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: “СИСТЕМА ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ”

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

_____ Андрій МАКАРЕНКО

(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБДМ-61
Андрій МАКАРЕНКО

Керівник:
д-р іст. н., професор Володимир ШУЛЬГА

Рецензент:
д.т.н., професор Галина ГАЙДУР

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 Макаренку Андрію Вадимовичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи: “Система забезпечення кіберстійкості критичної інфраструктури в умовах гібридних загроз ”
керівник кваліфікаційної роботи Володимир Шульга, д-р іст.н., професор
(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:
4. Перелік питань, які потрібно розробити:
   1. Проаналізувати сучасні гібридні загрози та їхній вплив на критичну інфраструктуру, та міжнародні стандарти та нормативно-правову базу щодо кіберстійкості (NIST, ISO/IEC 27032, ENISA).
   2. Дослідити сучасні методи управління ризиками та реагування на кіберінциденти.
   3. Розробити системну модель забезпечення кіберстійкості критичної інфраструктури.
   4. Сформувати комплекс заходів для протидії гібридним загрозам та мінімізації їхніх наслідків.
   5. Провести апробацію розробленої моделі на умовному або реальному прикладі.
   6. Підготувати практичні рекомендації щодо впровадження системного підходу на підприємствах критичної інфраструктури.
5. Перелік ілюстративного матеріалу: *презентація*
6. Дата видачі завдання “02” жовтня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назви етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	10.10.2025	
2.	Збір та аналіз літератури.	23.10.2025	
3.	Аналіз поняття критичної інформаційної інфраструктури та її значення для національної безпеки	27.10.2025	
4	Аналіз міжнародних стандартів і нормативно-правовової бази щодо кіберстійкості (NIST, ISO/IEC 27032, ENISA	05.10.2025	
5.	Аналіз гібридних загроз та їх впливу на критичну інфраструктуру	10.11.2025	
6	Аналіз методів управління ризиками та оцінки загроз у критичній інфраструктурі	13.11.2025	
7.	Розробка моделі системи забезпечення кіберстійкості критичної інфраструктури	15.11.2025	
8	Формування комплексу заходів протидії гібридним загрозам та мінімізації їх наслідків, апробація моделі	19.11.2025	
9.	Формулювання висновків за результатами дослідження.	22.11.2025	
10.	Оформлення роботи.	04.12.2025	
11.	Оформлення презентації.	14.12.2025	
12.	Отримання рецензії на роботу.	18.12.2025	
13.	Захист в ЕК.	__.01.2026	

Здобувач вищої освіти _____ Андрій Макаренко
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Володимир ШУЛЬГА
(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 Макаренко А.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: "Система забезпечення кіберстійкості критичної інфраструктури в умовах гібридних загроз"
Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач **МАКАРЕНКО Андрій** ґрунтовно проаналізував теоретико-методологічні засади забезпечення кіберстійкості критичної інфраструктури, дослідив сучасні гібридні загрози та їх вплив на функціонування критичних інформаційних систем, здійснив аналіз міжнародних стандартів і нормативно-правової бази у сфері кіберстійкості, а також сучасних методів управління ризиками, моніторингу та реагування на кіберінциденти.

Основним науково-практичним результатом кваліфікаційної роботи є **р**озробка системної моделі забезпечення кіберстійкості критичної інфраструктури, яка поєднує організаційні, технічні та управлінські заходи та враховує специфіку гібридних загроз. Запропоновано комплекс практичних заходів щодо протидії таким загрозам і мінімізації їх наслідків, а також проведено апробацію розробленої моделі на умовному прикладі.

Отримані результати свідчать про вміння здобувача критично мислити, узагальнювати інформацію та формулювати обґрунтовані висновки. Матеріал викладено логічно, з використанням сучасних наукових джерел та міжнародних стандартів.

Все це дозволяє оцінити кваліфікаційну роботу здобувача **МАКАРЕНКА Андрія** на оцінку «добре» та рекомендувати присвоїти йому кваліфікацію "Магістр з кібербезпеки та захисту інформації за освітньо-професійною програмою Управління інформаційною та кібернетичною безпекою".

Керівник кваліфікаційної роботи _____ Володимир ШУЛЬГА
(підпис). *(Ім'я, ПРІЗВИЩЕ)*

"____" _____2025 року

Висновок кафедри про кваліфікаційну роботу

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

Завідувач кафедрою
Управління інформаційною та кібернетичною безпекою _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну магістерську роботу

здобувача вищої освіти Макаренка Андрія Вадимовича
на тему “ Система забезпечення кіберстійкості критичної інфраструктури в умовах гібридних загроз ”

Актуальність Актуальність кваліфікаційної магістерської роботи зумовлена зростанням кількості та складності гібридних загроз, які поєднують кібернетичні, інформаційні, фізичні та організаційні впливи на об’єкти критичної інфраструктури. Забезпечення кіберстійкості таких об’єктів є однією з ключових умов національної безпеки та безперервності функціонування держави і суспільства. У цьому контексті обрана тема є своєчасною та має важливе теоретичне й практичне значення.

Позитивні сторони

До позитивних сторін кваліфікаційної роботи слід віднести логічну та послідовну структуру, достатній рівень теоретичного опрацювання проблематики кіберстійкості критичної інфраструктури, а також коректне використання міжнародних стандартів і нормативно-правових документів (NIST, ISO/IEC 27032, ENISA). Практичну цінність становить розроблена автором системна модель забезпечення кіберстійкості, що поєднує організаційні, технічні та управлінські заходи, а також сформований комплекс рекомендацій щодо протидії гібридним загрозам і мінімізації їх наслідків.

Недоліки

Доцільно більш детально розглянути галузеві особливості впровадження запропонованої системи кіберстійкості для окремих об’єктів критичної інфраструктури. Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи

Висновок: Кваліфікаційна магістерська робота виконана на належному науково-методичному рівні, відповідає вимогам, що висуваються до магістерських робіт за спеціальністю 125 «Кібербезпека та захист інформації», та заслуговує позитивної оцінки. Здобувач Макаренко Андрій Вадимович заслуговує присвоєння кваліфікації «Магістр з кібербезпеки та захисту інформації» за освітньо-професійною програмою «Управління інформаційною та кібернетичною безпекою».

Рецензент: завідувач кафедри
Систем та технологій кібербезпеки

д-р техн. н., професор _____ Галина ГАЙДУР

підпис *Ім’я, ПРІЗВИЩЕ*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 87 стор., 11 рис., 12 табл., 60 джерел.

Метою роботи є розробка системного підходу та моделі забезпечення кіберстійкості критичної інфраструктури в умовах гібридних загроз, що дозволяє підвищити рівень захищеності критичних інформаційних систем та мінімізувати наслідки деструктивних впливів.

Об'єктом дослідження є критична інформаційна інфраструктура та процеси забезпечення її кіберстійкості в умовах гібридних загроз.

Предмет дослідження – методи, моделі та інструменти забезпечення кіберстійкості критичної інфраструктури з урахуванням сучасних гібридних загроз.

Мета дослідження – розробити системний підхід до забезпечення кіберстійкості критичних об'єктів, що дозволяє ефективно протидіяти гібридним загрозам та мінімізувати наслідки атак.

Методи дослідження. Для досягнення поставленої мети та вирішення завдань кваліфікаційної магістерської роботи використано комплекс загальнонаукових і спеціальних методів дослідження. Зокрема, застосовано методи аналізу та синтезу – для вивчення теоретико-методологічних засад забезпечення кіберстійкості критичної інфраструктури; порівняльний аналіз – для оцінки ефективності сучасних підходів і технологій протидії гібридним загрозам; системний підхід – для формування комплексної моделі забезпечення кіберстійкості.

Методи класифікації та узагальнення використано для структурування гібридних загроз і заходів кіберзахисту. Методи оцінки ризиків та моделювання застосовано для аналізу впливу загроз на об'єкти критичної інфраструктури. Також використано елементи експертної оцінки для формування практичних рекомендацій щодо підвищення рівня кіберстійкості.

Короткий зміст роботи. У кваліфікаційній роботі розглянуто проблеми

забезпечення кіберстійкості критичної інфраструктури в умовах гібридних загроз. Проаналізовано теоретичні основи кіберстійкості, сутність і класифікацію гібридних загроз, а також міжнародні стандарти та нормативно-правові документи у сфері кібербезпеки.

У роботі розроблено системну модель забезпечення кіберстійкості критичної інфраструктури та запропоновано комплекс практичних заходів щодо протидії гібридним загрозам і мінімізації їх негативних наслідків, що сприяє підвищенню рівня захищеності критичних інформаційних систем.

Галузь застосування. Результати кваліфікаційної магістерської роботи можуть бути використані у діяльності підприємств і організацій, що належать до об’єктів критичної інфраструктури, а також у структурах, відповідальних за забезпечення кібербезпеки та управління інформаційними ризиками. Запропоновані підходи та модель кіберстійкості доцільно застосовувати при проєктуванні, модернізації та оцінці ефективності систем кіберзахисту критичних інформаційних систем.

Ключові слова: КІБЕРСТІЙКІСТЬ, КРИТИЧНА ІНФРАСТРУКТУРА, ГІБРИДНІ ЗАГРОЗИ, КІБЕРБЕЗПЕКА, УПРАВЛІННЯ РИЗИКАМИ, СИСТЕМНИЙ ПІДХІД.

ABSTRACT

The qualification work is devoted to the study of information security awareness and training technologies for personnel. The work consists of an introduction, three chapters containing 2 figures, conclusions and the list of references containing 60 items. The total volume of the work is 87 pages, of which 3 pages are occupied by the list of abbreviations and the list of references.

The purpose of the study is to develop a systemic approach and a model for ensuring the cyber resilience of critical infrastructure under hybrid threats, which makes it possible to increase the level of protection of critical information systems and minimize the consequences of destructive impacts.

The object the study is critical information infrastructure and the processes of ensuring its cyber resilience under hybrid threats.

The subject of the study is methods, models, and tools for ensuring the cyber resilience of critical infrastructure taking into account modern hybrid threats.

Research methods. In order to achieve the research objective and solve the tasks of the qualification work, a set of general scientific and special research methods is used, including analysis and synthesis to study theoretical and methodological foundations of cyber resilience, comparative analysis to assess the effectiveness of modern approaches to countering hybrid threats, a systematic approach to develop a comprehensive cyber resilience model, as well as classification, risk assessment, modeling methods, and elements of expert evaluation.

Summary of the work. As a result of the study, the theoretical foundations of cyber resilience are analyzed, modern hybrid threats and their impact on critical infrastructure are examined, and international standards and regulatory frameworks in the field of cyber resilience are studied. A systemic model for ensuring the cyber resilience of critical infrastructure is developed, a set of measures to counter hybrid threats and minimize their consequences is proposed, and practical recommendations for improving cybersecurity management are formulated.

Field of application. The results of the qualification work can be applied in the

activities of enterprises and organizations belonging to critical infrastructure sectors, as well as in structures responsible for cybersecurity and information risk management. The proposed model and recommendations can be used in the design, modernization, and evaluation of cybersecurity systems for critical information infrastructure.

Keywords: CYBER RESILIENCE, CRITICAL INFRASTRUCTURE, HYBRID THREATS, CYBERSECURITY, RISK MANAGEMENT, SYSTEMIC APPROACH.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

AI *Artificial Intelligence* (штучний інтелект)

API *Application Programming Interface* (прикладний програмний інтерфейс)

BCP *Business Continuity Planning* (планування безперервності діяльності)

CERT *Computer Emergency Response Team* (команда реагування на комп'ютерні інциденти)

CII *Critical Information Infrastructure* (критична інформаційна інфраструктура)

CSIRT *Computer Security Incident Response Team* (команда реагування на інциденти інформаційної безпеки)

DLP *Data Loss Prevention* (запобігання витоку даних)

ENISA *European Union Agency for Cybersecurity* (Агентство Європейського Союзу з кібербезпеки)

IDS *Intrusion Detection System* (система виявлення вторгнень)

IEC *International Electrotechnical Commission* (Міжнародна електротехнічна комісія)

ISO *International Organization for Standardization* (Міжнародна організація зі стандартизації)

ISMS *Information Security Management System* (система управління інформаційною безпекою)

IT *Information Technology* (інформаційні технології)

KII *Critical Information Infrastructure* (критична інформаційна інфраструктура)

ML *Machine Learning* (машинне навчання)

NIST *National Institute of Standards and Technology* (Національний інститут стандартів і технологій США)

OT *Operational Technology* (операційні технології)

RCA *Root Cause Analysis* (аналіз першопричин інцидентів)

SIEM *Security Information and Event Management* (система управління подіями та інформацією безпеки)

SOC *Security Operations Center* (центр операційної безпеки)

STRIDE *Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege* (модель класифікації загроз)

TI *Threat Intelligence* (аналітика кіберзагроз)

ICS *Industrial Control Systems* (промислові системи керування)

ВСТУП

Актуальність теми. За останні роки кіберзлочинці стали більш активнішими та вдосконалили свої методи атак, що часто націлені на слабкі сторони інфраструктури. Це змушує підприємства поставати перед викликом постійних змін та вдосконалень своїх заходів кібербезпеки. І враховуючи, що малим та середнім підприємствам часто бракує ресурсів для повноцінного захисту, оптимізація процесів виявлення та реагування на кібератаки дозволить ефективніше використати наявні ресурси. Дослідження у цій області важливе для забезпечення безпеки підприємств та збереження їхньої конкурентоспроможності на ринку.

З огляду на зазначене дослідження технологій формування обізнаності й навчання персоналу з інформаційної безпеки є актуальним науковим завданням.

Мета роботи є розробка системного підходу та моделі забезпечення кіберстійкості критичної інфраструктури в умовах гібридних загроз, що дозволяє підвищити рівень захищеності критичних інформаційних систем та мінімізувати наслідки деструктивних впливів.

Для досягнення поставленої мети у роботі передбачено вирішення таких завдань:

1. Проаналізувати сучасні гібридні загрози та їхній вплив на критичну інфраструктуру, та міжнародні стандарти та нормативно-правову базу щодо кіберстійкості (NIST, ISO/IEC 27032, ENISA).

2. Дослідити сучасні методи управління ризиками та реагування на кіберінциденти.

3. Розробити системну модель забезпечення кіберстійкості критичної інфраструктури.

4. Сформувати комплекс заходів для протидії гібридним загрозам та мінімізації їхніх наслідків.

5. Провести апробацію розробленої моделі на умовному або реальному прикладі.

6. Підготувати практичні рекомендації щодо впровадження системного підходу на підприємствах критичної інфраструктури.

Об'єкт дослідження є критична інформаційна інфраструктура та процеси забезпечення її кіберстійкості в умовах гібридних загроз.

Предмет дослідження – методи , моделі та інструменти забезпечення кіберстійкості критичної інфраструктури з урахуванням сучасних гібридних загроз.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, експертної оцінки, системного підходу до управління інформаційною безпекою.

Наукова новизна. Розроблено та описано архітектуру системи кіберстійкості, побудовану з урахуванням концепцій багаторівневої оборони (Defense-in-Depth) та нульової довіри (Zero Trust), адаптовану до специфіки функціонування підприємств критичної інфраструктури України, яка відрізняється від відомих тим, що враховує конвергенцію IT- та OT-компонентів і передбачає застосування мікросегментації мереж, спеціалізованих засобів моніторингу промислових систем управління, автоматизованих механізмів виявлення аномалій та реагування на інциденти, а також комплексу організаційних заходів, спрямованих на забезпечення безперервності надання критичних послуг..

Практичне значення одержаних результатів. Застосування напрацювань дасть змогу ефективніше використати наявні ресурси малих та середніх підприємств для виявлення та протидії кіберзагрозам.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції "Стратегії кіберстійкості: управління ризиками та безперервність бізнесу" 28 лютого 2025 року.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСНОВИ ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Сучасний етап цивілізаційного розвитку характеризується глобальною трансформацією соціально-економічних систем під впливом інформаційно-комунікаційних технологій. Цифровізація перестала бути лише допоміжним інструментом оптимізації процесів, перетворившись на фундаментальну основу функціонування держави. У цьому контексті архітектура національної безпеки зазнає докорінних змін, центром тяжіння яких стає захист критичної інформаційної інфраструктури (КІІ). Залежність життєдіяльності суспільства від безперебійного функціонування інформаційних мереж, асвтоматизованих систем управління та баз даних створює нові виклики, які вимагають глибокого теоретичного осмислення та нормативного врегулювання [1].

1.1. Поняття критичної інформаційної інфраструктури та її значення для національної безпеки

В українському законодавчому полі поняття критичної інформаційної інфраструктури було імплементоване як відповідь на зростаючі кіберзагрози. Базовим документом, що визначає термінологічний апарат у цій сфері, є Закон України «Про основні засади забезпечення кібербезпеки України». Відповідно до положень цього нормативно-правового акта, під критичною інформаційною інфраструктурою розуміється сукупність об’єктів критичної інформаційної інфраструктури, до яких належать комунікаційні, інформаційні та інформаційно-телекомунікаційні системи, а також технологічні мережі. Ключовою ознакою, що дозволяє віднести систему до категорії КІІ, є її функціональне призначення: вона має забезпечувати стале функціонування об’єктів критичної

інфраструктури, порушення роботи яких може призвести до негативних наслідків для національної безпеки та оборони, природного середовища, а також створити загрозу життю та здоров'ю людей. Законодавець акцентує увагу на тому, що такі системи є необхідними для надання життєво важливих послуг, для яких відсутні альтернативні механізми реалізації [2].

