого доступу через віддалені підключення, обмежений контроль змін конфігурацій	0,85 (дуже високий)	Передбачити жорстке розмежування мереж, багатофакторний доступ, посилений контроль змін і пріоритетну інтеграцію АСУ ТП у систему управління ризиками
Інформаційні системи обліку споживачів і розрахунків	Функціонують на базі кількох прикладних систем, резервне копіювання здійснюється нерегулярно	Ризик втрати або викривлення даних, відсутність повної схеми резервування, низький рівень шифрування архівів	0,65 (середньо-високий)	У моделюванні закласти впорядкування політики резервування, посилення захисту даних і контроль доступу до критичних масивів

Продовження таблиці 3.7

1	2	3	4	5
Підготовка і обізнаність персоналу	Були разові короткі інструктажі, відсутні повноцінні навчальні програми щодо кібертероризму	Низька спроможність виявляти соціотехнічні атаки, ризик помилкових дій під час інцидентів, відсутність навичок роботи за сценаріями	0,70 (високий)	Передбачити модуль навчання і тренувань, у тому числі з використанням сценаріїв воєнних та комбінованих атак
Взаємодія з державними органами та галузевими центрами	Передача інформації про інциденти здійснюється епізодично, відсутня відпрацьована процедура взаємодії у кризових ситуаціях	Затримки в ескалації, ризик неконсистентної інформації, обмежена участь у спільних навчаннях і тренуваннях	0,60 (середній)	У моделі закласти формалізовані протоколи взаємодії, визначення контактних осіб, участь у спільних навчаннях з органами безпеки

Джерело: складено автором

Наведені вихідні характеристики демонструють, що найуразливішими елементами об’єкта є АСУ ТП, організаційна система управління кібербезпекою та підготовка персоналу, де рівень ризику сягає 0,70–0,85. Це обґрунтовує пріоритетність саме цих напрямів під час апробації розробленої моделі, оскільки їх посилення може дати найбільший ефект з погляду зниження загального ризику кібертерористичних впливів.

Орієнтовні показники бюджету сформовано для чотирьох етапів моделі: підготовчого, пілотного, етапу розгортання та етапу оптимізації. Вихідною базою є структура ресурсних потреб (технічна інфраструктура, програмні засоби, навчання персоналу, організаційно-правове забезпечення, резервний фонд), адаптована до масштабу оператора регіональної енергетичної мережі у воєнних умовах. Сумарний бюджет відображає не лише початкові капітальні інвестиції, а й потребу у резерві на непередбачені витрати, пов’язані з пошкодженням

інфраструктури, збоєм постачання обладнання, додатковими навчальними циклами.

Формули для розрахунку бюджету:

1. Сума витрат за етапом

$$B_{\text{етап}} = \sum_{i=1}^{n} b_i \qquad (3.1)$$

де b_i– витрати за окремою статтею (технічна інфраструктура, програмні засоби, навчання, організаційно-правове забезпечення, резервний фонд), $B_{\text{етап}}$– загальна сума витрат за етапом.

2. Загальний бюджет проєкту

$$B_{\text{заг}} = \sum_{j=1}^{m} B_{\text{етап}_j} \qquad (3.2)$$

де m– кількість етапів впровадження моделі.

Таблиця 3.8

Орієнтовний бюджет впровадження моделі комплексної системи протидії кібертероризму, млн грн

Показник	Підготовчий	Пілотний	Розгортання	Оптимізація	Разом
Технічна інфраструктура	40	60	120	30	250
Програмні засоби і ліцензії	10	20	35	15	80
Навчання персоналу	5	10	15	10	40
Організаційно-правове забезпечення	8	5	5	4	22
Резервний фонд	7	10	15	6	38
Разом	70	105	190	65	430

Джерело: складено автором

Підготовчий і пілотний етапи потребують відносно менших, але критичних інвестицій у організаційно-правову базу та перші хвилі навчання. Резервний фонд становить умовно 38 млн грн і виконує роль фінансового буфера в умовах війни, що знижує ризик зупинки проєкту через непередбачені обставини.

Календарний план реалізації моделі демонструє поетапний перехід від аналітико-підготовчих робіт до повномасштабного розгортання та подальшої оптимізації системи протидії кібертероризму протягом чотирьох років (табл. 3.9).

Таблиця 3.9

Календарний план реалізації етапів впровадження моделі

Етап	Початок (рік-місяць)	Завершення (рік-місяць)	Тривалість, місяців	Коротка характеристика змісту робіт
Підготовчий	2026-03	2026-12	10	Аналіз вихідного стану, деталізація моделі, розробка нормативних документів, формування координаційних структур
Пілотний	2027-01	2027-12	12	Вибір пілотних об’єктів, впровадження модулів моніторингу і реагування, відпрацювання протоколів, перша хвиля навчань персоналу
Розгортання	2028-01	2028-12	12	Масштабування рішень на всі основні об’єкти, інтеграція з національними і галузевими центрами, розширення технічної інфраструктури
Оптимізація	2029-01	2029-12	12	Оцінка результатів, коригування карт ризиків, модернізація засобів захисту, закріплення постійних регламентів і програм навчання

Джерело: складено автором

Логіка послідовності етапів дає змогу спочатку сформувати нормативно-організаційну базу і протестувати рішення на обмеженій кількості пілотних об’єктів, а потім забезпечити масштабування технічної інфраструктури та інтеграцію з національними і галузевими центрами (рис. 3.2). Завершальний етап зосереджений на оцінюванні результатів, коригуванні ризик-профілів та інституціоналізації постійних регламентів і програм навчання, що перетворює

модель на довгостроковий інструмент управління кібербезпекою критичної інфраструктури.