Розвиток нормативної бази продовжився із прийняттям у 2021 році Закону України «Про критичну інфраструктуру», який систематизував підходи до захисту стратегічно важливих об'єктів. Важливим кроком у практичній площині стало прийняття Постанови Кабінету Міністрів України № 943 від 9 жовтня 2020 року «Деякі питання об'єктів критичної інформаційної інфраструктури». Цей документ регламентував порядок формування переліку об'єктів КІІ, визначивши чіткі критерії їх ідентифікації, та закріпив за Державною службою спеціального зв'язку та захисту інформації України (Держспецзв'язку) функції державного регулятора та координатора у цій сфері. Таким чином, на державному рівні було сформовано інституційний механізм, покликаний забезпечити цілісність та стійкість національного кіберпростору [3].

Визначення сфери охоплення критичної інфраструктури базується на секторальному принципі, що відповідає кращим європейським практикам. До переліку галузей, які складають основу життєдіяльності держави, віднесено енергетику (включаючи електроенергетику та нафтогазовий комплекс), транспортну галузь, банківський та фінансовий сектори, сферу інформаційних технологій та телекомунікацій, хімічну промисловість, систему охорони здоров'я, а також комунальну сферу, зокрема системи водопостачання та водовідведення (табл.1.1). Окреме місце у цьому переліку посідають сектори оборони та державного управління, стабільність яких є запорукою суверенітету країни. У кожному із зазначених секторів функціонують специфічні інформаційні системи – від систем диспетчерського управління SCADA в

енергетиці до систем електронних платежів у банківській сфері, – які і становлять об’єкти критичної інформаційної інфраструктури [4].

Таблиця 1.1

Ключові сектори критичної інфраструктури та їх інформаційні компоненти

Сектор інфраструктури	**Типові об’єкти**	**Критичні інформаційні системи (об’єкти КІІ)**
Енергетика	АЕС, ТЕС, ГЕС, електричні підстанції, газотранспортна система	Системи диспетчерського управління та збору даних (SCADA), автоматизовані системи комерційного обліку електроенергії (АСКОЕ)
Транспорт	Залізниця, аеропорти, морські порти, метрополітен	Системи управління рухом поїздів/літаків, системи навігації та сигналізації, сервіси продажу квитків
Банківський сектор	Національний банк, системні банки, фондові біржі	Системи електронних платежів (СЕП), процесингові центри, автоматизовані банківські системи (АБС)
Телекомунікації	Мобільні оператори, інтернет-провайдери, телецентри	Білінгові системи, системи управління мережевим трафіком, центри обробки даних (ЦОД)
Державне управління	Міністерства, відомства, ЦНАПи	Єдині державні реєстри, системи електронного документообігу, портали надання державних послуг («Дія»)

З метою ефективного розподілу ресурсів та пріоритезації заходів захисту законодавством запроваджено категоризацію об’єктів критичної інфраструктури за рівнем потенційного впливу на національну безпеку. Виділяють чотири категорії критичності. До І-ї категорії віднесено особливо важливі об’єкти загальнодержавного значення, порушення функціонування яких призводить до виникнення кризової ситуації національного масштабу та може мати транскордонні наслідки. ІІ-а категорія охоплює життєво важливі об’єкти регіонального значення, збій у роботі яких дестабілізує ситуацію в межах одного або кількох регіонів. ІІІ-я категорія включає важливі об’єкти місцевого значення, критичні для територіальних громад, а IV-а категорія – об’єкти локального значення, важливі для функціонування окремих підприємств. Варто підкреслити, що інформаційні системи, які забезпечують управління об’єктами І та ІІ категорій, автоматично класифікуються як об’єкти КІІ, до яких висуваються

найжорсткіші вимоги щодо забезпечення конфіденційності, цілісності та доступності інформації [5] (табл 1.2).

Таблиця 1.2

Категоризація об’єктів критичної інфраструктури за рівнем впливу

Категорія	**Рівень значення**	**Масштаб наслідків у разі порушення функціонування**
I категорія	Загальнодержавний	Кризова ситуація національного рівня; суттєвий вплив на безпеку, економіку, міжнародний імідж держави.
II категорія	Регіональний	Кризова ситуація в межах одного або декількох регіонів; порушення життєдіяльності великих територій.
III категорія	Місцевий	Кризова ситуація локального характеру (місто, район, територіальна громада).
IV категорія	Локальний	Порушення роботи окремого об’єкта або підприємства без значного впливу на зовнішнє середовище.

Емпіричним підтвердженням теоретичних положень щодо критичності зазначеної інфраструктури є історія кіберагресії проти України, яка фактично стала полігоном для випробування новітніх видів кіберзброї в умовах гібридної війни. Аналіз хронології інцидентів дозволяє простежити еволюцію загроз від розвідувальних операцій до відверто деструктивних дій, спрямованих на фізичне знищення інфраструктури. Показовим прецедентом стала кібератака на енергетичний сектор України, що відбулася 23 грудня 2015 року. Група зловмисників, ідентифікована як Sandworm, здійснила скоординоване втручання в інформаційні мережі «Прикарпаттяобленерго», «Київобленерго» та «Чернівціобленерго». Використовуючи шкідливе програмне забезпечення BlackEnergy, хакери отримали доступ до систем телемеханіки та в ручному режимі відключили десятки підстанцій. Наслідком атаки стало знеструмлення близько 230 тисяч споживачів протягом кількох годин . Цей випадок увійшов у світову історію як перший офіційно підтверджений факт успішної кібератаки на енергосистему, що призвела до фізичних наслідків у реальному світі [6].

Продовженням цієї тенденції стала атака у грудні 2016 року на підстанцію «Північна» НЕК «Укренерго». Цього разу агресор застосував ще більш

досконалий інструментарій – шкідливе програмне забезпечення *Industroyer*, яке було спеціально розроблене для автоматизованого перехоплення контролю над промисловими системами управління. Хоча знеструмлення тривало лише близько години, сам факт використання спеціалізованої кіберзброї проти цивільної інфраструктури засвідчив перехід конфлікту на якісно новий рівень .

Найбільш руйнівною за своїми економічними наслідками стала масштабна кібероперація 27 червня 2017 року із використанням вірусу-шифрувальника *NotPetya*. Атака була реалізована через механізм оновлення популярного бухгалтерського програмного забезпечення M.E.Doc, що дозволило зловмисникам одночасно інфікувати мережі тисяч організацій. Жертвами атаки стали ключові об’єкти критичної інфраструктури: державні банки («Ощадбанк», «Укргазбанк»), транспортні вузли (міжнародний аеропорт «Бориспіль», АТ «Укрзалізниця»), енергетичні компанії («Укренерго», ДТЕК), а також телеком-оператори та органи державної влади. Вірус незворотно шифрував дані на жорстких дисках, повністю паралізуючи роботу установ . За оцінками експертів, ця атака завдала українській економіці збитків, що вимірюються сотнями мільйонів доларів, а її глобальні наслідки для транснаціональних корпорацій сягнули 10 мільярдів доларів, що робить *NotPetya* найдорожчою кібератакою в історії людства [7].

З початком повномасштабного військового вторгнення Російської Федерації у лютому 2022 року кібернетичні атаки остаточно інтегрувалися у стратегію ведення бойових дій. Напередодні вторгнення, 15–16 лютого 2022 року, відбулися безпрецедентні за потужністю DDoS-атаки на веб-ресурси Міністерства оборони України, Збройних Сил України та державного банківського сектору («ПриватБанк», «Ощадбанк»). Метою цієї операції було не викрадення даних, а створення інформаційного вакууму, поширення паніки серед населення та блокування фінансових розрахунків у критичний момент . Синхронізація кіберударів із наземними операціями підтвердила тезу про те, що критична інформаційна інфраструктура розглядається супротивником як пріоритетна ціль для нанесення ураження [8].

Сучасні загрози продовжують еволюціонувати, набуваючи ознак терористичної діяльності. Яскравим прикладом є цільова кібератака на інформаційну інфраструктуру АТ «Укрзалізниця», зафіксована у березні 2025 року. Зловмисникам вдалося тимчасово вивести з ладу сервіси онлайн-продажу квитків та порушити роботу внутрішніх систем управління перевезеннями. Урядова команда реагування CERT-UA кваліфікувала цей інцидент як акт кібертероризму, оскільки він був спрямований на дезорганізацію логістичних процесів та ускладнення евакуації цивільного населення , . Ще більш резонансною подією став злам ядра мережі національного мобільного оператора «Київстар» 12 грудня 2023 року. Внаслідок атаки, яку здійснило підконтрольне російським спецслужбам хакерське угруповання, 24 мільйони абонентів залишилися без мобільного зв’язку та доступу до мережі Інтернет. Це призвело до порушення роботи систем оповіщення про повітряну тривогу, терміналів безготівкової оплати та ускладнило комунікацію екстрених служб . Президент компанії назвав цей інцидент найбільшою хакерською атакою на телеком-інфраструктуру у світі, метою якої було руйнування, а не шпигунство [9].

Аналіз наведених фактів дає підстави стверджувати, що порушення функціонування критичної інформаційної інфраструктури має системний, каскадний вплив на державу. Технологічний збій в одному секторі неминуче провокує кризові явища в суміжних галузях: зупинка енергопостачання призводить до колапсу зв’язку та транспорту; блокування банківської системи паралізує торгівлю та логістику. Крім прямих економічних збитків, успішні кібератаки завдають удару по репутації державних інституцій, підривають довіру громадян до спроможності влади забезпечити безпеку та можуть провокувати соціальну напругу. В умовах воєнного стану захист КІІ трансформується з технічного завдання в імператив національної безпеки, що вимагає консолідації зусиль державних органів, приватного сектору та міжнародних партнерів [10].

1.2. Поняття кіберстійкості та її основні характеристики

Зростання інтенсивності, складності та асиметричності кіберзагроз, що спостерігається протягом останнього десятиліття, зумовило необхідність перегляду фундаментальних парадигм у сфері захисту інформації. Традиційна модель кібербезпеки (cybersecurity), яка базувалася на концепції «захищеного периметру» та превентивних заходах (недопущення інциденту), виявилася недостатньо ефективною в умовах сучасного динамічного середовища. Глобальна цифровізація розмила чіткі межі корпоративних мереж, а поява нових векторів атак (зокрема, загроз нульового дня та складних сталих загроз – APT) зробила ймовірність успішного проникнення зловмисника питанням часу, а не можливості. Відповіддю на ці виклики стала концепція кіберстійкості (cyber resilience), яка зміщує фокус уваги з запобігання атакам на забезпечення життєздатності системи в умовах перманентного ворожого впливу [11].

У сучасній науковій літературі та міжнародних нормативних документах термін «кіберстійкість» інтерпретується як інтегральна характеристика системи. Національний інститут стандартів і технологій США (NIST) у своїй фундаментальній роботі SP 800-160 Vol. 2 визначає кіберстійкість як «здатність передбачати, витримувати, відновлюватися та адаптуватися до несприятливих умов, навантажень, атак або компрометацій систем, що використовують або забезпечуються кіберресурсами» . Це визначення підкреслює, що кіберстійкість не є статичним станом захищеності, а являє собою динамічний процес управління ризиками протягом усього життєвого циклу системи. Європейське агентство з мережевої та інформаційної безпеки (ENISA) доповнює це розуміння, акцентуючи увагу на тому, що кіберстійкість – це спроможність організації продовжувати виконання своєї місії та надавати послуги навіть у випадку, коли компоненти її IT-інфраструктури скомпрометовані або виведені з ладу [12].

Принципова відмінність між поняттями «кібербезпека» та «кіберстійкість» полягає у зміні філософії захисту (табл. 1.3).

Таблиця 1.3

Порівняльна характеристика концепцій кібербезпеки та кіберстійкості

Критерій порівняння	**Кібербезпека (Cybersecurity)**	**Кіберстійкість (Cyber Resilience)**
Основна мета	Запобігти атаці та захистити дані.	Забезпечити безперервність бізнес-процесів.
Базове припущення	Систему можна зробити невразливою («Фортеця»).	Інцдент неминучий («Питання часу»).
Фокус уваги	Захист периметру, контроль доступу, превенція.	Виявлення, реагування, відновлення, адаптація.
Результат	Відсутність інцидентів (в ідеалі).	Виживання системи та збереження функціональності під час інциденту.
Часовий горизонт	До моменту атаки.	Протягом усього циклу (до, під час і після атаки).

Кібербезпека традиційно орієнтована на забезпечення конфіденційності, цілісності та доступності інформації (тріада CIA) шляхом впровадження технічних засобів контролю доступу, шифрування та антивірусного захисту. Її головна мета – «не допустити ворога всередину». Натомість кіберстійкість виходить із песимістичного, але реалістичного припущення, що будь-який захист може бути подолано. Тому головною метою стає не уникнення інциденту за будь-яку ціну, а забезпечення безперервності бізнес-процесів (Business Continuity) та мінімізація негативних наслідків успішної атаки . Якщо кібербезпека відповідає на питання «Як ми можемо захиститися?», то кіберстійкість ставить питання «Як ми будемо функціонувати, коли нас зламають?».

Аналіз міжнародних стандартів та кращих практик (NIST, ISO 22301, MITRE) дозволяє виокремити чотири фундаментальні атрибути (або цілі) кіберстійкої системи (Рис. 1.1), які формують замкнений цикл адаптивного управління.

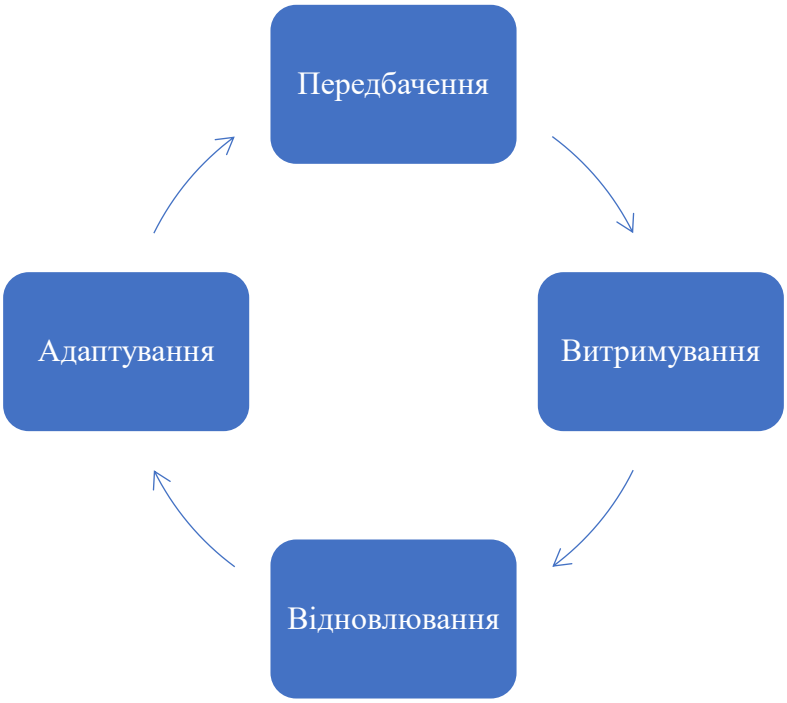

Рис. 1.1. Цілі кіберстійкості системи

Першим атрибутом є здатність передбачати (Anticipate). Це проактивна складова кіберстійкості, яка передбачає діяльність із випередження загроз до моменту їх реалізації. Організація повинна підтримувати стан постійної ситуаційної обізнаності, що досягається шляхом впровадження процесів кіберрозвідки (Threat Intelligence). Це включає збір та аналіз інформації про тактики, техніки та процедури (TTPs) потенційних зловмисників, моніторинг вразливостей у програмному забезпеченні, а також моделювання можливих векторів атак. Важливим елементом передбачення є також проведення регулярних навчань персоналу (кібернавчань) та стрес-тестувань систем, що дозволяє виявити слабкі місця в архітектурі безпеки до того, як ними скористається ворог [13].

Другим атрибутом є здатність витримувати (Withstand). Ця характеристика визначає спроможність системи продовжувати виконання критично важливих функцій безпосередньо під час атаки або в умовах підвищеного навантаження. Технічна реалізація цієї здатності базується на принципах відмовостійкості та живучості. До ключових механізмів належать: резервування критичних вузлів (надлишковість), сегментація мережі для обмеження горизонтального

переміщення зловмисника (принцип Zero Trust), а також використання гетерогенних (різноманітних) компонентів, що ускладнює експлуатацію однієї вразливості для враження всієї системи. Система повинна вміти працювати в режимі деградованої функціональності, коли другорядні сервіси відключаються заради збереження працездатності ядра [14].

Третім атрибутом є здатність відновлюватися (Recover). Цей аспект характеризує еластичність системи, тобто швидкість її повернення до штатного режиму функціонування після інциденту. Ефективність відновлення визначається такими показниками, як цільовий час відновлення (Recovery Time Objective – RTO) та цільова точка відновлення (Recovery Point Objective – RPO). Забезпечення цієї здатності вимагає наявності детально розроблених та протестованих планів аварійного відновлення (Disaster Recovery Plan – DRP) і планів забезпечення безперервності бізнесу (Business Continuity Plan – BCP). Критично важливим є створення надійної системи резервного копіювання даних, яка повинна включати створення незмінних (immutable) копій та їх зберігання в ізольованому від основної мережі середовищі (air-gapped backups), що унеможливлює їх знищення вірусами-шифрувальниками [15].

Четвертим атрибутом є здатність адаптуватися (Adapt). Кіберстійкість – це не кінцевий стан, а постійний процес еволюції. Після кожного інциденту, навіть якщо він був успішно нейтралізований, організація повинна проводити ретельний аналіз (post-incident review) для встановлення кореневих причин та оцінки ефективності заходів реагування. На основі отриманих уроків («lessons learned») здійснюється модифікація архітектури системи, оновлення політик безпеки та коригування процедур. Адаптивність дозволяє системі «навчатися» на власному досвіді, підвищуючи свій імунітет до майбутніх атак. Система, що не здатна до адаптації, з часом неминуче втрачає свою ефективність перед обличчям еволюціонуючих загроз .

В українському контексті концепція кіберстійкості набула унікального практичного втілення в умовах повномасштабної війни, ставши ключовим фактором збереження керованості державою. Екстремальні умови бойових дій

змусили Україну реалізувати безпрецедентні за своїми масштабами та швидкістю заходи із забезпечення життєздатності цифрової інфраструктури. Одним із найяскравіших прикладів успішної реалізації стратегії кіберстійкості стала масштабна міграція державних інформаційних ресурсів у хмарні середовища [16].

Ще до початку повномасштабного вторгнення, розуміючи ризики фізичного знищення наземних дата-центрів внаслідок ракетних обстрілів, Верховна Рада України оперативно внесла зміни до законодавства, дозволивши розміщення державних реєстрів та баз даних на серверах за межами країни (що раніше було заборонено з міркувань суверенітету даних). Це відкрило шлях до співпраці з провідними світовими технологічними компаніями, такими як Amazon Web Services (AWS), Microsoft Azure, Google Cloud та Oracle. У найкоротші терміни було здійснено перенесення критично важливих даних, що забезпечило їх збереження та доступність. Цей крок дозволив державі продовжувати надавати адміністративні та соціальні послуги громадянам (зокрема, через екосистему «Дія»), здійснювати пенсійні виплати та забезпечувати функціонування банківської системи навіть в умовах блекаутів та руйнування фізичної інфраструктури зв’язку .

Окрім технологічної трансформації, Україна суттєво посилила інституційну спроможність системи кіберзахисту. У 2025 році було затверджено Національний план реагування на кіберінциденти, який став нормативним фундаментом для уніфікації процедур взаємодії між різними суб’єктами сектору безпеки і оборони, а також приватним сектором. Цей документ ввів чітку класифікацію інцидентів за рівнями критичності та визначив алгоритми ескалації реагування. Важливим елементом стало розширення повноважень урядової команди реагування на комп’ютерні надзвичайні події України (CERT-UA), яка отримала право оперативно втручатися в роботу інформаційних систем об’єктів критичної інфраструктури для локалізації загроз, що дозволяє зупиняти поширення атак на ранніх стадіях [17].

Також варто відзначити роль міжнародного співробітництва у підвищенні національної кіберстійкості. Україна інтегрувалася в європейську систему обміну інформацією про кіберзагрози, налагодивши постійну комунікацію з ENISA та кіберцентрами країн-партнерів. Отримання даних про індикатори компрометації (IoCs) в режимі реального часу дозволяє українським фахівцям реалізувати функцію «передбачення», блокуючи шкідливу активність ще до того, як вона завдасть шкоди.

Таким чином, українська модель кіберстійкості демонструє ефективне поєднання технологічних інновацій (хмарні технології, децентралізація), організаційних реформ (нові регламенти реагування) та людського капіталу. Досвід України підтверджує тезу про те, що в умовах сучасних гібридних конфліктів кіберстійкість перестає бути суто технічною дисципліною і трансформується у стратегічний імператив національної безпеки, від якого безпосередньо залежить здатність держави виживати та перемагати.

1.3. Гібридні загрози: визначення, види та тенденції розвитку

Трансформація геополітичного ландшафту XXI століття характеризується зміною природи міждержавних конфліктів. Класична концепція війни, що передбачає пряме військове зіткнення армій на полі бою, поступово поступається місцем стратегіям непрямих дій, де застосування військової сили є лише одним із елементів (і часто не вирішальним) широкого спектру інструментів примусу. Цей феномен у науковому та політичному дискурсі отримав назву «гібридна війна», а сукупність деструктивних впливів, що в ній застосовуються, – «гібридні загрози». У контексті захисту критичної інфраструктури розуміння сутності гібридних загроз є фундаментальним, оскільки саме вони визначають вектор атак на інформаційні системи держави.

Поняття гібридних загроз є складним та багатовимірним конструктом, що не має єдиного універсального визначення, проте провідні міжнародні безпекові інституції демонструють консенсус щодо його ключових ознак.

Північноатлантичний альянс (НАТО) визначає гібридні загрози як поєднання військових і невійськових, а також відкритих і прихованих засобів, включаючи дезінформацію, кібератаки, економічний тиск, розгортання іррегулярних збройних формувань та використання регулярних військ . Гібридні методи застосовуються для розмивання меж між війною та миром, посіяння сумнівів у свідомості цільової аудиторії та дестабілізації суспільства. Європейський Союз у своїй доктринальній базі підкреслює, що гібридні загрози – це скоординовані та синхронізовані дії зловмисного характеру, спрямовані на використання вразливостей демократичних держав та підрив їхніх інституцій . Головною метою гібридної агресії є не фізичне захоплення території (хоча це не виключається як кінцева фаза), а зламування волі супротивника до опору шляхом створення внутрішнього хаосу та паралічу систем управління [18].

Структура гібридних загроз (рис. 1.2) характеризується інтеграцією кількох доменів впливу, де кожен компонент підсилює дію іншого (синергетичний ефект). Кіберпростір у цій архітектурі відіграє роль універсального «мультиплікатора сили», оскільки дозволяє впливати на всі сфери життєдіяльності держави дистанційно, анонімно та з мінімальними витратами ресурсів.

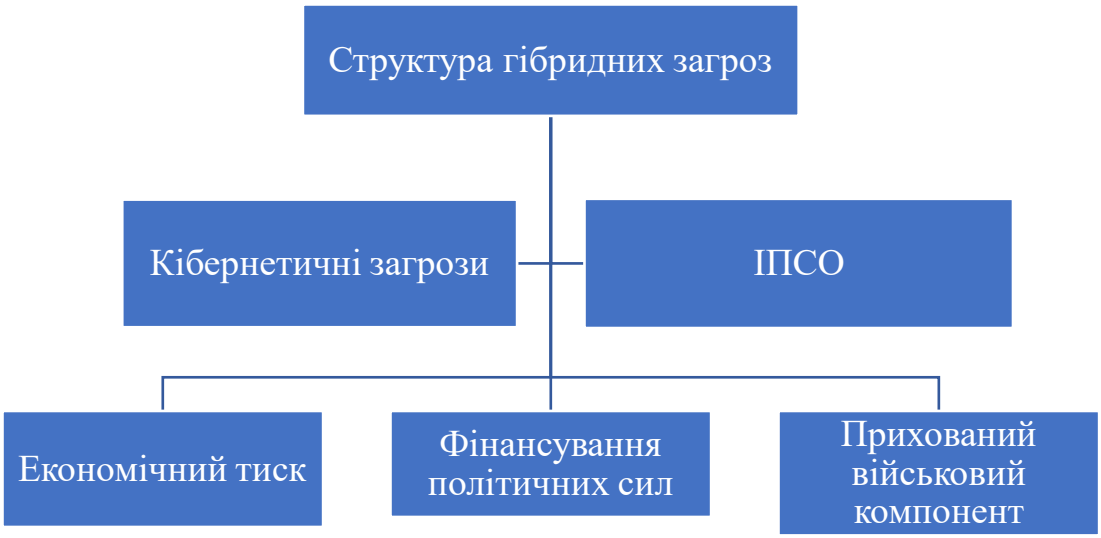

Рис. 1.2. Структура гібридних загроз

По-перше, кібернетичні загрози як самостійний вид зброї. Вони використовуються для проведення операцій кібершпигунства (ексфільтрація конфіденційної інформації з державних органів), саботажу (порушення роботи промислових систем управління) та підготовки плацдарму для кінетичних дій. Особливістю кіберзброї є її здатність завдавати фізичної шкоди інфраструктурі (наприклад, виведення з ладу електростанцій або транспортних вузлів) без необхідності перетину кордону військовими підрозділами. Проблема атрибуції (складність встановлення джерела атаки) дозволяє державі-агресору уникати політичної та юридичної відповідальності, діючи під «чужим прапором» (false flag operations).

По-друге, інформаційно-психологічні операції (ІПСО), що реалізуються через кіберпростір. Цей вид загроз спрямований на когнітивну сферу – свідомість громадян та процес прийняття рішень лідерами держави. Інструментарій ІПСО включає поширення дезінформації (fake news), пропаганду, маніпуляцію громадською думкою через соціальні мережі («ферми ботів») та соціальну інженерію. Кібертехнології дозволяють автоматизувати процес доставки контенту, таргетовано впливаючи на конкретні соціальні групи для поляризації суспільства та розпалювання ворожнечі. Яскравим прикладом є використання цифрових платформ для втручання у виборчі процеси, що підриває легітимність демократичних інститутів .

По-третє, економічний тиск, посилений кібератаками. Сюди відносяться енергетичний шантаж, торговельні ембарго, блокування транспортних коридорів та атаки на фінансовий сектор. Злам банківських систем або блокування платіжних шлюзів здатні спровокувати фінансову паніку, девальвацію національної валюти та інвестиційну кризу, що значно послаблює економічний потенціал держави-жертви.

По-четверте, Агресор може використовувати кіберзасоби для фінансування та координації радикальних політичних рухів, організації протестних акцій та дискредитації політичного керівництва країни. Метою таких

дій є делегітимізація влади та створення умов для зміни політичного курсу держави [19].

По-п’яте, прихований військовий компонент. Це використання сил спеціальних операцій (ССО), приватних військових компаній (ПВК) та місцевих колаборантів без розпізнавальних знаків (так звані «зелені чоловічки»). Кіберрозвідка забезпечує ці підрозділи необхідною інформацією про переміщення військ супротивника та стан його оборони .

Динаміка розвитку технологій визначає постійну еволюцію гібридних загроз. Аналіз звітів провідних аналітичних центрів та досвіду російсько-української війни дозволяє виділити низку тривожних тенденцій, які формуватимуть ландшафт безпеки у найближчі роки (табл.1.4).

Таблиця 1.4.

Актуальні тенденції розвитку гібридних кіберзагроз

Тенденція	**Сутність загрози**	**Потенційний вплив на КІ**
ШІ та Deepfakes	Використання штучного інтелекту для створення фішингу, шкідливого коду та дезінформації.	Автоматизація атак, обхід традиційних засобів захисту, дискредитація керівництва.
Supply Chain Attacks	Атака на захищену ціль через вразливості її підрядників або постачальників ПЗ.	Отримання прихованого доступу до критичних мереж через довірені канали.
Ransomware 2.0 / Wipers	Використання програм-вимагачів для маскування шпигунства або повного знищення даних.	Параліч економічної діяльності, втрата критично важливої інформації без можливості відновлення.
Кібер-фізичні атаки (IoT)	Злам підключених пристроїв (сенсорів, камер, контролерів) у промислових мережах.	Фізичне пошкодження обладнання, техногенні аварії, загроза життю персоналу.

Однією з ключових тенденцій є мілітаризація штучного інтелекту (ШІ). Зловмисники дедалі активніше використовують технології Generative AI для автоматизації кібератак. ШІ дозволяє створювати унікальний шкідливий код, який здатний обходити традиційні системи захисту (поліморфні віруси), а також генерувати високоякісні фішингові листи, які неможливо відрізнити від легітимної кореспонденції. Особливу небезпеку становить технологія Deepfake (глибинні фейки) – створення реалістичних синтетичних відео- та аудіозаписів. Цей інструмент може бути використаний для

фальсифікації заяв політичних лідерів (наприклад, фейкове звернення Президента про капітуляцію), дискредитації військового командування або шантажу посадових осіб [20].

Другим важливим трендом є зміщення вектору атак на ланцюги постачання (Supply Chain Attacks). Оскільки захист критичних об'єктів (банків, міністерств) постійно посилюється, хакери шукають слабкі ланки в їхньому оточенні. Компрометація довіреного постачальника програмного забезпечення або послуг дозволяє зловмисникам отримати прихований доступ до мереж сотень і тисяч його клієнтів. Класичним прикладом такої атаки є інцидент із SolarWinds, який вразив урядові структури США. В Україні подібна тактика була використана під час атаки NotPetya через ПЗ M.E.Doc. Агентство Європейського Союзу з кібербезпеки (ENISA) визначає атаки на ланцюги постачання як одну з головних загроз для європейської безпеки, оскільки вони підривають саму основу довіри в цифровій екосистемі [21].

Третя тенденція пов'язана з трансформацією феномену програм-вимагачів (Ransomware). Якщо раніше такі атаки здійснювалися переважно кіберзлочинцями з метою фінансового збагачення, то сьогодні вони стають інструментом у руках державних хакерів (state-sponsored actors). Агресори використовують шифрувальники як «димову завісу» для маскування деструктивних дій або шпигунства. Крім того, з'явилися так звані «вайпери» (Wipers) – шкідливі програми, які імітують роботу вірусів-вимагачів, але фактично призначені для безповоротного знищення даних без можливості їх відновлення. Такі інструменти використовуються для нанесення максимальних економічних збитків супротивнику в умовах конфлікту.

Четвертим напрямком є зростання загрози кібертероризму та конвергенція кібернетичного і фізичного світів. Поширення технологій Інтернету речей (IoT) у критичній інфраструктурі (розумні міста, автоматизовані системи управління транспортом, медичне обладнання) значно розширює поверхню атаки. Злам незахищених IoT-пристроїв може бути використаний не лише для створення ботнетів, а й для організації техногенних катастроф, порушення роботи

медичних закладів або транспортного колапсу, що створює безпосередню загрозу життю людей [22].

Таким чином, гібридні загрози являють собою складний, адаптивний механізм агресії, що постійно вдосконалюється. Ефективна протидія їм вимагає виходу за рамки суто технічного розуміння кібербезпеки та впровадження комплексного підходу, що поєднує технологічні, інформаційні, правові та дипломатичні інструменти захисту на рівні всієї держави.

1.4. Міжнародні стандарти та нормативно-правові акти у сфері забезпечення кіберстійкості

Ефективне забезпечення кіберстійкості критичної інфраструктури неможливе в рамках ізольованого національного підходу. Глобальний характер кіберзагроз вимагає уніфікації методів захисту, термінології та процедур реагування. Саме тому фундаментом побудови національних систем кібербезпеки виступають міжнародні стандарти та регуляторні практики провідних світових гравців. Для України, яка закріпила курс на євроінтеграцію, гармонізація вітчизняного законодавства з нормами ЄС та стандартами НАТО є не лише політичним зобов’язанням, а й технологічною необхідністю для забезпечення сумісності систем безпеки.

У світовій практиці сформувався комплекс стандартів, які регламентують різні аспекти кіберстійкості: від управління ризиками до інженерії систем (табл.1.5). Серед них ключове місце посідають розробки Національного інституту стандартів і технологій США (NIST), Міжнародної організації зі стандартизації (ISO) та нормативні акти Європейського Союзу.

Таблиця 1.5

Ключові міжнародні стандарти та нормативи у сфері кіберстійкості

Стандарт / Документ	**Розробник / Регіон**	**Сфера застосування**	**Основний фокус**
NIST CSF 2.0	США (NIST)	Універсальний	Управління ризиками через функції: Govern, Identify, Protect, Detect, Respond, Recover.

Продовження таблиці 1.5

NIST SP 800-160 Vol.2	США (NIST)	Інженерія систем	Побудова архітектури кіберстійких систем (Cyber Resilient Systems).
ISO 22301	ISO (Міжнародний)	Менеджмент	Забезпечення безперервності бізнесу (Business Continuity).
NIS2 Directive	Європейський Союз	Загальнодержавний	Посилення кібербезпеки в критичних секторах, відповідальність менеджменту.
DORA	Європейський Союз	Фінансовий сектор	Цифрова операційна стійкість фінансових установ та їхніх IT-постачальників.

Стандарти NIST

Найбільш впливовим документом у цій сфері є NIST Cybersecurity Framework (CSF). Хоча він розроблявся для критичної інфраструктури США, завдяки своїй гнучкості та універсальності він став де-факто глобальним стандартом. Структура CSF базується на п’яти (в оновленій версії 2.0 – шести) функціях ядра, які описують життєвий цикл управління кібер ризиками (рис. 1.3):

1. Govern (Управління). Визначення стратегії, політик та організаційної культури безпеки.
2. Identify (Ідентифікація). Розуміння контексту, активів та ризиків організації.
3. Protect (Захист). Впровадження гарантій для забезпечення надання критичних послуг.
4. Detect (Виявлення). Своєчасна ідентифікація подій кібербезпеки.
5. Respond (Реагування). Вжиття заходів щодо виявленого інциденту.
6. Recover (Відновлення). Відновлення можливостей або послуг, які були порушені .

Для українських об’єктів КІІ цей фреймворк є методичною основою при розробці відомчих планів захисту, оскільки дозволяє оцінити поточний рівень зрілості (Tiers) та сформувати дорожню карту його підвищення [23].