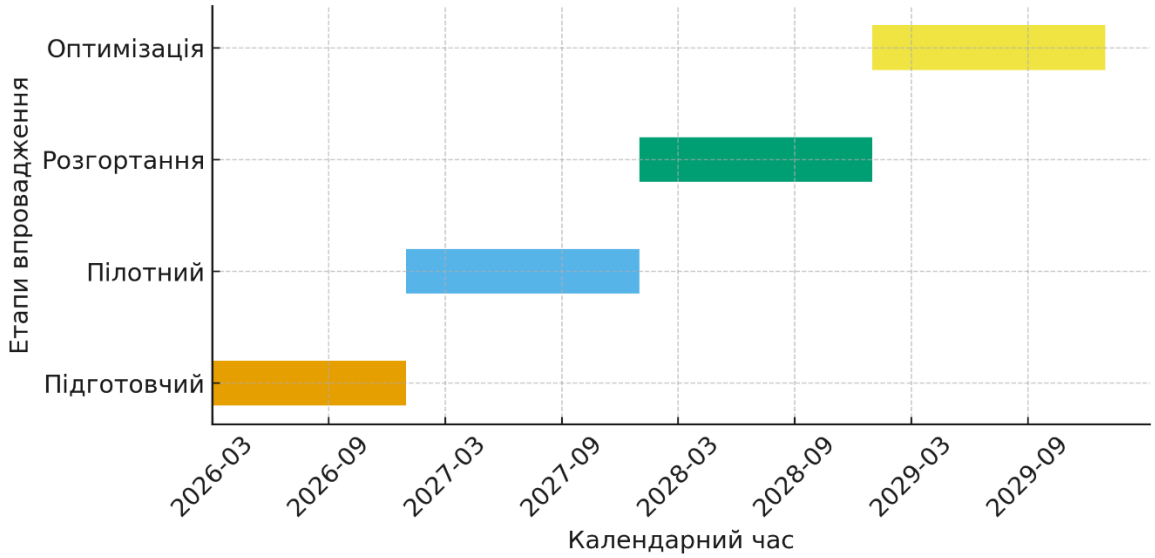

Рис. 3.2 Діаграма Ганта етапів впровадження моделі комплексної системи протидії кібертероризму

Джерело: побудовано автором

Підготовчий етап створює базу для пілотного, результати пілотного етапу забезпечують обґрунтоване розгортання, а оптимізація перетворює модель на постійно діючу систему. Така структура відповідає вимогам до проєктів у сфері безпеки у воєнних умовах і дозволяє планувати фінансування та кадрове забезпечення з урахуванням багаторічного горизонту

Вихідні показники стану до впровадження моделі сформовано на основі умовно усереднених даних за попередній рік роботи оператора енергетичної мережі: журнали інцидентів, звіти підрозділів інформаційної безпеки, дані диспетчерських служб та результати внутрішніх аудитів.

Показники після впровадження моделі відображають стан через умовно один рік роботи за новими регламентами, з урахуванням повноцінного запуску модулів моніторингу, аналізу інцидентів, управління ризиками, координації реагування та відновлення (табл. 3.10).

Таблиця 3.10

Порівняльна динаміка ключових показників функціонування оператора енергетичної мережі

Показник	Значення до	Значення після	Абсолютна зміна	Відносна зміна, %
Середній час виявлення інциденту, годин	12,0	2,5	−9,5	−79,2
Середній час реагування до локалізації, годин	8,0	3,0	−5,0	−62,5
Частка сегментів АСУ ТП у моніторингу, відсотків	40,0	85,0	+45,0	+112,5
Кількість успішних атак на критичні системи, випадків на рік	6,0	2,0	−4,0	−66,7
Інтегральний індекс ризику кібертерористичних загроз (0–1)	0,78	0,46	−0,32	−41,0
Коефіцієнт доступності ключових сервісів	0,965	0,985	+0,020	+2,1
Частка персоналу з навчанням з кібербезпеки, відсотків	25,0	80,0	+55,0	+220,0

Джерело: складено автором

Найбільший відносний ефект досягається у підвищенні покриття моніторингом АСУ ТП та підготовці персоналу, де збільшення перевищує 100%. Одночасно різко скорочується час виявлення і реагування та кількість успішних атак, що безпосередньо знижує інтегральний індекс ризику приблизно на 41%. Невелике, але відчутне зростання коефіцієнта доступності сервісів відображає реальний системний результат для споживачів у воєнних умовах.

Для деталізації ефекту моделі доцільно окремо оцінити ризики за ключовими підсистемами: організаційне управління, мережна інфраструктура,

АСУ ТП, інформаційні системи, персонал, взаємодія з державними органами (табл. 3.11).

Таблиця 3.11

Інтегральна оцінка ризиків основних підсистем до і після впровадження моделі

Підсистема	Рівень ризику до	Рівень ризику після	Абсолютне зниження	Зниження, %
Організаційна система управління кібербезпекою	0,75	0,45	−0,30	−40,0
Мережна інфраструктура офісного сегмента	0,70	0,42	−0,28	−40,0
Автоматизовані системи управління технологічними процесами	0,85	0,50	−0,35	−41,2
Інформаційні системи обліку споживачів і розрахунків	0,65	0,40	−0,25	−38,5
Підготовка і обізнаність персоналу	0,70	0,43	−0,27	−38,6
Взаємодія з державними органами та галузевими центрами	0,60	0,38	−0,22	−36,7

Джерело: складено автором

Відносно збалансоване зниження ризику по всіх підсистемах на 36–41 %, що свідчить про комплексний характер впливу моделі, а не про точкові покращення. Найбільше зниження фіксується для АСУ ТП і організаційної системи управління, що відповідає вибраним пріоритетам на етапі впровадження. Залишкові значення ризику демонструють, що навіть після реалізації моделі повне усунення загроз неможливе, однак ризики переходять у керовану зону.

На діаграмі видно, що всі підсистеми зміщуються до нижчих рівнів ризику, однак АСУ ТП навіть після зниження залишаються у групі підвищеної уваги. Організаційна система і мережна інфраструктура демонструють суттєве зниження ризику, що підтверджує значення управлінських і технічних змін (рис. 3.3).

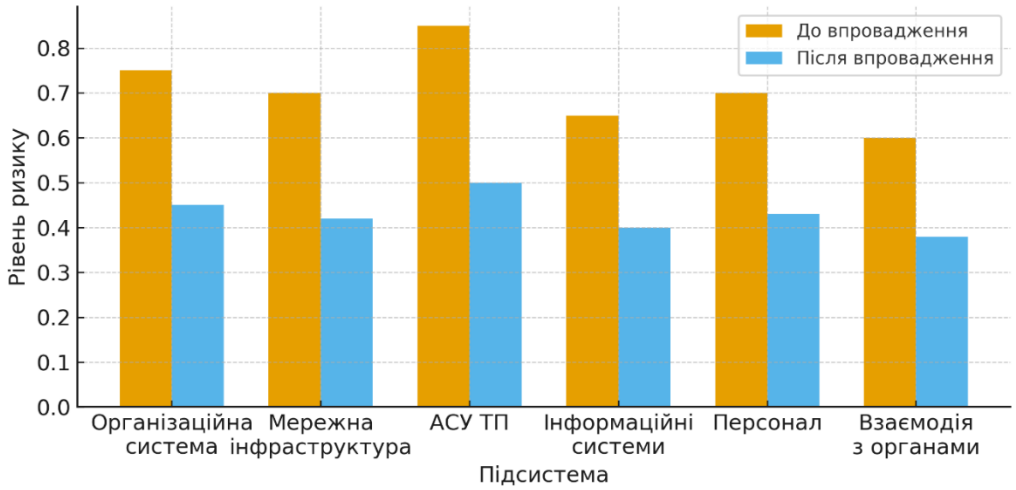

Рис. 3.3 Діаграма ризиків підсистем (бал)

Джерело: побудовано автором

Взаємодія з органами та підготовка персоналу покращуються, але потребують подальшої підтримки, щоб утримати досягнутий рівень у тривалому періоді.