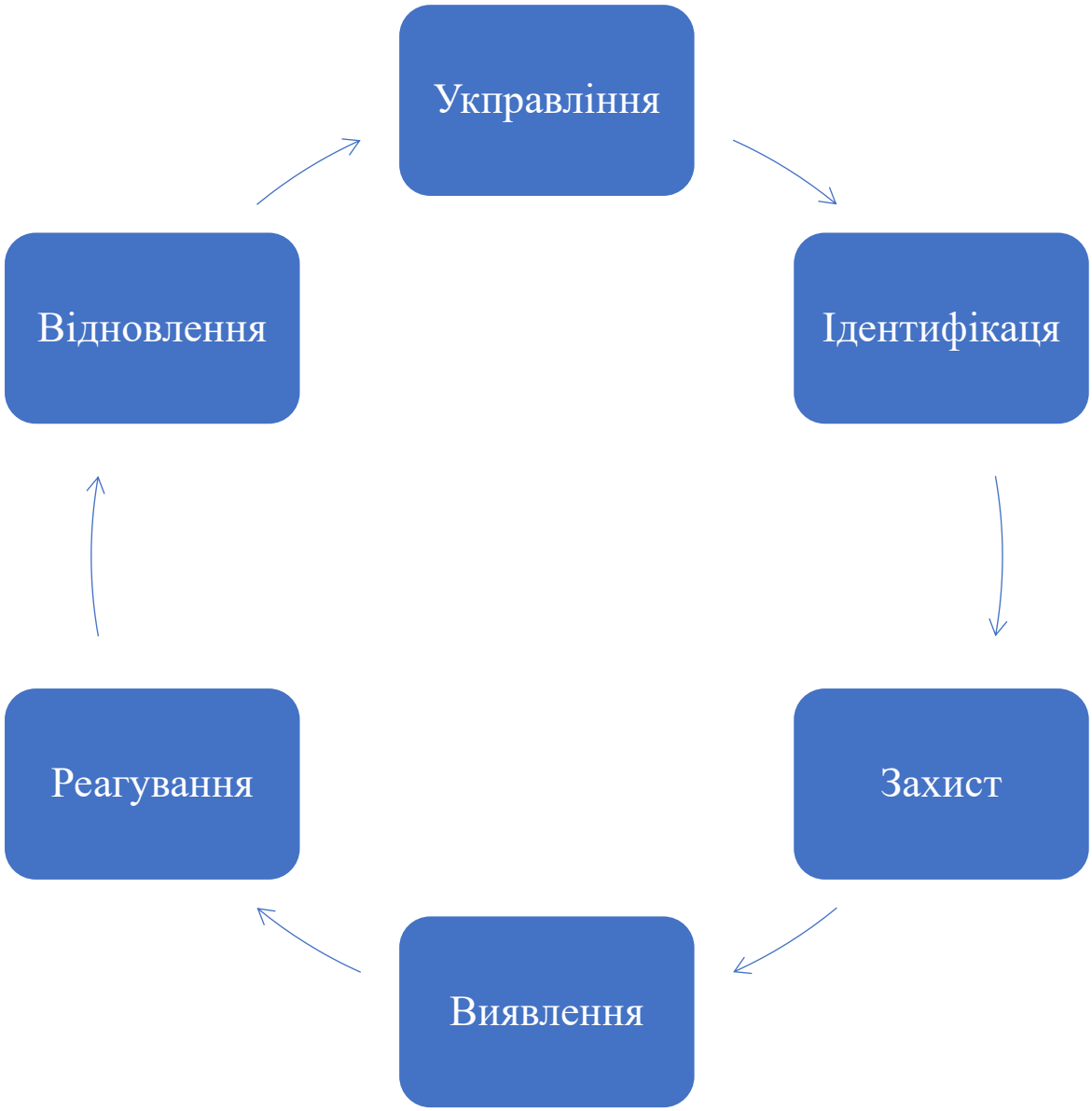

Рис. 1.3. Життєвий цикл управління кібер ризиками

Окреме місце посідає спеціальна публікація NIST SP 800-160 Vol. 2 (Developing Cyber Resilient Systems). Це перший у світі системний стандарт інженерії кіберстійкості. Він пропонує розглядати стійкість не як «надбудову» над системою, а як її невід'ємну архітектурну властивість. Документ визначає набір патернів проєктування (design patterns), таких як адаптивна реакція, аналітичний моніторинг, скоординований захист, різноманітність (diversity) та надлишковість (redundancy), впровадження яких дозволяє системі функціонувати навіть в умовах часткової компрометації .

Стандарти серії ISO/IEC

Міжнародні стандарти ISO забезпечують процедурну основу менеджменту безпеки:

- ISO/IEC 27001: встановлює вимоги до Системи управління інформаційною безпекою (ISMS). Його цінність полягає у впровадженні циклічного підходу PDCA (Plan-Do-Check-Act), що забезпечує постійне вдосконалення процесів захисту.
- ISO 22301 (Business Continuity): є критично важливим саме в контексті кіберстійкості. Цей стандарт регламентує процеси забезпечення безперервності бізнесу. Він вимагає від організацій проведення аналізу впливу на бізнес (Business Impact Analysis – BIA), визначення критичних процесів та розробки стратегій їх відновлення у визначені терміни (RTO/RPO). Без відповідності цьому стандарту неможливо гарантувати, що об’єкт КІІ зможе пережити масштабну атаку.
- ISO/IEC 27032: фокусується безпосередньо на кібербезпеці як стані захищеності кіберпростору, регулюючи взаємодію між різними стейкхолдерами в Інтернеті .

Регуляторне поле Європейського Союзу

ЄС останніми роками здійснив справжню революцію в законодавстві, перейшовши від рекомендаційних директив до жорстких регламентів прямої дії, які формують єдиний цифровий простір безпеки.

По-перше, Директива NIS2 (Network and Information Security Directive 2), прийнята у 2022 році. Вона замінила попередню директиву NIS, значно посиливши вимоги. Ключові новації документу:

- розширення сфери дії на нові сектори (виробництво продуктів харчування, поштові послуги, управління відходами, космос, хімічна промисловість);
- запровадження персональної відповідальності топ-менеджменту за невиконання вимог кібербезпеки (аж до тимчасової заборони обіймати керівні посади);

– жорсткі вимоги до звітування про інциденти: «раннє попередження» має бути надіслане регулятору протягом 24 годин після виявлення загрози;

– обов’язковий контроль безпеки ланцюгів постачання (supply chain security), що змушує операторів КІІ перевіряти кібергігієну своїх підрядників .

По-друге, Регламент DORA (Digital Operational Resilience Act), який набуває чинності у 2025 році. Це спеціалізований нормативний акт для фінансового сектору (банки, страхові компанії, інвестиційні фірми). DORA встановлює унікальні вимоги до цифрової операційної стійкості: фінансові установи зобов’язані не лише захищатися, а й доводити свою здатність витримувати атаки шляхом проведення просунутих тестувань на проникнення (TLPT – Threat-Led Penetration Testing). Крім того, DORA вперше вводить прямий нагляд європейських регуляторів за критичними постачальниками ІКТ-послуг (зокрема хмарними провайдерами, такими як AWS чи Microsoft), що раніше перебували у «сірій зоні» регулювання [24].

По-третє, Директива CER (Critical Entities Resilience). Вона доповнює NIS2, фокусуючись на фізичній стійкості критичних об’єктів. Директива визнає, що загрози можуть мати гібридний характер (наприклад, кібератака, поєднана з фізичною диверсією або природним лихом). Тому вона зобов’язує держави-члени проводити національну оцінку ризиків з урахуванням усіх видів небезпек (all-hazards approach) та забезпечувати фізичний захист інфраструктури .

Аналіз міжнародної нормативної бази свідчить про зміну глобального підходу: від точкового захисту інформації до побудови комплексних екосистем стійкості. Для України імплементація положень NIS2, DORA та стандартів NIST є безальтернативним шляхом. Закон України «Про критичну інфраструктуру» вже містить низку положень, співзвучних із Директивою CER, а вимоги Національного банку до кіберзахисту банківської системи багато в чому відповідають філософії DORA. Однак повноцінна інтеграція вимагає подальшої гармонізації законодавства, зокрема в частині класифікації інцидентів, посилення відповідальності бізнесу та запровадження дієвих механізмів державно-приватного партнерства [25].

Висновки до розділу 1

Проведене у першому розділі теоретико-методологічне дослідження дозволяє сформулювати низку узагальнюючих висновків, які розкривають сутність проблеми забезпечення кіберстійкості критичної інфраструктури в сучасних умовах.

Критична інформаційна інфраструктура (КІІ) як центр тяжіння національної безпеки у XXI столітті КІІ трансформувалася з сукупності технічних засобів у фундаментальну основу існування держави. Забезпечення життєдіяльності суспільства – від енергопостачання та фінансових розрахунків до управління обороною – повністю залежить від безперебійного функціонування інформаційних систем. Як свідчить досвід України, яка стала об'єктом безпрецедентної кіберагресії (атаки BlackEnergy, NotPetya, атаки на «Київстар»), порушення роботи КІІ здатне спровокувати системну кризу, паралізувати економіку та дестабілізувати суспільно-політичну ситуацію. Тому захист КІІ є стратегічним пріоритетом, рівнозначним захисту територіальної цілісності.

Традиційна концепція кібербезпеки, орієнтована на запобігання інцидентам, вичерпала свій потенціал в умовах асиметричних загроз. Сучасною відповіддю на виклики є концепція кіберстійкості (cyber resilience) – здатності системи функціонувати в умовах постійного ворожого впливу. Вона базується на чотирьох стовпах: передбаченні загроз, витривалості під час атаки, швидкому відновленні та постійній адаптації. Український кейс (зокрема, міграція даних у хмару та збереження цифрових сервісів під час війни) довів життєздатність та ефективність саме такого підходу.

Кіберпростір став ключовим доменом гібридної війни. Загрози для КІІ більше не є ізольованими технічними інцидентами; вони є частиною скоординованих кампаній, що включають інформаційно-психологічний тиск, економічний шантаж та фізичні диверсії. Технологічні тренди – використання штучного інтелекту, атаки на ланцюги постачання, кібертероризм – вимагають

від держави застосування комплексних контрзаходів, що виходять за межі компетенції лише IT-спеціалістів і потребують залучення всіх суб'єктів сектору безпеки.

Побудова ефективної системи кіберстійкості неможлива без уніфікації підходів на основі міжнародних стандартів (NIST, ISO) та регуляторних практик ЄС (NIS2, DORA, CER). Ці документи задають високу планку вимог до управління ризиками, безперервності бізнесу та взаємодії стейкхолдерів. Для України їх імплементація є не лише умовою євроінтеграції, а й необхідним кроком для побудови сумісної з партнерами архітектури колективної безпеки.

Таким чином, забезпечення кіберстійкості критичної інфраструктури є складним, багатофакторним завданням, вирішення якого вимагає системного підходу, поєднання нормативно-правових, організаційних та технічних механізмів, а також постійної адаптації до змінного ландшафту загроз.

РОЗДІЛ 2
АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

2.1. Методи управління ризиками та оцінки загроз у критичній інфраструктурі

Сучасна парадигма забезпечення національної безпеки зазнає фундаментальних трансформацій, зумовлених стрімкою цифровізацією всіх сфер суспільного життя та зростанням рівня загроз у кіберпросторі. Критична інфраструктура держави, яка включає енергетичні, транспортні, фінансові та комунікаційні системи, стає головною мішенню в умовах гібридних конфліктів. У цьому контексті забезпечення кіберстійкості (cyber resilience) виходить за рамки суто технічного завдання і набуває статусу стратегічного пріоритету. На відміну від традиційної концепції кібербезпеки, яка фокусується на побудові захищених периметрів та намаганні унеможливити проникнення зловмисника, концепція кіберстійкості базується на ймовірнісному підході. Вона визнає неминучість інцидентів та спрямовує зусилля на забезпечення безперервності функціонування критичних сервісів навіть в умовах деструктивного впливу. Фундаментом такої системи є процес управління ризиками, який дозволяє ідентифікувати потенційні загрози, оцінити їхній можливий вплив та розробити адекватні заходи реагування [26].

Теоретико-методологічні основи управління ризиками

Управління ризиками інформаційної безпеки являє собою системний, циклічний процес, який охоплює ідентифікацію, аналіз, оцінювання та обробку ризиків, що загрожують активам організації. Науково-методичний апарат цього процесу базується на комплексі міжнародних стандартів, які забезпечують уніфікацію підходів та створюють спільну термінологічну базу для фахівців усього світу. Одним із ключових нормативних документів у цій сфері є спеціальна публікація Національного інституту стандартів і технологій США

NIST SP 800-30 Rev. 1 «Guide for Conducting Risk Assessments». Цей стандарт, який де-факто став еталонним для країн-членів НАТО, пропонує загрозо-орієнтований підхід до оцінки ризиків. Його особливість полягає в тому, що аналіз починається не з активів, а з вивчення можливостей, намірів та методів потенційних зловмисників. Такий підхід є найбільш релевантним для захисту критичної інфраструктури, яка постійно перебуває під прицілом висококваліфікованих хакерських угруповань, спонсорованих іноземними державами.

Процес оцінки ризиків згідно з методологією NIST структурований у чотири послідовні етапи (рис. 2.1).

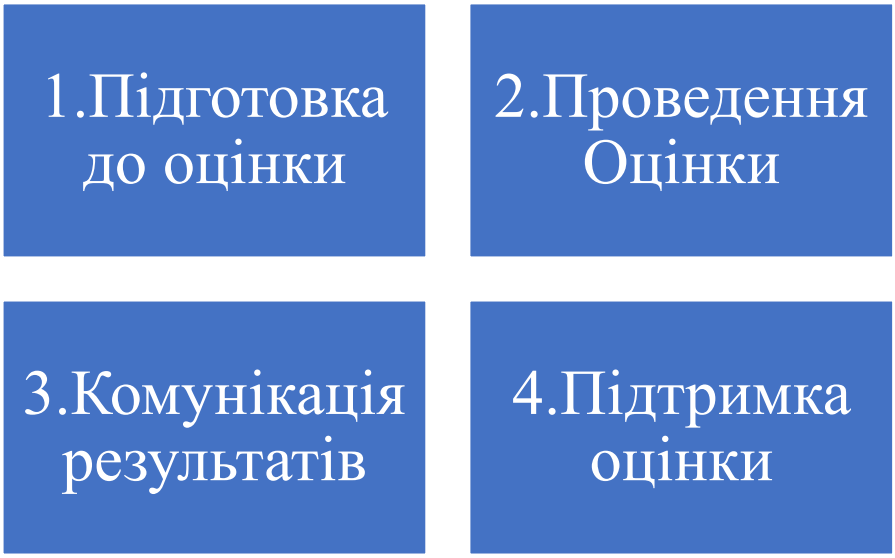

Рис.2.1. Оцінка ризиків згідно з методологією NIST

Перший етап – підготовка до оцінки – має критичне значення для успіху всього процесу. На цьому етапі організація повинна чітко визначити мету оцінки, її масштаб (охоплення конкретних систем чи всієї інфраструктури), а також встановити припущення та обмеження, пов'язані з ресурсами та часовими рамками. Важливим аспектом підготовки є визначення джерел інформації про загрози, які будуть використовуватися в аналізі, а також встановлення критеріїв оцінки ризику. Організація має сформулювати свою толерантність до ризику

(risk tolerance), тобто визначити той рівень ризику, який керівництво готове прийняти без вжиття додаткових заходів мітигації [27].

Другий етап – проведення оцінки – є аналітичним ядром процесу. Він передбачає виконання низки взаємопов'язаних дій. Насамперед здійснюється ідентифікація джерел загроз, які можуть мати як ворожий характер (кіберзлочинці, хактивісти, інсайдери), так і неворожий (технічні збої, помилки персоналу, природні явища). Далі визначаються події загроз, тобто конкретні сценарії, за якими джерело загрози може вплинути на систему. Наступним кроком є ідентифікація вразливостей в інформаційних системах, процедурах безпеки або внутрішніх контролях, які можуть бути експлуатовані джерелами загроз. На основі зібраних даних експерти визначають ймовірність реалізації кожного сценарію загрози та оцінюють потенційний вплив такої реалізації на місію організації, її активи та репутацію. Синтез показників ймовірності та впливу дозволяє розрахувати рівень ризику.

Третій етап – комунікація результатів – спрямований на забезпечення обізнаності осіб, що приймають рішення. Результати оцінки ризиків повинні бути представлені у зрозумілій для бізнес-керівництва формі, що дозволить обґрунтувати необхідність виділення бюджетів на заходи безпеки.

Четвертий етап – підтримка оцінки – забезпечує актуалізацію результатів у часі. Оскільки ландшафт кіберзагроз змінюється надзвичайно динамічно, а в інфраструктурі постійно з'являються нові елементи, оцінка ризиків не може бути одноразовою дією. Вона вимагає постійного моніторингу факторів ризику та перегляду оцінок у разі суттєвих змін у середовищі функціонування системи [28].

Альтернативним, але не менш важливим підходом є методологія, викладена в міжнародних стандартах серії ISO. Стандарт ISO 31000:2018 «Risk Management – Guidelines» надає загальну архітектуру управління ризиками, яка може бути застосована до будь-якої сфери діяльності. У контексті інформаційної безпеки цей підхід деталізується стандартом ISO/IEC 27005:2022. Особливістю методології ISO є використання актив-орієнтованого підходу. Згідно з ним,

процес оцінки ризиків починається з повної інвентаризації активів організації – інформації, процесів, програмного та апаратного забезпечення. Для кожного активу визначається його цінність та критичність для бізнес-процесів. Лише після цього здійснюється ідентифікація загроз, які можуть вплинути на конкретний актив, та вразливостей, притаманних цьому активу. Такий підхід дозволяє забезпечити повноту покриття ризиків, гарантуючи, що жоден критичний елемент інфраструктури не залишиться поза увагою аналітиків [29].

Класифікація ризиків у середовищі критичної інфраструктури

Специфіка критичної інфраструктури полягає у глибокій конвергенції інформаційних технологій (IT) та операційних технологій (OT). Сучасні промислові системи управління (ICS/SCADA), які керують енергомережами, водопостачанням чи транспортом, все частіше інтегруються з корпоративними мережами та підключаються до Інтернету для забезпечення віддаленого моніторингу та управління. Це створює унікальний, гібридний ландшафт ризиків, де кібернетичні загрози можуть мати фізичні наслідки. Якщо в класичних IT-системах головним пріоритетом безпеки є конфіденційність даних, то в системах критичної інфраструктури домінує тріада доступності, цілісності та фізичної безпеки.

Аналіз загроз дозволяє виділити кілька основних категорій ризиків, притаманних критичній інфраструктурі (рис. 2.2).

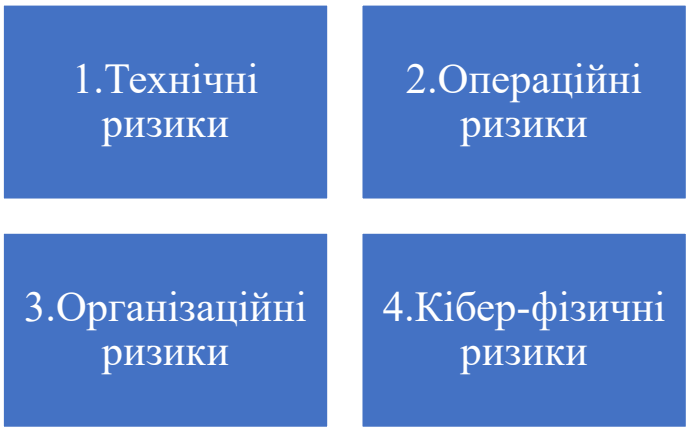

Рис. 2.2. Категорії ризиків, притаманних критичній інфраструктурі

Першу групу складають технічні або технологічні ризики. Вони безпосередньо пов'язані з функціонуванням апаратно-програмних комплексів. До цієї категорії належать ризики, спричинені наявністю вразливостей у програмному забезпеченні контролерів та серверів, використанням слабких алгоритмів шифрування або їх повною відсутністю, помилками в архітектурі мереж. Особливою проблемою для критичної інфраструктури є наявність великої кількості успадкованих систем (legacy systems). Це обладнання, яке було розроблене та впроваджене десятиліття тому, коли питання кібербезпеки не були пріоритетними. Такі системи часто використовують відкриті протоколи передачі даних, мають жорстко закодовані паролі та не підтримують встановлення оновлень безпеки без зупинки технологічного процесу, що робить їх легкою мішенню для зловмисників [30].

Другу групу становлять операційні ризики, які виникають внаслідок недоліків у внутрішніх процесах та процедурах організації. Сюди відносяться помилки персоналу при налаштуванні обладнання, відсутність чітких регламентів реагування на інциденти, неефективність процедур резервного копіювання та відновлення даних. У контексті критичної інфраструктури операційний ризик може реалізуватися через помилкову дію оператора диспетчерського центру, яка була спровокована підробленими даними телеметрії, що надаються зловмисником у ході кібератаки.

Третю групу формують організаційні ризики, які лежать у площині управління та стратегічного планування. До них належать ризики недостатнього фінансування програм кібербезпеки, відсутності кваліфікованих кадрів, низького рівня обізнаності співробітників з питань інформаційної безпеки. Часто саме організаційні прорахунки створюють умови для реалізації технічних атак. Наприклад, відсутність політики управління доступом призводить до надання користувачам надлишкових прав, що полегшує зловмисникам горизонтальне переміщення мережею після компрометації одного облікового запису [31].

Окрему категорію становлять фізичні та кібер-фізичні ризики. Оскільки об'єкти критичної інфраструктури мають фізичне втілення, вони вразливі до

природних катаклізмів, техногенних аварій та фізичного втручання. Однак в умовах сучасної війни найбільшу загрозу становлять кібер-фізичні атаки, коли кібернетичний вплив на інформаційну систему призводить до фізичного руйнування обладнання або створення аварійних ситуацій. Прикладами таких ризиків є виведення з ладу електростанцій, зміна хімічного складу води на водоочисних спорудах або порушення роботи систем залізничної сигналізації. Важливою характеристикою ризиків критичної інфраструктури є їх здатність до каскадного поширення. Збій в одній критичній системі, наприклад в електроенергетиці, автоматично генерує критичні ризики для всіх суміжних секторів, які залежать від електропостачання – зв'язку, банківської сфери, транспорту та охорони здоров'я.

Методи та інструментарій оцінки ризиків

Вибір методу оцінки ризиків є важливим стратегічним рішенням, яке залежить від рівня зрілості організації, наявності історичних даних про інциденти та специфічних вимог регуляторів. У світовій практиці виділяють три основні групи методів: якісні, кількісні та комбіновані.

Якісні методи оцінки ризиків базуються на використанні експертних суджень та лінгвістичних шкал для вимірювання ймовірності та впливу подій. Найбільш поширеним інструментом у цій групі є матриця ризиків (Risk Matrix). Експерти оцінюють ймовірність реалізації загрози за шкалою, наприклад, від «низької» до «дуже високої», та потенційний вплив за аналогічною шкалою. Перетин цих двох параметрів на матриці визначає рівень ризику. Перевагою якісних методів є їх відносна простота, наочність результатів та можливість швидкого проведення оцінки без необхідності збору складних статистичних даних. Це робить їх ідеальним інструментом для початкового етапу побудови системи управління ризиками, а також для оцінки ризиків, які важко виміряти кількісно, наприклад репутаційних. Водночас, якісні методи мають суттєві недоліки, головним з яких є високий рівень суб'єктивності. Різні експерти можуть по-різному трактувати поняття «високий ризик», що призводить до

неузгодженості результатів. Крім того, якісні оцінки важко використовувати для обґрунтування економічної ефективності інвестицій у засоби захисту [32].

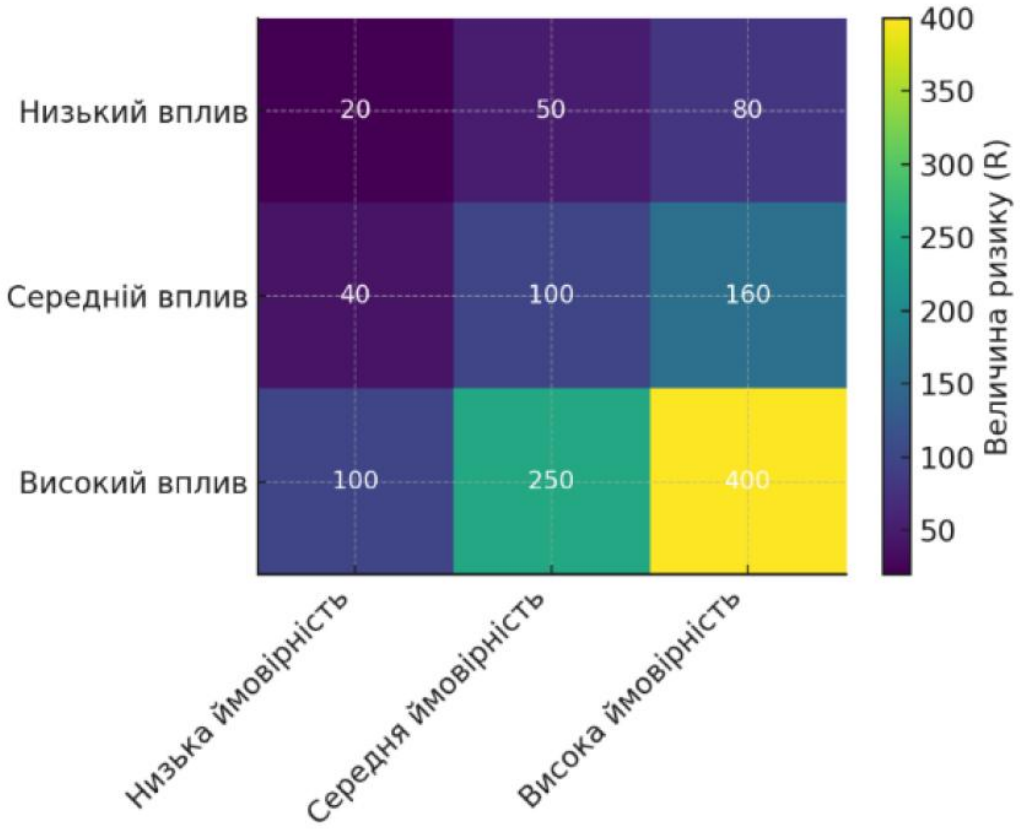

Рис. 2.3 Матриця оцінки кіберризиків (Heat Map)

Кількісні методи оцінки ризиків ставлять за мету вимірювання величини ризику в числових показниках, найчастіше у грошовому еквіваленті. Однією з найбільш прогресивних методологій у цій сфері є FAIR (Factor Analysis of Information Risk). Цей підхід декомпозує ризик на фундаментальні фактори: частоту події втрат (Loss Event Frequency) та ймовірну величину втрат (Loss Magnitude). Використовуючи методи статистичного моделювання, зокрема метод Монте-Карло, FAIR дозволяє розрахувати ймовірний діапазон фінансових втрат з певною довірчою ймовірністю. Кількісний підхід забезпечує об'єктивність оцінок, дозволяє порівнювати різнорідні ризики та говорити з бізнес-керівництвом мовою фінансових показників. Це значно спрощує процес бюджетування кібербезпеки та прийняття рішень щодо страхування ризиків.

Однак впровадження кількісних методів вимагає значних зусиль зі збору та верифікації вхідних даних, а також високої кваліфікації аналітиків.

Комбіновані або напівкількісні методи намагаються поєднати переваги обох підходів. Прикладом такої методології є OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), розроблена Інститутом програмної інженерії університету Карнегі-Меллона. Вона фокусується на організаційних ризиках та передбачає залучення персоналу різних рівнів до процесу самооцінки активів та загроз. Ризикам присвоюються умовні бали, що дозволяє їх ранжувати більш точно, ніж при суто якісному аналізі, але без надмірної математичної складності кількісних методів (табл.2.1) [33].

Таблиця 2.1.

Порівняльна характеристика методів оцінки ризиків кібербезпеки

Характеристика	**Якісні методи (Qualitative)**	**Кількісні методи (Quantitative)**	**Комбіновані методи (Hybrid)**
Основний інструмент	Матриця ризиків (Risk Matrix), експертні опитування.	Статистичне моделювання (напр., Монте-Карло), FAIR.	Рейтингові шкали, самооцінка (напр., OCTAVE).
Результат оцінки	Рівень ризику (Низький / Середній / Високий).	Грошовий еквівалент втрат (напр., $100k на рік).	Умовні бали або рейтинги пріоритетності.
Вимоги до даних	Суб'єктивні знання експертів.	Велика кількість історичних та статистичних даних.	Знання внутрішніх процесів та архітектури.
Переваги	Швидкість, простота, наочність для персоналу.	Об'єктивність, можливість розрахунку ROI (повернення інвестицій).	Баланс між точністю та складністю виконання.
Недоліки	Суб'єктивність, неможливість точного порівняння.	Складність впровадження, висока вартість аналізу.	Залежність від компетентності внутрішньої команди.

2.2. Системи моніторингу та виявлення інцидентів (SIEM, SOC)

В сучасних умовах, коли кібератаки стають дедалі складнішими та непомітнішими, покладатися лише на превентивні засоби захисту є стратегічною помилкою. Аксіомою сучасної кібербезпеки є твердження про неминучість

інциденту: питання полягає не в тому, чи буде систему зламано, а в тому, коли це станеться і як швидко захисники зможуть це виявити. Тому ключовими показниками ефективності системи безпеки стають час виявлення інциденту (Mean Time To Detect – MTTD) та чheaac його нейтралізації (Mean Time To Respond – MTTR). Для мінімізації цих показників та забезпечення повної ситуаційної обізнаності (Situational Awareness) об'єкти критичної інфраструктури розгортають централізовані системи моніторингу на базі технології SIEM та створюють спеціалізовані операційні центри безпеки (SOC) [34].

Технологічна платформа SIEM: Архітектура та функціональні можливості

Системи управління інформацією про безпеку та подіями (SIEM – Security Information and Event Management) виступають технологічним ядром сучасного центру моніторингу. Основна проблема, яку вирішує SIEM, – це обробка гігантських масивів даних. В інфраструктурі великого підприємства щосекунди генеруються тисячі записів журналів подій (логів), ручний аналіз яких є фізично неможливим. SIEM автоматизує цей процес, збираючи дані з усієї мережі, аналізуючи їх у реальному часі та виявляючи аномалії, що свідчать про атаку.

Архітектура типової SIEM-системи є багаторівневою та включає кілька функціональних компонентів. Перший рівень – це підсистема збору даних. Спеціалізовані програмні агенти або безпосередні колектори збирають логи з усіх елементів інфраструктури: серверів, робочих станцій, мережевого обладнання, баз даних, засобів захисту інформації та прикладного програмного забезпечення. Важливо забезпечити максимальне покриття джерел, щоб у зловмисника не залишилося «сліпих зон», де він міг би діяти непоміченим [35].

Другий рівень – це агрегація та нормалізація даних. Оскільки різні пристрої та програми генерують логи у власних, часто несумісних форматах, система повинна привести їх до єдиного стандарту. Процес нормалізації передбачає парсинг сирих логів та виділення з них ключових полів: часу події,

IP-адреси джерела та призначення, імені користувача, типу дії тощо. На цьому етапі також відбувається збагачення даних контекстною інформацією, наприклад, додавання геолокації IP-адреси або даних про підрозділ, в якому працює користувач.

Третій, найважливіший рівень – це кореляція подій. Механізм кореляції є інтелектуальним ядром SIEM, яке аналізує потік нормалізованих подій у пошуках взаємозв'язків. Кореляція дозволяє перетворити набір розрізнених технічних подій, кожна з яких окремо може виглядати легітимною, у цілісний інцидент безпеки. Наприклад, правило кореляції може пов'язати подію фізичного входу співробітника в офіс у Києві з подією успішної авторизації під його обліковим записом у VPN-шлюзі з IP-адреси в іншій країні. Таке поєднання подій однозначно свідчить про компрометацію облікового запису і вимагає негайної реакції.

Четвертий рівень – це візуалізація та звітність. SIEM надає аналітикам зручний графічний інтерфейс для моніторингу стану безпеки. Інтерактивні дашборди дозволяють у реальному часі бачити статистику інцидентів, географію атак, статус критичних активів. Крім оперативного моніторингу, система забезпечує генерацію звітів для відповідності вимогам регуляторів та стандартів, таких як ISO 27001 або PCI DSS. Сучасні SIEM-платформи еволюціонують у напрямку використання технологій штучного інтелекту, інтегруючи модулі поведінкової аналітики, які здатні виявляти загрози не за статичними правилами, а шляхом виявлення відхилень від нормальної поведінки користувачів та сутностей [36].

Security Operations Center (SOC): Організаційна структура та процеси

Технологія SIEM є лише інструментом, ефективність якого залежить від людей, які ним керують. Тому невід'ємною складовою системи кіберстійкості є Security Operations Center (SOC) – організаційна структура, яка відповідає за оперативне управління інцидентами кібербезпеки. SOC об'єднує кваліфікований

персонал, чітко визначені процеси та передові технології для забезпечення безперервного моніторингу та захисту інформаційних активів.

Організаційна модель сучасного SOC зазвичай будується за ієрархічним принципом, що дозволяє ефективно розподіляти завдання та використовувати експертизу фахівців різного рівня (табл.2.2).

Таблиця 2.2

Розподіл функцій у багаторівневій структурі SOC

Рівень (Tier)	**Роль**	**Основні завдання**	**Режим роботи**
Tier 1	Triage Specialist (Аналітик моніторингу)	Моніторинг консолі SIEM, фільтрація хибних спрацювань, реєстрація тікетів, первинна класифікація.	24/7 (змінний графік)
Tier 2	Incident Responder (Реагувальник)	Глибокий аналіз інциденту, визначення масштабу атаки, ізоляція хостів, видалення шкідливого ПЗ, відновлення систем.	Робочий час + On-call (виклики)
Tier 3	Threat Hunter (Мисливець за загрозами)	Проактивний пошук прихованих загроз, форензика (цифрова криміналістика), аналіз складних APT-атак, оптимізація правил SIEM.	Робочий час / Проектна робота
SOC Manager	Керівник центру	Управління персоналом, звітність перед бізнесом, розробка стратегії, контроль SLA та KPI.	Управлінський режим

Першу лінію оборони (Tier 1) складають аналітики з моніторингу. Вони працюють у змінному режимі, забезпечуючи нагляд за інфраструктурою 24/7/365. Їхнє основне завдання – первинна обробка потоку сповіщень, що надходять від SIEM-системи. Аналітики першого рівня проводять тріаж інцидентів: фільтрують очевидні хибні спрацювання, класифікують події за рівнем критичності та збирають первинну інформацію для подальшого розслідування [37].

Другу лінію (Tier 2) формують фахівці з реагування на інциденти. Це більш досвідчені експерти, які приймають в роботу складні випадки, ескальовані з першого рівня. Їхнє завдання – провести глибокий аналіз інциденту, встановити

його причини, масштаб та потенційні наслідки. Головна мета аналітиків другого рівня – стримування загрози та мінімізація шкоди. Вони виконують активні дії з протидії атаці: блокують мережеві з'єднання, ізолюють заражені хости, видаляють шкідливе програмне забезпечення та координують процес відновлення нормального функціонування систем.