Матриця ризиків формалізує поєднання ймовірності та тяжкості наслідків для ключових груп загроз, характерних для оператора енергетичної мережі у воєнних умовах (табл. 3.12).

Таблиця 3.12

Матриця оцінювання ризиків кібертерористичних загроз

Група загроз	Ймовірність (1–5)	Тяжкість наслідків (1–5)	Інтегральний бал ризику	Зона ризику
1	2	3	4	5
Атаки на АСУ ТП	5	5	25	Критична
Проникнення в офісну мережу	4	4	16	Висока
Порушення цілісності баз даних споживачів	3	4	12	Висока

Продовження табл. 3.12

1	2	3	4	5
Соціотехнічні атаки на персонал	4	3	12	Висока
Збої у взаємодії з державними органами	3	3	9	Середня

Джерело: складено автором

Матриця демонструє, що найбільш критичною загрозою є атаки на АСУ ТП, де поєднуються максимальні ймовірність і наслідки. Група високих ризиків включає атаки на офісну мережу, соціотехнічні впливи і порушення цілісності баз даних, що потребує постійного посилення технічних і організаційних заходів (рис. 3.4).

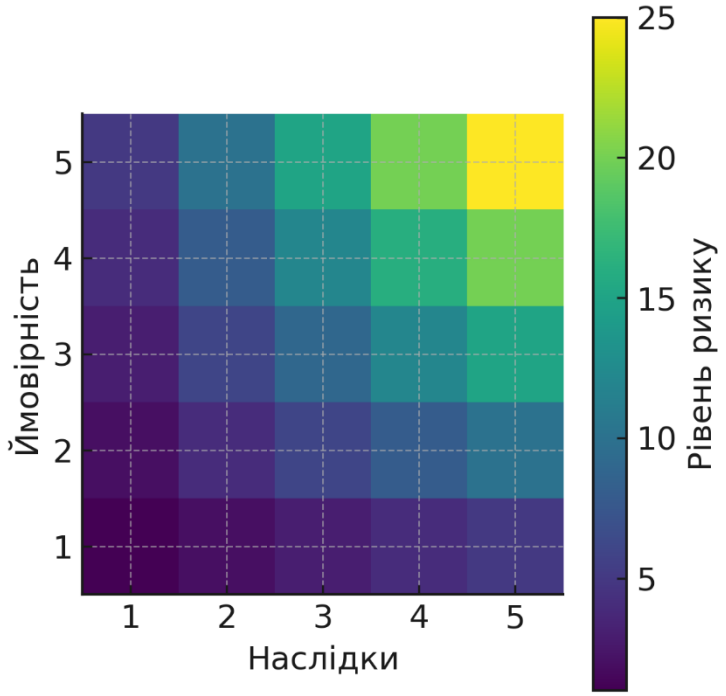

Рис. 3.4 Карта ризиків кібертерористичних загроз

Джерело: побудовано автором

Загрози, пов’язані зі збоями у взаємодії з державними органами, залишаються у середній зоні, однак у воєнних умовах їх ігнорування може накопичувати системні ефекти.

Результати апробації демонструють, що розроблена модель комплексної системи протидії кібертероризму забезпечує помітне скорочення часу виявлення та локалізації інцидентів, зниження інтегрального рівня ризику й кількості успішних атак, підвищення доступності ключових сервісів і рівня підготовки персоналу. Сильна сторона моделі полягає у поєднанні багаторівневої архітектури (національний, галузевий, рівень суб'єкта критичної інфраструктури) з функціональними модулями, що утворюють замкнений цикл управління загрозами – від моніторингу до відновлення та навчання. Це створює керовану, масштабовану конструкцію, придатну для поетапного розгортання в енергетичному секторі та на інших об'єктах критичної інфраструктури України.

Модель має низку обмежень, пов'язаних із високою ресурсомісткістю, залежністю від кадрового потенціалу, технологічних постачальників і стійкості державних інституцій у воєнних умовах. Подальший розвиток моделі доцільно спрямувати на поглиблення аналітичних можливостей управління ризиками, розширення сценарного моделювання комбінованих атак, інтеграцію результатів апробації в галузеві стандарти, посилення участі наукових і експертних центрів.

Перспективним напрямом є створення єдиних методичних платформ для навчання персоналу та обміну практикою між операторами критичної інфраструктури, що дасть змогу перетворити модель на динамічну систему, здатну адаптуватися до розвитку кібертерористичних загроз у довгостроковому періоді.

Висновки до розділу 3

Модель проєктного підходу до протидії кібертероризму у третьому розділі визначає стратегічну мету системи, передбачає декомпозицію завдань на стратегічному, оперативному та тактичному рівнях і ґрунтується на принципах цілісності, узгодженості, безперервності, адаптивності та ресурсної достатності. Така побудова формує логічну рамку, у якій протидія кібертерористичним

загрозам розглядається як керована система, поєднана з цілями національної безпеки і захисту критичної інфраструктури України в умовах війни.

Розроблена модель комплексної системи захисту критичної інфраструктури описує багаторівневу архітектуру з чітким розподілом функцій між національним, галузевим рівнями та рівнем суб'єкта, а також виділяє п'ять ключових модулів: моніторинг загроз, аналіз інцидентів, управління ризиками, координація реагування, відновлення та навчання. Інтеграція технічних, організаційних і правових механізмів у межах цієї моделі формує керовану конструкцію, яку можна адаптувати до різних секторів критичної інфраструктури і масштабувати за єдиними принципами.