Третю лінію (Tier 3) складають експерти з полювання на загрози (Threat Hunters) та цифрової криміналістики. На відміну від попередніх рівнів, які працюють реактивно, реагуючи на сповіщення системи, аналітики третього рівня діють проактивно. Вони висувають гіпотези про можливу наявність у мережі прихованих загроз, які оминули автоматичні засоби захисту, і перевіряють ці гіпотези шляхом ручного аналізу даних. Також вони займаються розслідуванням складних цільових атак (APT), аналізом шкідливого коду (Reverse Engineering) та розробкою нових правил детектування для SIEM-системи [38].

Ефективна робота SOC неможлива без формалізації процесів. Основою операційної діяльності центру є сценарії реагування (Playbooks). Це детальні інструкції, які описують послідовність дій персоналу при виявленні типових інцидентів, таких як фішинг, зараження вірусом-вимагачем або DDoS-атака. Стандартизація процедур реагування дозволяє мінімізувати вплив людського фактору, забезпечити стабільну якість роботи та прискорити навчання нових співробітників. В умовах дефіциту кадрів багато організацій переходять до гібридних моделей побудови SOC, делегуючи рутинні функції моніторингу зовнішнім спеціалізованим провайдерам (MSSP), залишаючи за собою функції контролю та прийняття критичних рішень.

2.3. Розвідка кіберзагроз (Threat Intelligence)

Еволюція ландшафту кібербезпеки характеризується появою нового класу супротивників – так званих Advanced Persistent Threats (APT). Це високоорганізовані групи, часто спонсоровані державними структурами, які

володіють значними ресурсами, часом та мотивацією для проведення складних, тривалих кампаній кібершпигунства або саботажу проти об'єктів критичної інфраструктури. У протистоянні з таким ворогом традиційна реактивна модель захисту, яка базується на виявленні та блокуванні атак у момент їх здійснення, виявляється недостатньо ефективною. Захисники постійно перебувають у позиції наздоганяючих, реагуючи на інциденти постфактум, коли шкоду вже часто заподіяно. Щоб змінити розстановку сил та перехопити ініціативу, організації повинні перейти до проактивної моделі оборони, яка базується на глибокому розумінні тактики, техніки та процедур супротивника. Інструментом реалізації такої стратегії є розвідка кіберзагроз (Cyber Threat Intelligence – CTI) [39].

Сутність та рівні Threat Intelligence

Розвідка кіберзагроз – це процес збору, обробки, аналізу та поширення знань про наявні або потенційні загрози, що дозволяє організації приймати обґрунтовані рішення щодо захисту своїх активів. На відміну від простого накопичення даних (data) або інформації (information), розвідка (intelligence) передбачає додавання контексту, аналітичну обробку та верифікацію, що перетворює сирі факти на інструкції до дії. CTI відповідає на питання: «Хто атакує?», «Чому вони атакують?», «Які інструменти використовують?» та «Як ми можемо це виявити та зупинити?».

Залежно від характеру інформації та цільової аудиторії, розвідку кіберзагроз прийнято класифікувати на три ієрархічні рівні: стратегічний, оперативний та тактичний.

Стратегічний рівень (Strategic CTI) орієнтований на вище керівництво організації – генеральних директорів, членів правління, директорів з інформаційної безпеки (CISO). Інформація на цьому рівні має нетехнічний характер і фокусується на довгострокових тенденціях та бізнес-ризиках. Стратегічні звіти аналізують глобальні зміни в ландшафті загроз, геополітичні фактори, мотивацію хакерських груп, націлених на конкретну галузь чи регіон. Метою стратегічної розвідки є надання керівництву контексту для прийняття

управлінських рішень: визначення пріоритетів розвитку системи безпеки, обґрунтування бюджетів, оцінки ризиків для нових бізнес-проектів або злиттів та поглинань. Наприклад, розуміння того, що політична напруга в регіоні підвищує ризик деструктивних кібератак на енергетичний сектор, дозволяє керівництву енергокомпанії завчасно виділити ресурси на посилення відмовостійкості систем [39].

Оперативний рівень (Operational CTI) призначений для фахівців, які безпосередньо відповідають за організацію захисту: керівників SOC, аналітиків загроз, інженерів безпеки. Цей рівень надає детальну інформацію про поведінку зловмисників, відому як TTPs (Tactics, Techniques, and Procedures). Оперативна розвідка описує конкретні кампанії, інструментарій (malware variants), методи соціальної інженерії та експлойти, які використовують хакерські групи. Знання TTPs дозволяє захисникам зрозуміти логіку дій атакуючого та адаптувати систему захисту до реальних загроз. Наприклад, отримавши інформацію про те, що певна APT-група використовує специфічний метод бічного переміщення (lateral movement) через протокол RDP, аналітики можуть налаштувати правила кореляції в SIEM для виявлення саме такої активності [40].

Тактичний рівень (Tactical CTI) фокусується на технічних деталях і призначений для системних адміністраторів та автоматизованих засобів захисту. Основним продуктом тактичної розвідки є індикатори компрометації (Indicators of Compromise – IoC). Це конкретні цифрові сліди, які залишає атака: IP-адреси командних серверів (C2), доменні імена, URL-адреси фішингових сторінок, хеш-суми шкідливих файлів, ключі реєстру. Тактичний CTI є найбільш динамічним та автоматизованим: потоки індикаторів (feeds) завантажуються безпосередньо в міжмережеві екрани, системи IDS/IPS, EDR та SIEM для автоматичного блокування або детектування відомих загроз (табл.2.3). Хоча термін життя тактичних індикаторів є коротким (зловмисники часто змінюють інфраструктуру), їх використання дозволяє відсіяти значну частину масових атак та звільнити ресурси аналітиків для полювання на більш складні загрози.

Таблиця 2.3.

Рівні та характеристики розвідки кіберзагроз (CTI)

Рівень CTI	Цільова аудиторія	Тип інформації	Приклад використання
Стратегічний	Топ-менеджмент (CISO, CEO, Рада директорів)	Тренди, геополітичні ризики, мотивація нападників, фінансові оцінки.	Прийняття рішень про бюджет, оцінка бізнес-ризиків при виході на нові ринки.
Оперативний	Керівники SOC, Threat Hunters	Тактики, Техніки та Процедури (TTPs), опис кампаній хакерських груп.	Налаштування правил кореляції, розуміння контексту атаки («Хто і як?»).
Тактичний	Системні адміністратори, SIEM, Firewalls	Індикатори компрометації (IoC): IP-адреси, хеші файлів, домени.	Автоматичне блокування на шлюзах, пошук слідів зараження в мережі.

Роль фреймворку MITRE ATT&CK та платформ обміну даними

Для ефективної комунікації та обміну знаннями про загрози світова спільнота кібербезпеки потребувала єдиної термінології та структурної моделі. Таким стандартом де-факто стала матриця MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) (рис. 2.4). Це глобальна база знань, яка систематизує поведінку зловмисників, базуючись на реальних спостереженнях. Матриця структурує дії хакерів за етапами життєвого циклу атаки (Cyber Kill Chain), виділяючи тактики (тактичні цілі супротивника) та техніки (конкретні методи досягнення цих цілей) [41].

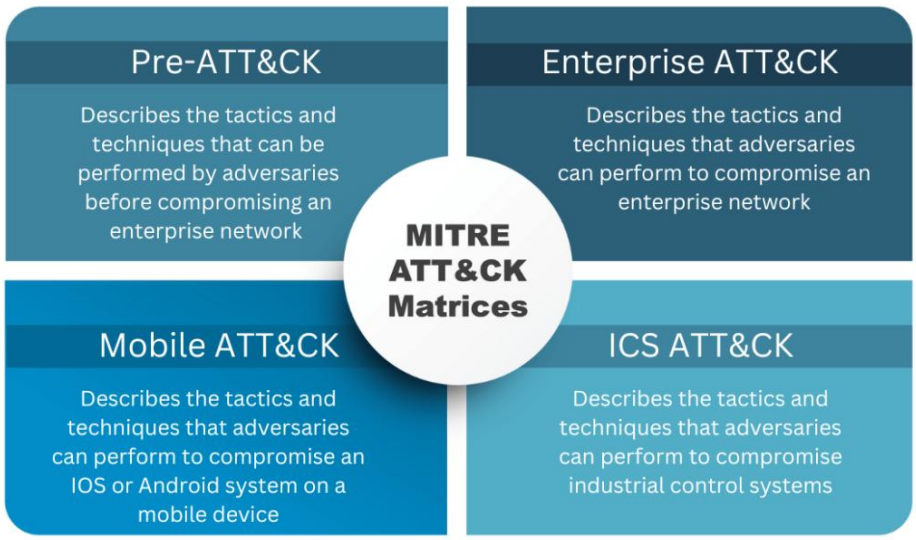

Рис. 2.4. Структура матриці MITRE ATT&CK

Тактики ATT&CK відповідають на питання «Що намагається зробити зловмисник?». До них належать, наприклад, отримання початкового доступу (Initial Access), виконання коду (Execution), закріплення в системі (Persistence), підвищення привілеїв (Privilege Escalation), обхід захисту (Defense Evasion), ексфільтрація даних (Exfiltration) та вплив (Impact). Кожна тактика включає набір технік, які описують, як саме це робиться. Наприклад, тактика «Отримання початкового доступу» може бути реалізована через техніки «Фішинг», «Експлуатація публічних сервісів» або «Використання довірених відносин» [42].

Застосування фреймворку MITRE ATT&CK дозволяє організаціям критичної інфраструктури вирішувати низку практичних завдань. По-перше, це профілювання загроз: аналітики можуть створювати цифрові профілі актуальних для їхнього сектору APT-груп, визначаючи, які техніки ті використовують найчастіше. По-друге, це оцінка ефективності захисту (Gap Analysis): наклавши можливості існуючих засобів детектування на матрицю ATT&CK, організація може візуалізувати своє покриття (coverage map) і виявити «сліпі зони», де дії зловмисника залишаться непоміченими. По-третє, це проведення навчань з емуляції атак (Adversary Emulation), коли команда «червоних» (Red Team) імітує дії реального супротивника за сценарієм ATT&CK, перевіряючи здатність SOC виявити та зупинити атаку [43].

Критично важливим елементом екосистеми Threat Intelligence є обмін інформацією (Information Sharing). В умовах, коли одні й ті самі хакерські групи атакують безліч цілей в одному секторі, ізольована оборона приречена на поразку. Організації повинні об'єднувати зусилля, обмінюючись даними про інциденти та індикатори компрометації. Цю функцію виконують галузеві центри обміну інформацією та аналізу (ISAC – Information Sharing and Analysis Centers) та національні команди реагування (CERT). Для автоматизації обміну використовуються спеціалізовані платформи (TIP – Threat Intelligence Platforms), такі як MISP, та стандартизовані протоколи: STIX (мова структурованого опису загроз) та TAXII (транспортний механізм обміну). Колективний обмін даними

створює ефект «цифрового імунітету»: виявлення атаки на одного учасника спільноти дозволяє миттєво попередити всіх інших, роблячи повторне використання тієї ж інфраструктури атаки неефективним для зловмисника [44].

2.4. Новітні технології та підходи: UEBA, SOAR, AI/ML

Стрімкий розвиток технологій, збільшення обсягів даних та ускладнення інфраструктури створюють нові виклики для систем кібербезпеки. Традиційні підходи, які покладаються на ручну працю аналітиків та статичні правила детектування, вже не здатні впоратися зі швидкістю та масштабом сучасних загроз. Це стимулює індустрію до впровадження інноваційних технологій, заснованих на автоматизації та штучному інтелекті.

Поведінкова аналітика (UEBA)

Класичні засоби захисту, такі як антивіруси чи системи виявлення вторгнень (IDS), працюють на основі сигнатур – відомих ознак шкідливого коду або мережевої активності. Такий підхід ефективний проти відомих загроз, але безсилий проти нових видів атак (Zero-day) або дій інсайдерів, які використовують легітимні облікові дані. Відповіддю на це обмеження стала технологія поведінкової аналітики користувачів та сутностей (UEBA – User and Entity Behavior Analytics) [45].

UEBA змінює парадигму виявлення загроз: замість того, щоб шукати «відоме зло», вона шукає відхилення від норми (табл. 2.4).

Таблиця 2.4.

Відмінність традиційного захисту від UEBA

Характеристика	**Традиційний захист (SIEM / IDS)**	**Поведінкова аналітика (UEBA)**
Метод виявлення	Сигнатурний аналіз, статичні правила кореляції.	Машинне навчання, профілювання поведінки (Baseline).
Об'єкт пошуку	Відомі загрози («Чорні списки»).	Аномалії та відхилення від норми.
Ефективність проти	Масових вірусів, відомих експлойтів.	Інсайдерів, скомпрометованих акаунтів, Zero-day атак.
Джерело тривоги	Спрацювання конкретного правила.	Підвищення ризик-балу (Risk Score) користувача.

Система використовує алгоритми машинного навчання для аналізу історичних даних та побудови базового профілю нормальної поведінки (baseline) для кожного об'єкта в мережі – користувача, сервера, робочої станції чи додатку. Профіль враховує безліч параметрів: час роботи, геолокацію, обсяги переданих даних, типові ресурси, до яких здійснюється доступ, використовувані протоколи.

Коли система фіксує активність, що суттєво відхиляється від базового профілю, вона підвищує рівень ризику для відповідного об'єкта. Наприклад, якщо обліковий запис співробітника відділу кадрів, який зазвичай працює з текстовими документами в робочий час, раптом починає сканувати порти серверів бази даних у нічний час, UEBA ідентифікує це як аномалію та генерує інцидент. При цьому, з точки зору традиційних засобів контролю доступу, дії можуть виглядати легітимними, оскільки використовується валідний пароль. UEBA є критично важливим інструментом для виявлення складних загроз, таких як компрометація облікових записів (Credential Theft), зловмисні дії інсайдерів, а також повільні, низькоінтенсивні атаки (Low and Slow), які розтягнуті у часі і не викликають спрацювання порогових правил SIEM [46].

Оркестрація та автоматизація реагування (SOAR)

Однією з найгостріших проблем сучасних SOC є так звана «втома від сповіщень» (alert fatigue). Кількість подій безпеки, що генеруються різноманітними засобами захисту, часто перевищує фізичні можливості аналітиків щодо їх якісної обробки. Це призводить до того, що значна частина сповіщень ігнорується або розслідується поверхнево, що підвищує ризик пропуску реальної атаки. Вирішенням цієї проблеми є технологія оркестрації, автоматизації та реагування (SOAR – Security Orchestration, Automation, and Response).

SOAR – це програмна платформа, яка об'єднує три ключові функції. Оркестрація забезпечує інтеграцію різнорідних засобів захисту (SIEM, EDR, Firewalls, поштові шлюзи, Threat Intelligence) в єдину екосистему через програмні інтерфейси (API), дозволяючи керувати ними з однієї консолі.

Автоматизація дозволяє виконувати рутинні, повторювані дії без участі людини за допомогою заздалегідь налаштованих сценаріїв (Playbooks). Реагування забезпечує координацію процесу обробки інциденту, ведення журналу дій та комунікацію між членами команди [47].

Впровадження SOAR дозволяє кардинально скоротити час реагування на типові інциденти. Розглянемо приклад фішингової атаки. У ручному режимі аналітик повинен проаналізувати заголовок листа, витягти вкладення, перевірити його репутацію на зовнішніх ресурсах, і в разі підтвердження загрози – вручну створити запит на блокування відправника та видалення листа. Цей процес може зайняти від 20 хвилин до години. SOAR виконує всі ці дії автоматично за лічені секунди: система сама перевіряє індикатори, отримує вердикт і, залежно від налаштувань, або автоматично блокує загрозу, або надає аналітику готове рішення для підтвердження одним кліком. Це не лише прискорює реакцію, а й звільняє висококваліфікованих фахівців від рутини, дозволяючи їм зосередитися на розслідуванні складних, нестандартних інцидентів [48].

Штучний інтелект та машинне навчання (AI/ML)

Штучний інтелект (Artificial Intelligence – AI) та його підмножина – машинне навчання (Machine Learning – ML) – стають наскрізними технологіями, що трансформують всі аспекти кіберстійкості. Застосування AI дозволяє перейти від статичних моделей захисту до адаптивних, самонавчальних систем, здатних протистояти еволюціонуючим загрозам.

У сфері захисту кінцевих точок (Endpoint Security) технології ML замінюють традиційний сигнатурний аналіз. Антивіруси нового покоління (NGAV) використовують математичні моделі для аналізу структури файлів та їхньої поведінки при запуску, що дозволяє виявляти нові модифікації шкідливого ПЗ (поліморфні віруси) та програми-вимагачі, які раніше не зустрічалися дослідникам. У мережевій безпеці алгоритми ML використовуються для аналізу трафіку (Network Traffic Analysis – NTA). Вони здатні виявляти приховані канали управління ботнетами (C2) та ознаки

ексфільтрації даних навіть у зашифрованому трафіку, аналізуючи метадані з'єднань, розміри пакетів та часові інтервали передачі [49].

Ще одним перспективним напрямком є використання AI для предиктивної аналітики. Аналізуючи величезні масиви даних про глобальні загрози, вразливості та стан інфраструктури, системи на базі AI можуть прогнозувати ймовірні вектори атак та надавати рекомендації щодо превентивного посилення захисту.