Проєктні рекомендації щодо впровадження моделі включають поетапний план реалізації (підготовчий, пілотний, розгортання, оптимізація), ресурсне забезпечення із деталізацією фінансових, кадрових, технічних, інформаційних та організаційно-правових потреб, а також комплекс організаційних і методичних рішень. Запропоновані внутрішні регламенти, програми навчання, протоколи взаємодії та діаграма Ганта перетворюють модель на інструмент практичного управління, що дає змогу планувати обсяги інвестицій, строки реалізації та очікувані результати в розрізі етапів.

Визначені сильні сторони моделі (комплексність, багаторівневість, орієнтація на цикл «моніторинг – реагування – відновлення – навчання») поєднуються з окресленими обмеженнями, пов'язаними з ресурсомісткістю та залежністю від кадрового й інституційного потенціалу. Це створює підґрунтя для подальшого поглиблення аналітичних модулів, розвитку сценарного моделювання комбінованих загроз і оновлення галузевих стандартів кібербезпеки критичної інфраструктури України.

ВИСНОВКИ

Розглянуто сутність кібертероризму як політично та ідеологічно вмотивованої діяльності з використанням інформаційно-комунікаційних технологій, спрямованої на дестабілізацію роботи критичної інфраструктури, органів влади та суспільства. Визначено його вплив на ключові компоненти національної безпеки та відмежовано кібертероризм від кіберзлочинності, кіберрозвідки й кібервоєнних дій за мотивацією, об'єктами посягання і масштабом наслідків.

Охарактеризовано класифікацію кібертерористичних загроз і атак за джерелом походження, об'єктами впливу, рівнем координації та очікуваними ефектами, а також виокремлено стратегічні, операційні та інформаційно-психологічні загрози. Показано, що систематизація типів атак, етапів ескалації та технічних форм реалізації створює основу для побудови моделей ризику, пріоритизації ресурсів кіберзахисту і проєктування механізмів раннього виявлення.

Досліджено міжнародні стандарти та нормативно-правову базу протидії кібертероризму, включно з рамкою NIST Cybersecurity Framework, рекомендаціями ENISA та законодавством України у сфері кібербезпеки, боротьби з тероризмом і захисту критичної інфраструктури. Узагальнено, що українська система загалом узгоджується з ризик орієнтованими міжнародними підходами, проте потребує подальшої деталізації секторальних вимог, процедур оцінювання кіберризиків і механізмів практичної імплементації.

Розглянуто роль державних органів, операторів критичної інфраструктури й приватного сектору у формуванні стійкої системи протидії кібертероризму та підкреслено значення публічно-приватного партнерства й міжнародної координації. Показано, що поєднання нормотворчих, координаційних, оперативних, аналітичних функцій і взаємодії з бізнесом формує інституційне підґрунтя для реалізації комплексних механізмів запобігання, виявлення та нейтралізації кібертерористичних загроз.

Проаналізовано сучасні технічні методи захисту критичної інфраструктури, встановлено їх місце у багаторівневій архітектурі кібербезпеки: IDS/IPS забезпечують фільтрацію та блокування атак на периметрі, SIEM і SOC формують централізований моніторинг інцидентів, а методи штучного інтелекту і машинного навчання підсилюють можливості виявлення складних і нових загроз.

Встановлено, що результативність протидії кібертероризму істотно залежить від організаційних та адміністративних заходів: розподілу функцій між державними органами, спеціальними службами безпеки й операторами критичної інфраструктури, наявності внутрішніх політик та процедур реагування, а також систематичної підготовки персоналу і послідовного формування культури кібербезпеки.

Сформовано уявлення про правові та етичні засади забезпечення національної безпеки в кіберсфері, показано узгодженість української моделі з підходами Європейського Союзу, Сполучених Штатів Америки та Республіки Корея, а також окреслено потребу подальшої гармонізації законодавства, посилення наглядових механізмів і впровадження запобіжників для захисту прав людини під час застосування інструментів кіберзахисту.

Проведено порівняльний аналіз ефективності технічних, організаційних і правових механізмів протидії кібертероризму, який засвідчив відносно вищий рівень розвитку технічних рішень порівняно з організаційною зрілістю та правовим забезпеченням; на цій основі визначено пріоритетні напрями посилення системи, передусім розширення інфраструктури моніторингу, стандартизацію процедур управління інцидентами та поглиблення імплементації міжнародних вимог до захисту критичної інфраструктури.

Обґрунтовано стратегічну мету системи протидії кібертероризму як сформування стійкої, скоординованої та ресурсно забезпеченої моделі захисту критичної інфраструктури в структурі національної безпеки. Показано її узгодження з інформаційною, військовою, економічною, енергетичною, техногенною та соціальною безпекою через систему цілей, завдань і

вимірюваних показників, декомпозованих за рівнями управління та компонентами безпеки.

Сформовано трирівневу архітектуру комплексної системи захисту критичної інфраструктури (національний, галузевий рівень і рівень суб'єкта) з чітким розподілом функцій, інформаційних потоків та інструментів реалізації. Виділено функціональні модулі моніторингу загроз, аналізу інцидентів, управління ризиками, координації реагування, відновлення та навчання, що утворюють замкнений цикл управління кібертерористичними загрозами на основі принципів цілісності, узгодженості, безперервності, адаптивності та ресурсної достатності.

Розроблено поетапний план впровадження комплексної системи протидії кібертероризму (підготовчий, пілотний, розгортання, оптимізація) з визначеними змістом робіт, відповідальними суб'єктами, строками та проміжними результатами. Сформовано ресурсну модель із деталізацією фінансових, кадрових, технічних, інформаційних та організаційно-правових потреб, орієнтовних бюджетних параметрів і основних обмежень воєнного періоду, що дозволяє поєднати амбіції проєкту з реалістичними можливостями держави та операторів критичної інфраструктури.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Левченко О.В., Охрімчук В.В. Особливості антиукраїнського інформаційного (кібер) впливу на Україну. *Захист інформації.* 2022. № 4. С. 156–163.

2. Правове регулювання національної безпеки : навчальний посібник / О. Г. Боднарчук, О. І. Боднарчук, М. В. Глух, А. В. Гарбінська-Руденко ; Державний податковий університет. Ірпінь, 2024. 202 с. URL: https://dpu.edu.ua/images/Documents/NAUKA/Naukova%20biblioteka/Navcalno-metodicna%20literatura/N/Pravove%20reguluvanna%20nacionalnoi%20bezpeki.pdf (дата звернення: 01.12.2025).

3. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 01.12.2025).

4. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26 серпня 2021 року № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021 (дата звернення: 09.12.2025).

5. Мельник Д. С. Кібертероризм: зміст, форми та перспективні заходи протидії. *Вісник Харківського національного університету внутрішніх справ.* 2023. № 3(102). С. 144–158. URL: https://visnyk.univd.edu.ua/index.php/VNUAF/article/view/654 (дата звернення: 01.12.2025).

6. Мазур Я. П. Основні кіберзагрози в умовах ведення інформаційної війни. *Аналітично-порівняльне правознавство.* 2024. № 6. С. 599–604. URL: https://app-journal.in.ua/wp-content/uploads/2024/12/100.pdf (дата звернення: 01.12.2025).

7. Галушко П. П. Кіберзлочинність: поняття та соціально-правова природа. *Вісник Кримінологічної асоціації України.* 2025. Т. 34, № 1. С. 808–817. URL: https://vca.univd.edu.ua/index.php/vca/article/view/516 (дата звернення: 02.12.2025).

8. Топчій В. В., Бодунова О. М. Проблемні питання забезпечення кібербезпеки в Україні. *Аналітично-порівняльне правознавство*. 2025. № 1. С. 664–669. URL: https://app-journal.in.ua/2025-1 (дата звернення: 02.12.2025).

9. Зінченко О. І. Політичні проблеми розвитку кібертероризму в міжнародному просторі. Politicus. 2024. № 4. С. 154–160. URL: https://politicus.od.ua/4_2024/25.pdf (дата звернення: 02.12.2025).

10. Бараненко Р. В. Кібератаки як одна з форм кібертероризму. *Вчені записки Таврійського національного університету імені В. І. Вернадського*. Серія: Технічні науки. 2021. Т. 32(71), ч. 1, № 1. С. 45–50. URL: https://www.tech.vernadskyjournals.in.ua/journals/2021/1_2021/part_1/9.pdf (дата звернення: 02.12.2025).

11. Богдан Б. В. Критична інформаційна інфраструктура як об'єкт забезпечення кібербезпеки. *Актуальні питання у сучасній науці.* 2025. № 3(33). С. 473–482. URL: https://perspectives.pp.ua/index.php/sn/article/view/21395/21369(дата звернення: 02.12.2025).

12. Огляд подій в сфері кібербезпеки, липень 2024. Cyber Digest. Українська фундація безпекових студій, Рада національної безпеки і оборони України, USAID «Кібербезпека критично важливої інфраструктури України». Київ, 2024. URL: https://ufss.com.ua/wp-content/uploads/2024/08/Cyber-digest_Jul_2024_UA.pdf (дата звернення: 02.12.2025).

13. Дьяком Л. В., Невмержицький Є. В., Бутенко О. В. Кібертероризм як загроза національній безпеці України. *Науковий вісник Національної академії Служби безпеки України.* 2020. № 2. С. 120–129. URL: https://academy.ssu.gov.ua/uploads/publications/2020/10/05/nauk_visnyk_2_2020.pdf (дата звернення: 02.12.2025).

14. Світличний Д. О. Аналіз сучасного стану кіберзагроз для об'єктів критичної інфраструктури та існуючих підходів до їх класифікації // Актуальні питання забезпечення кібербезпеки та захисту інформації: збірник матеріалів науково-практичної конференції (Запоріжжя, 24 квітня 2025 р.). Запоріжжя:

Запорізький національний університет, 2025. С. 109–111. URL: https://files.znu.edu.ua/files/Bibliobooks/Inshi84/0063968.pdf (дата звернення: 03.12.2025).

15. Аркуша Л. І. Нормативно-правове забезпечення кібербезпеки: навчально-методичні матеріали. Одеса: Національний університет «Одеська юридична академія», 2024. 72 с. URL: https://dspace.onua.edu.ua/bitstreams/bcc742c0-132f-4245-a316-607662bea653/download (дата звернення: 03.12.2025).

16. Інформаційна безпека держави: силабус навчальної дисципліни. Харків: Національний технічний університет «Харківський політехнічний інститут», кафедра кібербезпеки, 2024. 34 с.

17. Зінченко О. І. Політичні проблеми розвитку кібертероризму в сучасному міжнародному порядку. *Politicus.* 2024. № 4. С. 180–186. URL: https://politicus.od.ua/4_2024/25.pdf (дата звернення: 03.12.2025).

18. Гребенюк А. М. DDoS атаки в Україні: виклики та документування // Міжнародна та національна безпека: теоретичні і прикладні аспекти : матеріали VIII Міжнародної науково-практичної конференції (Дніпро, 15 березня 2024 року) : у 2 частинах. Дніпро: Дніпровський державний університет внутрішніх справ, 2024. Ч. 2. С. 313–315. URL: https://er.dduvs.edu.ua/handle/123456789/14227

19. Дьяченко О. В., Тирусь Б. Ю. Захист державних електронних інформаційних ресурсів як складова національної безпеки України. *Scientific and analytical journal «Social and administrative sciences».* 2025. № 10(20). С. 453–463. URL: https://perspectives.pp.ua/index.php/sas/article/view/30601 (дата звернення: 03.12.2025).

20. Живило Є. Макрофінансова стабільність держави в умовах кіберзагроз. *Актуальні проблеми державного управління. 2024*. № 2(65). С. 120–137. URL: https://www.researchgate.net/publication/389165058_Makrofinansova_stabilnist_derzavi_v_umovah_kiberzagroz.

21 Кірпічніков Ю. та ін. Модель оцінювання стійкості інформаційної інфраструктури в умовах відсічі збройної агресії. Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ ім. І. Черняховського. 2025. С. 69–78.

22. Шевчук М. О. Сучасні виклики і загрози в сфері національної інформаційної безпеки в умовах цифрової трансформації. Актуальні проблеми вітчизняної юриспруденції. 2024. № 6. С. 130–135. URL: https://apnl.dnu.in.ua/6_2024/27.pdf

23. Бідзіля Ю. М. Державна політика інформаційної безпеки в умовах гібридних загроз. *Український політико-правовий дискурс*, (17). 2025. https://doi.org/10.5281/zenodo.17757320

24. Саєнко М. Г. Основи кіберзахисту інформаційних систем: навчальний посібник. Київ: Національний авіаційний університет, 2022. 212 с. URL: https://er.nau.edu.ua/bitstream/NAU/57412/1/navchalnyi_posibnyk_Osnovy_kiberzakhystu.pdf

25. Романенко С. О. Модель оцінювання наслідків витоку державної таємниці від кібератак на критичну інформаційну інфраструктуру держави. *Вісник Черкаського державного технологічного університету. Серія: Технічні науки.* 2018. № 1. С. 29-35.