Однак широке впровадження AI створює і нові ризики. Зловмисники також починають використовувати штучний інтелект для автоматизації своїх атак: створення переконливих фішингових листів (Deepfakes), пошуку вразливостей та обходу систем захисту. Виникає феномен Adversarial AI – атак на самі алгоритми машинного навчання, коли шляхом маніпуляції вхідними даними зловмисник змушує модель приймати хибні рішення (наприклад, класифікувати шкідливий файл як безпечний). Це призводить до ескалації технологічного протистояння, перетворюючи кібербезпеку на «війну алгоритмів» [50].

Висновки до розділу 2

У другому розділі проведено комплексний аналіз методів та засобів забезпечення кіберстійкості критичної інфраструктури. Результати дослідження дозволяють сформулювати низку узагальнюючих висновків, які визначають архітектуру сучасної системи захисту.

Трансформація парадигми безпеки. Відбувається незворотний перехід від реактивної моделі «кібербезпеки», орієнтованої на захист периметру, до проактивної моделі «кіберстійкості», що базується на управлінні ризиками. Це вимагає впровадження системних процесів ідентифікації та оцінки загроз згідно з міжнародними стандартами (NIST, ISO), що дозволяє приймати обґрунтовані рішення в умовах невизначеності.

Централізація та видимість. Ключовим елементом операційної безпеки стає створення центрів моніторингу (SOC) на базі технологій SIEM.

Забезпечення повної видимості подій у гетерогенних мережах КІ є передумовою для своєчасного виявлення інцидентів. Ефективність SOC залежить не лише від технологій, а й від зрілості процесів та кваліфікації персоналу.

Інтелектуалізація захисту. Ефективна протидія кваліфікованим супротивникам (APT) неможлива без використання розвідки кіберзагроз (Threat Intelligence). Розуміння тактик та технік ворога (MITRE ATT&CK) дозволяє перейти від сліпого реагування до випереджаючих дій.

Автоматизація як відповідь на швидкість. Зростання інтенсивності атак робить ручне реагування неефективним. Технології SOAR та UEBA стають критичними компонентами екосистеми безпеки, дозволяючи автоматизувати рутинні операції, скоротити час реакції та виявляти складні аномалії.

Адаптивність системи. Сучасна система кіберстійкості не є статичною конструкцією. Вона повинна постійно еволюціонувати, використовуючи технології штучного інтелекту для адаптації до нових векторів загроз. Лише поєднання методології ризик-менеджменту, передових технологій моніторингу та кваліфікованого людського капіталу здатне забезпечити надійне функціонування критичної інфраструктури держави.

РОЗДІЛ 3
РОЗРОБКА СИСТЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

3.1. Постановка завдань та принципи системного підходу до кіберстійкості

В умовах перманентної ескалації загроз у кібернетичному просторі, що набувають ознак повномасштабного кібернетичного протиборства, проблематика захисту критичної інфраструктури (КІ) трансформується з площини суто технічного адміністрування інформаційних систем у площину забезпечення національної стійкості та безпеки держави. Традиційні парадигми інформаційної безпеки, що базувалися на бінарній логіці «захищений/незахищений» та пріоритеті периметральної оборони, демонструють свою неспроможність перед лицем сучасних загроз класу APT (Advanced Persistent Threat) та складних ланцюгових атак на системи постачання (Supply Chain Attacks) [51].

У зв’язку з цим виникає об’єктивна необхідність зміни концептуального вектору досліджень та практичних розробок: перехід від концепції «кібербезпеки» (Cybersecurity), фокусом якої є запобігання інцидентам, до концепції «кіберстійкості» (Cyber Resilience). Під кіберстійкістю у межах даного дослідження розуміється емерджентна властивість складної соціотехнічної системи, яка характеризує її здатність адаптуватися до деструктивних впливів, забезпечувати неперервність виконання критичних функцій в умовах деградації окремих компонентів, а також динамічно відновлювати штатний режим функціонування після завершення інциденту.

Постановка науково-прикладного завдання розробки системи забезпечення кіберстійкості вимагає чіткої формалізації вихідних умов, обмежень та цільових функцій. Об’єкт критичної інфраструктури розглядається як складна динамічна система , що функціонує в агресивному стохастичному

середовищі. Метою функціонування системи захисту є мінімізація ризику порушення доступності, цілісності та конфіденційності критичних сервісів [52].

Формалізована постановка завдання включає наступні компоненти:

1. Ідентифікація об’єкта захисту. Необхідно визначити межі системи, включаючи всі апаратні, програмні, інформаційні та кадрові ресурси. Для об’єктів КІ специфікою є наявність тісної інтеграції між інформаційними технологіями (ІТ) та операційними технологіями (ОТ), що керують фізичними процесами. Завдання полягає у забезпеченні стійкості конвергентного середовища, де кібернетичний вплив може мати кінетичні наслідки.

2. Визначення вектору загроз. Завдання передбачає аналіз актуального ландшафту загроз, що включає не лише технічні вразливості, а й соціоінженерні методи, вплив на ланцюги постачання, а також гібридні сценарії, де кібератаки синхронізуються з фізичними діями або інформаційними операціями.

3. Формулювання критеріїв ефективності. На відміну від абстрактної «безпеки», кіберстійкість оперує вимірюваними метриками. Ключовими показниками, що мають бути закладені в основу системи, є:

– иаксимально допустимий час простою (Maximum Tolerable Period of Disruption – MTPD).

– цільовий час відновлення (Recovery Time Objective – RTO).

– цільова точка відновлення (Recovery Point Objective – RPO).

– рівень деградації сервісу (Service Degradation Level), допустимий в умовах кризової ситуації.

4. Врахування обмежень. Процес розробки системи відбувається в умовах жорстких обмежень: ресурсних (бюджет, кадри), часових, нормативно-правових (вимоги національного законодавства та галузевих регуляторів), а також технологічних (наявність застарілого обладнання, так званих legacy-систем, яке неможливо оновити або замінити без зупинки виробничого процесу).

Отже, завдання полягає у синтезі такої структури системи захисту, яка б при заданих обмеженнях забезпечувала утримання параметрів функціонування

об’єкта КІ в межах допустимого діапазону значень навіть за умов реалізації найгірших сценаріїв кібернетичного впливу.

Принципи системного підходу до забезпечення кіберстійкості (рис.3.1).

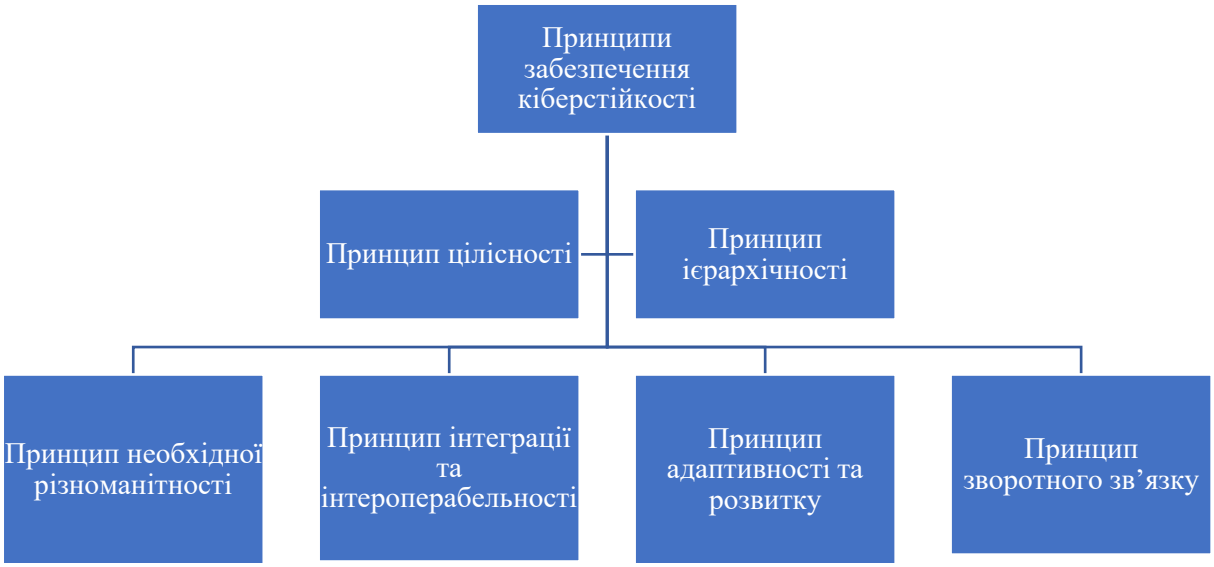

Рис. 3.1. Принципи забезпечення кіберстійкості

Методологічним фундаментом вирішення поставленого завдання є загальна теорія систем та системний аналіз. Застосування системного підходу дозволяє подолати фрагментарність і «клаптиковість», притаманну багатьом існуючим рішенням, коли впровадження окремих засобів захисту не створює загального контуру безпеки [53].

У контексті забезпечення кіберстійкості критичної інфраструктури системний підхід реалізується через дотримання низки фундаментальних принципів:

1. Принцип цілісності (холізму). Цей принцип постулює первинність цілого над частинами. Система кіберстійкості не є простою механічною сукупністю антивірусів, міжмережевих екранів, систем виявлення вторгнень та організаційних наказів. Вона є інтегрованою сутністю, де ефективність цілого залежить від якості взаємозв’язків між елементами. Наприклад, наявність

найсучаснішої системи SIEM (Security Information and Event Management) буде нівельована, якщо відсутні регламенти реагування на виявлені інциденти або якщо персонал не має достатньої кваліфікації для інтерпретації алертів. Цілісність вимагає розглядати технічні, процесні та людські аспекти як єдиний континуум безпеки.

2. Принцип ієрархічності та багаторівневості. Будь-яка складна система має ієрархічну будову. Система кіберстійкості підприємства КІ повинна будуватися як багаторівнева конструкція, що включає:

- стратегічний рівень: визначення політики, цілей, управління ризиками, взаємодія з державними регуляторами;
- тактичний рівень: розробка регламентів, впровадження архітектурних рішень, управління програмами навчання персоналу;
- операційний рівень: безпосередній моніторинг, адміністрування засобів захисту, реагування на інциденти в режимі реального часу;
- технічний рівень: функціонування конкретних засобів захисту на рівні мережі, хостів, додатків та даних.

Взаємодія між рівнями повинна бути двосторонньою: керуючі впливи транслюються зверху вниз, а дані про стан системи та інциденти – знизу вгору.

3. Принцип необхідної різноманітності (закон Ешбі). Стосовно кібербезпеки цей кібернетичний закон можна інтерпретувати так: різноманітність (складність) системи захисту повинна бути не меншою, ніж різноманітність загроз, що генеруються зовнішнім середовищем. Оскільки вектори атак постійно еволюціонують і диверсифікуються, система кіберстійкості не може бути статичною. Вона повинна володіти достатнім арсеналом механізмів (детекторів, пасток, засобів блокування, процедур відновлення) для протидії широкому спектру сценаріїв – від автоматизованих скриптів до цілеспрямованих дій кваліфікованих хакерських угруповань.

4. Принцип інтеграції та інтероперабельності. Підсистеми забезпечення кіберстійкості не повинні функціонувати ізольовано. Засоби фізичної безпеки (системи контролю доступу, відеоспостереження) мають бути інтегровані з

системами інформаційної безпеки. Наприклад, спроба входу в систему з обліковим записом працівника, який, згідно з даними системи контролю доступу (СКУД), фізично не перебуває на території підприємства, повинна автоматично блокуватися як аномальна. Інтероперабельність також передбачає здатність обмінюватися даними про інциденти та індикатори компрометації (IoC) з зовнішніми суб'єктами – галузевими CERT, національними центрами кібербезпеки та партнерами.

5. Принцип адаптивності та розвитку. Середовище функціонування об'єктів КІ характеризується високим рівнем невизначеності та динаміки. Статичні системи захисту, побудовані за принципом «встановив і забув», неминуче деградують з часом. Системний підхід вимагає закладення механізмів адаптації – здатності системи змінювати свою структуру, параметри та алгоритми функціонування під впливом змін у зовнішньому середовищі або внутрішньому стані. Це реалізується через процеси постійного моніторингу вразливостей, Threat Intelligence (розвідку загроз), регулярний перегляд політик безпеки та модернізацію засобів захисту.

6. Принцип зворотного зв'язку. Забезпечення стійкості неможливе без ефективних контурів зворотного зв'язку. Система повинна постійно отримувати інформацію про результати своєї роботи. Це досягається шляхом проведення регулярних аудитів, тестувань на проникнення (Penetration Testing), кібернавчань та аналізу уроків, винесених з реальних інцидентів (Lessons Learned). Отримана інформація використовується для корекції керуючих впливів, замикаючи цикл управління та забезпечуючи еволюційний розвиток системи.

Таким чином, системний підхід є не просто теоретичною абстракцією, а практичним інструментарієм, що дозволяє структурувати складну проблему забезпечення кіберстійкості, декомпозувати її на вирішувані підзадачі та синтезувати ефективне рішення, адекватне сучасним викликам гібридної війни (табл 3.1) [53].

Таблиця 3.1

Порівняльна характеристика підходів до забезпечення кібербезпеки КІ

Критерій порівняння	**Традиційний (фрагментарний) підхід**	**Системний підхід (Cyber Resilience)**
Цільова функція	Запобігання проникненню (Prevent)	Забезпечення безперервності та відновлення (Resist, Recover)
Об’єкт захисту	Окремі елементи IT-інфраструктури	Критичні бізнес-процеси та сервіси в цілому
Режим роботи	Реактивний (реагування на інциденти)	Проактивний (передбачення загроз, Threat Hunting)
Архітектура	Орієнтована на периметр ("Фортеця")	Глибока ешелонована оборона (Defense-in-Depth)
Роль персоналу	Користувачі розглядаються як джерело проблем	Персонал є активним елементом системи захисту ("Human Firewall")

3.2. Модель комплексної системи кіберстійкості для підприємств критичної інфраструктури

Концептуальна архітектура системи

Розробка моделі комплексної системи кіберстійкості для підприємства критичної інфраструктури базується на необхідності створення багаторівневої архітектури, яка охоплює всі аспекти функціонування організації: від технологічних процесів до управлінських рішень. Пропонована модель синтезує вимоги міжнародних стандартів (зокрема серії ISO/IEC 27000, NIST SP 800-53, NIST SP 800-160 Vol. 2 "Developing Cyber-Resilient Systems") та враховує специфіку вітчизняного правового поля і ландшафту загроз [54].

Архітектура моделі може бути представлена у вигляді тривимірної матриці, осями якої є:

1. Рівні управління (Стратегічний, Тактичний, Операційний).
2. Функціональні домени (Ідентифікація, Захист, Виявлення, Реагування, Відновлення).
3. Об’єкти захисту (Люди, Процеси, Технології).

Центральним елементом архітектури є Система управління інформаційною безпекою (СУІБ), яка виступає інтегратором усіх компонентів (рис. 3.2). Вона забезпечує відповідність заходів кібербезпеки бізнес-цілям підприємства та вимогам щодо забезпечення безперервності виробничих процесів.

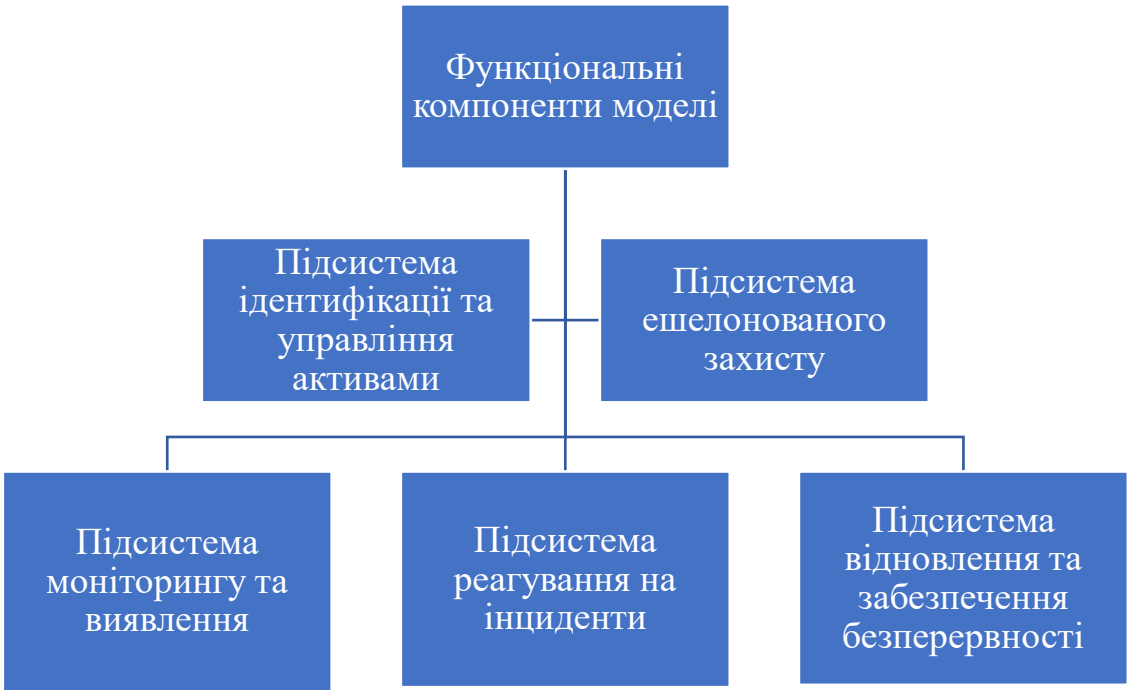

Рис. 3.2. Функціональні компоненти моделі

Розглянемо детально складові елементи моделі через призму функціональних доменів, що відповідають циклу забезпечення кіберстійкості.