26. Климчук В. О. Організаційні та технічні заходи раннього виявлення кіберзагроз у критичній інфраструктурі. Інформаційна безпека людини, суспільства, держави. 2024. № 1. С. 55–63. URL: https://journals.iucu.org.ua/index.php/security/article/view/321

27. Мануілов Я.С. Питання розробки індикаторів оцінки стану кібербезпеки. *Інформація і право*. № 4(51) (2024). С.144-152

28. Шульга В. П., Іванченко Є. В., Вишневська Н. С., Бербер А. С. Дослідження методів та моделей оцінювання кіберзахисту критичної інфраструктури держави. *Сучасний захист інформації.* 2024. № 3(59). С. 6–19.

29. European Union Agency for Cybersecurity. ENISA Threat Landscape 2020. 2020. URL: https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020 (дата звертання: 03.12.2025).

30. National Institute of Standards and Technology. NIST Cybersecurity Framework. Version 2.0. 2024. URL: https://www.nist.gov/cyberframework (дата звертання: 03.12.2025).

31. National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. Gaithersburg, 2018. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (дата звертання: 03.12.2025).

32. European Union Agency for Cybersecurity. ENISA Threat Landscape 2023. Heraklion, 2023. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (дата звертання: 03.12.2025).

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

34. Про боротьбу з тероризмом : Закон України від 20.03.2003 № 638-IV // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/638-15 (дата звернення: 04.12.2025).

35. Законодавство у сфері критичної інфраструктури // Міністерство економіки України : офіційний вебсайт. URL: https://mindev.gov.ua/diialnist/krytychna-infrastruktura/zakonodavstvo (дата звернення: 04.12.2025).

36. Деякі питання об’єктів критичної інфраструктури : постанова Кабінету Міністрів України від 09.10.2020 № 1109. URL: https://zakon.rada.gov.ua/go/1109-2020-%D0%BF (дата звернення: 04.12.2025).

37. Даник Ю.Г., Воробієнко П.П., Чернега В.М. Основи кібербезпеки та кібероборони: підручник. Вид. 2-е, перероб. та доп. Одеса: ОНАЗ, 2019. 320 с.

38. Панасюк Т. Державна політика України у сфері забезпечення інформаційної безпеки людини, суспільства, держави в умовах розвитку державно-приватного партнерства у сфері кібербезпеки. *Інформаційна безпека людини, суспільства, держави*. 2025. № 1(38). С. 44–47.

39. Казьмірук С. Д. Забезпечення кібербезпеки об'єктів критичної інфраструктури в умовах цифрової трансформації. *Law and Safety.* 2024. № 6. С. 312–319. URL: https://lsej.org.ua/6_2024/51.pdf (дата звернення: 04.12.2025).

40. Столбовий В. М. Заходи з підвищення кібербезпеки на рівні держави та корпоративного сектору. *Науковий вісник Львівського державного університету внутрішніх справ. Серія: юридична.* 2023. № 2. С. 145–152. URL: https://nzlubp.org.ua/index.php/journal/article/view/802

41. Андрух А. Кібербезпека критичної інфраструктури: виклики та напрями удосконалення системи захисту. *Журнал «Комп'ютерно-інтегровані технології: освіта, наука, виробництво».* 2024. № 3. С. 90–97. URL: https://cims.fti.dp.ua/j/article/view/210 (дата звернення: 04.12.2025).

42. United Nations Office on Drugs and Crime. International cooperation on cybersecurity matters. URL: https://www.unodc.org/cld/en/education/tertiary/cybercrime/module-8/key-issues/international-cooperation-on-cybersecurity-matters.html (дата звернення: 04.12.2025).

43. Cooperative Cyber Defence Centre of Excellence. CCDCOE – NATO Cooperative Cyber Defence Centre of Excellence. URL: https://ccdcoe.org/ (дата звернення: 04.12.2025).

44. Стендер С.В., Фротер О.С., Снітко Ю.М. Цифрова інтеграція та кіберзахист економіки України: правові аспекти та інноваційні стратегії. *Академічні візії.* Випуск №26, 2023. URL: http://dx.doi.org/10.5281/zenodo.10389831 (дата звернення: 04.12.2025).

45. Федик В.Р., Денисенко Г.В. Теоретико-методологічні підходи до управління ризиками кібербезпеки на об'єктах критичної інфраструктури: реагування на кіберінциденти та менеджмент кризових ситуацій. *Інформація і право.* Випуск №1(48), 2024. URL: https://doi.org/10.37750/2616-6798.2024.1(48).300822

46. Алексєєв М.М. Аналіз методологічних підходів щодо застосування технологій управління ризиками у сфері кібербезпеки. *Modern Information Technologiesinthe Sphere of Security and Defence.* 2019. № 1(34). С. 109-114.

47. Климчук В. О. Використання методів машинного навчання для аналізу кіберзагроз у системах критичної інфраструктури. *Інформаційна безпека людини, суспільства, держави*. 2024. № 1. С. 55–63.

48. Когут Ю. Правові засади формування та розвитку державної системи протидії кібертероризму в Україні. *Підприємництво, господарство і право*. 2020. № 12. С. 170-174.

49. Рогов П.Д. Ворович Б.О., Ткаченко В.А. Шляхи забезпечення кібернетичної безпеки об'єктів критичної інформаційної інфраструктури держави у воєнній сфері: збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2017. № 1. С. 64-72. URL: http://nbuv.gov.ua/UJRN/Znpcvsd_2017_1_13 (дата звернення: 04.12.2025).

50. Ткачук Н.А. Організаційно-правові засади формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави. *Інформація і право*. № 1(24), 2018. С. 133-138. URL: http://ippi.org.ua/sites/default/files/16_4.pdf (дата звернення: 04.12.2025).

51. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). EUR-Lex. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj (дата звернення: 05.12.2025).

52. Cybersecurity and Infrastructure Security Agency Act of 2018 : Public Law No. 115-278, 16 November 2018. *Congress.gov.* URL: https://www.congress.gov/bill/115th-congress/house-bill/3359 (дата звернення: 05.12.2025).

53. Act on the Protection of Information and Communications Infrastructure : Act No. 18870 of June 10, 2022 (amended). *Korea Legislation Research Institute.*

URL: https://elaw.klri.re.kr/eng_service/lawView.do?hseq=52998&lang=ENG (дата звернення: 05.12.2025).

54. State cybersecurity policy: Ukraine and international experience. ITTA : аналітичний огляд. 2025. 29 берез. URL: https://itta.info/en/state-cybersecurity-policy-ukraine-and-international-experience/ (дата звернення: 05.12.2025).

55. Paz S. National Cybersecurity Law, Governance, and Infrastructure in the Republic of Korea. Inter-American Development Bank, 2024. URL: https://publications.iadb.org/publications/english/document/National-Cybersecurity-Law-Governance-and-Infrastructure-in-the-Republic-of-Korea.pdf (дата звернення: 05.12.2025).

56. Cybersecurity of critical infrastructure in Ukrainian legislation and in Directive (EU) 2022/2555 (NIS2). ResearchGate, 2025. URL: https://www.researchgate.net/publication/375323482_Cybersecurity_of_Critical_Infrastructure_in_Ukrainian_Legislation_and_in_Directive_EU_20222555 (дата звернення: 05.12.2025).

57. Legal responses to cyberterrorism. *Tsinghua China Law Review*. 2024. URL: https://www.tsinghuachinalawreview.law.tsinghua.edu.cn/UploadFiles/2024-08-04/ecypv8egc26z3r4x.pdf (дата звернення: 05.12.2025).

58. Хаджирадєєва С. Захист персональних даних: між дотриманням прав людини та національною безпекою. *Scientific and Legal Studies (SLS Journal).* 2024. Т. 7, № 3. URL: https://sls-journal.com.ua/en/journals/tom-7-3-2024/zakhist-personalnikh-danikh-mizh-dotrimannyam-prav-lyudini-ta-natsionalnoyu-bezpekoyu (дата звернення: 05.12.2025).

59. Ethics of surveillance technologies: balancing privacy and security in a digital age. *Premier Journal of Data Science.* 2024. URL: https://premierscience.com/pjds-24-359/ (дата звернення: 05.12.2025).

60. The right to privacy in the digital age: report of the Office of the United Nations High Commissioner for Human Rights (A/HRC/51/17). United Nations, 2022. URL: https://digitallibrary.un.org/record/3985679 (дата звернення: 05.12.2025).

61. Council of Europe. Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users. Council of Europe, 2014. URL: https://rm.coe.int/168008c37f (дата звернення: 06.12.2025).

62. European Union Agency for Cybersecurity. *Multilayer framework for good cybersecurity practices for AI.* ENISA, 2022. URL: https://www.enisa.europa.eu/sites/default/files/publications/Multilayer%20Framework%20for%20Good%20Cybersecurity%20Practices%20for%20AI.pdf (дата звернення: 06.12.2025).

63. Tzanou M. National security and new forms of surveillance: the data retention saga and a data subject-centred approach. *European Papers.* 2025. URL: https://www.europeanpapers.eu/e-journal/national-security-forms-surveillance-data-retention-saga-data-subject-centred-approach (дата звернення: 06.12.2025).

64. Harnessing digital technology to disrupt, repress and intimidate: research brief. Geneva Academy of International Humanitarian Law and Human Rights, 2025. URL: https://geneva-academy.ch/wp-content/uploads/2025/09/Harnessing-Digital-Technology-to-Disrupt-Repress-and-Intimidate.pdf (дата звернення: 06.12.2025).

65. Cremer F., Müller S., Riemann A. Cyber risk and cybersecurity: a systematic review of data sources and data issues. *Cybersecurity.* 2022. Vol. 5, Art. 9. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8853293/ (дата звернення: 07.12.2025).

66. An evaluation framework for cyber security strategies. European Union Agency for Cybersecurity (ENISA), 2014. URL: https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies (дата звернення: 07.12.2025).

67. Cho H., Kim J., Park S. Quantifying cyber resilience: a framework based on availability metrics. *Electronics.* 2025. Vol. 14, No. 12. Art. 2465. URL: https://www.mdpi.com/2079-9292/14/12/2465 (дата звернення: 07.12.2025).

ДОДАТКИ

Додаток А

Анкетування експертів з кібербезпеки

Блок І. Оцінка загроз і готовності (питання 1–5)

1. Як Ви оцінюєте актуальність кібертерористичних загроз для критичної інфраструктури України у найближчі 3 роки?

А) Ризики залишаються помірними та контрольованими, різкого зростання не очікується.

Б) Ймовірне поступове посилення загроз, що вимагатиме адаптації існуючих механізмів захисту.

В) Ризики мають тенденцію до різкого зростання у зв’язку з воєнними діями та розвитком атакувальних технологій.

2. Наскільки, на Вашу думку, нинішній стан кіберзахисту критичної інфраструктури відповідає умовам війни?

А) Система в основному відповідає викликам, потребує лише планових удосконалень.

Б) Стан є частково відповідним, проте окремі сегменти суттєво відстають від вимог воєнного часу.

В) Система є фрагментарною, окремі елементи не пристосовані до реальних загроз.

3. Як Ви оцінюєте рівень узгодженості дій між різними операторами критичної інфраструктури у разі кіберінциденту?

А) Взаємодія системна, відпрацьована та формалізована у спільних регламентах.

Б) Взаємодія частково формалізована, значною мірою спирається на неформальні контакти.

В) Взаємодія переважно ситуативна, відсутні сталі процедури та практики спільного реагування.

4. Яким є рівень готовності керівництва Вашої організації до прийняття рішень у разі комплексної кібертерористичної атаки?

А) Керівництво добре обізнане з процедурами, регулярно долучається до навчань.

Б) Керівництво частково залучається до питань кібербезпеки, реагування часто має імпровізаційний характер.

В) Керівництво обмежено орієнтується в питаннях кібербезпеки, рішення приймаються із запізненням.

5. Як Ви оцінюєте вплив кібертерористичних загроз на безперервність основних послуг Вашої організації?

А) Ризик зупинки послуг є низьким, існують відпрацьовані резервні сценарії.

Б) Можливі локальні збої, частина сервісів має обмежені резервні можливості.

В) Існує висока ймовірність тривалих відмов, резервні сценарії є неповними або формальними.

Блок ІІ. Організаційні та правові механізми (питання 6–10)

6. Наскільки чітко у Вашій організації визначені ролі та відповідальність за кібербезпеку?

А) Ролі формалізовані у посадових інструкціях, існує чітка вертикаль відповідальності.

Б) Основні ролі визначені, але межі відповідальності інколи розмиті.

В) Розподіл відповідальності є фрагментарним, частина функцій фактично не закріплена.

7. Як Ви оцінюєте якість внутрішніх політик і регламентів з кібербезпеки у Вашій організації?

А) Документи актуалізуються регулярно, відповідають сучасним стандартам і умовам війни.

Б) Документи частково оновлені, окремі положення не враховують нові загрози.

В) Документи застарілі або розрізнені, фактично не виконують регулювальну функцію.

8. Чи забезпечує національна нормативно-правова база, на Вашу думку, достатні умови для захисту критичної інфраструктури від кібертероризму?

А) Нормативна база є цілісною, створює зрозумілий каркас для діяльності операторів.

Б) Основні засади прописані, проте існують прогалини у деталізації вимог і механізмів контролю.

В) Нормативна база є фрагментарною, значний обсяг практичних рішень залишається на розсуд операторів.

9. Як Ви оцінюєте ступінь інтегрованості питань кібертероризму у систему управління ризиками Вашої організації?

А) Кібертероризм є окремим напрямом у загальній системі ризик-менеджменту, проводиться регулярна переоцінка ризиків.

Б) Питання кібертероризму враховуються, але системна переоцінка ризиків здійснюється нерегулярно.

В) Підхід до ризиків має фрагментарний характер, кібертероризм розглядається лише епізодично.

10. Наскільки формалізовані процедури взаємодії Вашої організації з державними органами у разі кіберінцидентів?

А) Існують чіткі протоколи, визначені контактні точки, відпрацьовані процедури ескалації.

Б) Взаємодія частково регламентована, значна частина комунікації базується на попередніх домовленостях.

В) Взаємодія має епізодичний характер, формалізовані процедури практично відсутні.

Блок ІІІ. Технічні та ресурсні аспекти (питання 11–15)

11. Як Ви оцінюєте рівень захищеності автоматизованих систем управління технологічними процесами (АСУ ТП) у Вашій організації?

А) АСУ ТП ізольовані, контролюються, оснащені розвиненими засобами моніторингу та виявлення атак.

Б) Захист частково реалізований, проте існують канали доступу з обмеженим контролем.

В) Захист АСУ ТП є мінімальним, сегментація та моніторинг реалізовані лише частково.

12. Наскільки повно у Вашій організації впроваджені системи моніторингу подій безпеки (SIEM або їх аналоги) для критичних сегментів?

А) Моніторинг охоплює всі ключові сегменти, кореляція подій виконується постійно.

Б) Моніторинг частковий, окремі сегменти залишаються поза повноцінним контролем.

В) Системи моніторингу розміщені фрагментарно, аналіз подій має вибірковий характер.

13. Як Ви оцінюєте рівень підготовки персоналу до реагування на кібертерористичні інциденти?

А) Персонал регулярно проходить спеціалізовані навчання та тренування за сценаріями.

Б) Проводяться епізодичні тренінги, частина працівників має обмежені практичні навички.

В) Підготовка має формальний характер, більшість працівників не залучається до навчань.

14. Наскільки достатні фінансові ресурси, що виділяються на кібербезпеку у Вашій організації?

А) Фінансування відповідає реальним потребам, передбачає резерви на модернізацію та навчання.

Б) Фінансування дозволяє підтримувати базовий рівень, проте масштабні модернізації ускладнені.

В) Фінансування є недостатнім, більшість заходів реалізується із суттєвими обмеженнями.

15. Як Ви оцінюєте якість технічної інфраструктури (мережеве обладнання, засоби захисту, резервування) з погляду протидії кібертероризму?

А) Інфраструктура сучасна, побудована з урахуванням принципів резервування і сегментації.

Б) Інфраструктура частково модернізована, наявні окремі застарілі елементи.

В) Інфраструктура значною мірою застаріла, існують структурні обмеження для впровадження сучасних рішень.

Додаток Б

Приклади аналітичних звітів розробленої моделі

Таблиця Б.1

Динаміка показників кіберінцидентів та реагування оператора енергетичної мережі

Рік	Кількість зареєстрованих інцидентів, од.	Кількість успішних атак, од.	Середній час виявлення інциденту, годин	Середній час локалізації інциденту, годин	Коефіцієнт доступності ключових сервісів
2026 (до впровадження)	42	7	11,8	7,9	0,964
2027 (пілотний етап)	58	5	6,4	5,1	0,973
2028 (розгортання моделі)	71	3	3,6	3,2	0,981

Таблиця Б. 2

Річна інтегральна оцінка ризику основних підсистем, індекс (0–1)

Підсистема	2026 (до впровадження)	2027 (пілотний етап)	2028 (розгортання моделі)
Організаційна система управління кібербезпекою	0,76	0,59	0,46
Мережна інфраструктура офісного сегмента	0,71	0,55	0,43
Автоматизовані системи управління технологічними процесами	0,86	0,67	0,51
Інформаційні системи обліку і розрахунків	0,66	0,52	0,40
Підготовка і обізнаність персоналу	0,72	0,57	0,44
Взаємодія з державними та галузевими органами	0,62	0,50	0,39
Середній інтегральний індекс ризику	0,72	0,57	0,44

Таблиця Б.3

Оцінка економічного ефекту впровадження моделі, млн грн (умовні агреговані показники для оператора регіональної енергетичної мережі)

Показник	2026 (до впровадження)	2027 (пілотний етап)	2028 (розгортання моделі)
Орієнтовні прямі втрати від кіберінцидентів (пошкодження обладнання, позапланові ремонти), млн грн	38,0	27,5	19,0
Орієнтовні непрямі втрати (перерви в електропостачанні, штрафи, репутаційні втрати), млн грн	52,0	39,0	28,0
Сукупні витрати на впровадження та підтримання моделі за рік, млн грн	0,0	65,0	95,0
Сумарний обсяг відвернених втрат порівняно з 2026 роком, млн грн	–	23,5	43,0
Умовний чистий ефект року (відвернені втрати мінус витрати на модель), млн грн	–	−41,5	−52,0