1. Підсистема ідентифікації та управління активами (Identify). Фундаментом кіберстійкості є повне розуміння контексту функціонування організації. Ця підсистема включає:

– інвентаризацію активів: створення та підтримка в актуальному стані реєстру всіх апаратних засобів, програмного забезпечення, інформаційних активів та каналів зв’язку. Для КІ критично важливо обліковувати не лише ІТ-активи, а й компоненти АСУ ТП (контролери, датчики, виконавчі механізми).

– картографування інформаційних потоків: визначення маршрутів руху даних між системами, що дозволяє виявити критичні точки перетину та потенційні вектори атак.

– управління ризиками: безперервний процес ідентифікації загроз, оцінки вразливостей та розрахунку потенційних збитків. На основі оцінки ризиків формується пріоритетність впровадження захисних заходів.

2. Підсистема ешелонованого захисту (Protect).
Ця підсистема реалізує концепцію "Defense-in-Depth" (захист у глибину), створюючи множинні бар’єри на шляху зловмисника.

– фізична безпека. Захист периметру об’єкта, контроль доступу до серверних приміщень та диспетчерських пунктів.

– мережева безпека. Реалізація жорсткої сегментації мережі. Критично важливим є відокремлення корпоративного сегменту (IT) від технологічного (OT) через використання демілітаризованих зон (DMZ) та шлюзів безпеки. У найбільш критичних вузлах доцільне використання односпрямованих шлюзів (Data Diodes), які фізично унеможливлюють проходження трафіку всередину захищеного контуру.

– безпека кінцевих точок та додатків. Використання антивірусного ПЗ, EDR-систем (Endpoint Detection and Response), контроль запуску додатків (Application Whitelisting), регулярне оновлення ПЗ (Patch Management).

– криптографічний захист. Шифрування даних при зберіганні та передачі, управління ключовою інфраструктурою (PKI).

– управління доступом. Впровадження рольової моделі доступу (RBAC), принципу найменших привілеїв та обов’язкової багатофакторної автентифікації (MFA) для всіх віддалених та адміністративних доступів.

3. Підсистема моніторингу та виявлення (Detect).
Забезпечує ситуаційну обізнаність та здатність виявляти інциденти на ранніх стадіях.

– безперервний моніторинг. Збір логів з усіх систем, аналіз мережевого трафіку (NTA/NDR).

– центр операцій безпеки (SOC). Організаційна структура, що забезпечує централізований збір, кореляцію та аналіз подій безпеки за допомогою SIEM-систем.

– виявлення аномалій. Використання технологій машинного навчання (UBA/UEBA) для виявлення нестандартної поведінки користувачів або процесів, що може свідчити про наявність прихованої загрози.

4. Підсистема реагування на інциденти (Respond). Визначає здатність організації локалізувати інцидент та мінімізувати його наслідки.

– планування реагування. Розробка детальних сценаріїв (Playbooks) дій для різних типів інцидентів (DDoS-атака, зараження шкідливим ПЗ, витік даних).

– кризові комунікації. Алгоритми інформування керівництва, регуляторів, клієнтів та громадськості.

– технічне реагування. Інструментарій для ізоляції уражених хостів, блокування шкідливого трафіку, збору криміналістичних доказів (Forensics).

5. Підсистема відновлення та забезпечення безперервності (Recover). Ключовий елемент кіберстійкості, що відповідає за повернення системи до штатного стану.

– управління безперервністю бізнесу (BCP). Стратегії перемикання на резервні потужності, перехід на ручне управління технологічними процесами.

– відновлення після катастроф (DRP). Наявність резервних центрів обробки даних (Hot/Cold Sites).

– резервне копіювання. Реалізація стратегії "3-2-1" (3 копії, 2 носії, 1 копія офлайн/офсайт) для захисту від атак типу ransomware. Важлива наявність незмінних (immutable) резервних копій.

Модель нульової довіри (Zero Trust Architecture) як перспективний напрям

Окрему увагу в розробленій моделі приділено імплементації принципів Zero Trust. Традиційна модель захисту периметра ("фортеця та рів") втрачає ефективність в умовах розмивання меж мережі (хмарні технології,

віддалена робота, IoT). Модель Zero Trust базується на аксіомі "ніколи не довіряй, завжди перевіряй".

У контексті КІ це означає:

1. Жоден пристрій, користувач чи пакет даних не вважається довіреним за замовчуванням, незалежно від того, знаходиться він всередині периметра чи зовні.

2. Доступ до ресурсів надається на основі динамічної політики, що враховує не лише ідентифікатор користувача, а й контекст: стан безпеки пристрою, геолокацію, час доступу, поведінкові патерни.

3. Мікросегментація мережі дозволяє обмежити "радіус ураження": компрометація одного сегмента не дає зловмиснику автоматичного доступу до всієї мережі.

4. Всі сесії взаємодії повинні бути захищені шифруванням, а автентифікація – бути безперервною.

Впровадження моделі Zero Trust на підприємствах КІ є складним процесом, що потребує модернізації інфраструктури, проте саме такий підхід забезпечує найвищий рівень кіберстійкості проти сучасних цілеспрямованих атак.

Таким чином, запропонована модель комплексної системи кіберстійкості є інтегрованою, багаторівневою конструкцією, яка поєднує класичні методи захисту з новітніми архітектурними підходами, забезпечуючи надійне функціонування критичної інфраструктури в умовах агресивного кібернетичного середовища.

3.3. Розробка набору заходів протидії гібридним загрозам та мінімізації наслідків

Розробка ефективної системи протидії сучасним загрозам для об’єктів критичної інфраструктури (ОКІ) вимагає переходу від фрагментарних рішень до побудови комплексної системи, яка базується на глибокому аналізі природи

гібридних атак. Як було визначено у попередніх підрозділах, архітектура такої системи має бути багаторівневою і включати в себе взаємопов’язані підсистеми моніторингу, аналізу, реагування та відновлення.

Спираючись на аналіз, проведений у даному дослідженні, комплекс заходів протидії необхідно класифікувати за двома основними напрямами: технічні заходи (активна та пасивна протидія) та організаційні заходи (регламентація процесів та мінімізація наслідків) [55].

Технічні заходи протидії та виявлення атак

Технічна складова системи кіберстійкості базується на впровадженні спеціалізованих програмно-апаратних засобів, здатних функціонувати в режимі реального часу. Ключовим принципом тут виступає інтеграція різнорідних засобів захисту в єдиний контур управління інформаційною безпекою.

1. Системи виявлення та запобігання вторгненням (IDS/IPS)

Згідно з функціональною моделлю систем, системи IDS (Intrusion Detection System) та IPS (Intrusion Prevention System) відіграють роль першого рубежу активної оборони. Їхнє завдання полягає у безперервному аналізі мережевого трафіку для виявлення ознак несанкціонованого втручання.

Сигнатурний метод аналізу. Базовий рівень захисту забезпечується використанням сигнатурного методу. Він передбачає порівняння пакетів даних, що проходять через мережеві шлюзи, з базою даних відомих патернів атак (сигнатур). Це дозволяє з високою ефективністю блокувати відомі типи загроз, такі як сканування портів, спроби експлуатації відомих вразливостей операційних систем та протоколів, а також активність поширених шкідливих програм (хробаків, троянів). Важливою умовою ефективності є забезпечення механізму автоматичного оновлення баз сигнатур із довірених джерел.

Евристичний та поведінковий аналіз. Оскільки гібридні загрози часто використовують модифіковане шкідливе ПЗ або атаки «нульового дня» (Zero-day), сигнатурного аналізу недостатньо. Система IPS повинна використовувати алгоритми евристичного аналізу, які базуються на виявленні аномалій. До таких аномалій належать: нестандартна структура мережевих пакетів, нетипова

інтенсивність трафіку, спроби звернення до неавторизованих зовнішніх IP-адрес, використання нестандартних портів для передачі даних. Виявлення таких відхилень дозволяє блокувати атаку ще до того, як з’явиться відповідна сигнатура [56].

2. Системи управління інформаційною безпекою та подіями (SIEM)

Центральним елементом аналітичної підсистеми є SIEM-система (Security Information and Event Management). Її роль полягає в агрегації, нормалізації та кореляції даних про події безпеки, що надходять від усіх елементів інфраструктури: мережевого обладнання, серверів, робочих станцій, систем захисту (антивірусів, IDS/IPS) (рис. 3.3).

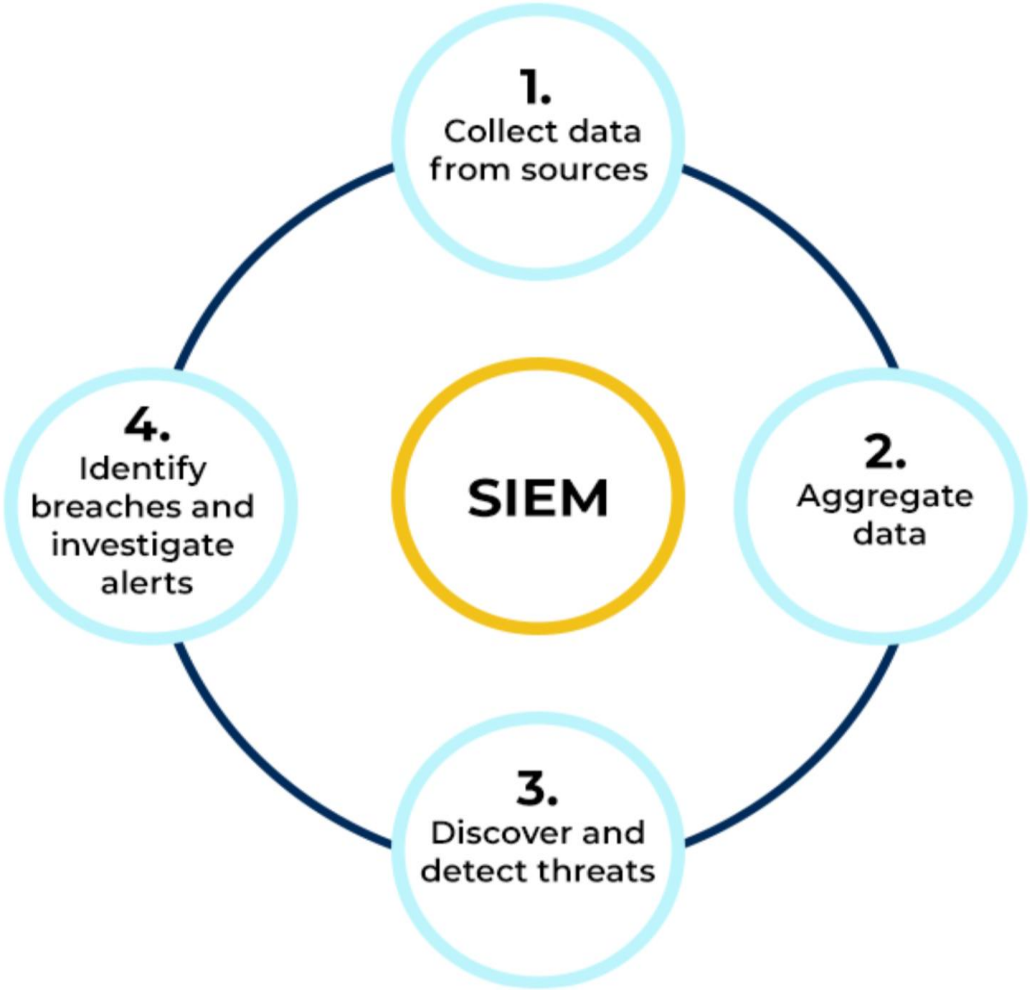

Рис. 3.3. Процес дії SIEM-системи

Функціонування SIEM-системи забезпечує реалізацію наступних критичних функцій:

– централізований збір логів. Система акумулює журнали подій у єдиному сховищі, що унеможливлює їх локальне видалення зловмисником на скомпрометованому вузлі з метою приховування слідів («замітання слідів»).

– кореляція подій. Це найбільш інтелектуальна функція SIEM. Система аналізує зв’язки між різними подіями, які окремо можуть виглядати безпечними, але в сукупності свідчать про складну атаку. Наприклад, SIEM може пов’язати подію фізичного проходу співробітника через турнікет (за даними СКУД) із подією входу в систему з його обліковим записом, але з іншої географічної локації або у нетиповий час. Така кореляція є індикатором компрометації облікових даних.

– пріоритезація інцидентів. В умовах великого потоку подій SIEM автоматично визначає рівень критичності кожного інциденту, дозволяючи операторам безпеки фокусувати увагу на найбільш небезпечних загрозах.

3. Захист від шкідливого програмного забезпечення

Враховуючи, що шкідливе ПЗ (віруси, програми-вимагачі, шпигунське ПЗ) є одним з основних інструментів гібридних атак, система захисту передбачає комплексне використання антивірусних засобів:

- антивірусний захист на шлюзах. Перевірка трафіку (WEB, Email) на наявність шкідливого коду до моменту його потрапляння у внутрішню мережу;
- захист кінцевих точок (Endpoint Protection). Встановлення агентів безпеки на робочі станції та сервери, які контролюють запуск процесів, перевіряють файлову систему та блокують підозрілу активність;
- «Пісочниці» (Sandboxing). Використання ізольованих середовищ для безпечного запуску та аналізу підозрілих файлів, отриманих з зовнішніх джерел, перед їх доставкою користувачеві (табл.3.2).

Таблиця 3.2

Матриця заходів протидії гібридним загрозам

Вектор загрози	**Технічні засоби протидії**	**Організаційні заходи**
Сканування та розвідка	IDS/IPS (блокування сканування), Honey-pots (пастки)	Приховування критичної інформації, моніторинг OSINT
Атаки на веб-додатки	WAF (фільтрація SQLi, XSS), аналіз логів веб-сервера	Регулярний аудит коду, контроль змін на сайті
Шкідливе ПЗ (віруси)	Антивірус/EDR, пісочниці (Sandbox), контроль додатків	Обмеження прав користувачів, заборона змінних носіїв
Соціальна інженерія	Фільтрація пошти (Anti-spam), маркування зовнішніх листів	Тренінги персоналу, тестові фішингові розсилки
Інсайдерські дії	DLP (контроль витоків), UEBA (аналіз поведінки), PAM	Угода про нерозголошення (NDA), контроль доступу

Організаційні заходи та регламентація процесів

Технічні засоби створюють інструментарій захисту, проте його ефективність напряму залежить від якості організаційних процесів. Як показано на Блок-схемі алгоритму роботи системи, реагування на загрози є чітко структурованим процесом.

1. Алгоритмізація дій при виявленні загрози

Згідно з розробленим алгоритмом, процес реагування поділяється на кілька послідовних етапів, кожен з яких має чіткі критерії переходу.

Етап моніторингу та детектування. Система перебуває в режимі постійного сканування. При виявленні події, що відповідає критеріям інциденту (наприклад, спрацювання сигнатури IDS), ініціюється процедура реагування.

Етап класифікації та сповіщення. Виявлена подія класифікується за типом загрози (наприклад, «DDoS-атака», «Спроба несанкціонованого доступу», «Шкідливе ПЗ»). На основі класифікації визначається коло осіб для сповіщення. Критично важливим є оперативне інформування керівництва та технічних спеціалістів.

Етап локалізації. Першочерговим завданням є не стільки розслідування, скільки припинення поширення загрози. Алгоритм передбачає автоматичне або

напівавтоматичне відключення уражених сегментів мережі, блокування облікових записів або зміну правил фільтрації трафіку.

Етап нейтралізації. Видалення компонентів загрози з системи (очищення від вірусів, закриття вразливостей, перевстановлення скомпрометованого ПЗ).

2. Забезпечення безперервності та мінімізація наслідків

Стратегія кіберстійкості виходить з того, що абсолютний захист неможливий, тому необхідно мінімізувати наслідки успішних атак.

Резервне копіювання (Backup). Регламент повинен передбачати регулярне створення резервних копій критично важливих даних, конфігурацій мережевого обладнання та налаштувань серверів. Копії повинні зберігатися у захищеному сховищі, фізично або логічно ізольованому від основної мережі, щоб уберегти їх від атак програм-вимагачів (Ransomware).

Плани відновлення (Disaster Recovery Plan). Розробка детальних інструкцій щодо відновлення працездатності систем після збоїв. План повинен містити чіткі часові нормативи відновлення (RTO) для кожного критичного сервісу.

Дублювання критичних вузлів. Забезпечення відмовостійкості за рахунок використання кластерних рішень, резервних каналів зв’язку та дублювання апаратних компонентів.

Таким чином, запропонований набір заходів формує ешелоновану систему захисту, де технічні засоби виявлення та блокування поєднуються з організаційними процедурами реагування та відновлення, що відповідає меті мінімізації ризиків та забезпечення безперервності функціонування об’єкта [57].

3.4. Апробація системи кіберстійкості критичної інфраструктури на реальному кейсі

В якості реального кейсу розглянемо українське енергетичне підприємство – регіональну електроенергетичну розподільчу компанію (обленерго), що відіграє ключову роль у критичній інфраструктурі країни. Це підприємство

забезпечує передачу та розподіл електроенергії до десятків тисяч споживачів у своєму регіоні, включаючи промислові об'єкти, лікарні, зв'язок та інші життєво важливі служби.

Відповідно до Закону України «Про критичну інфраструктуру» №1882-IX, такі оператори віднесені до критичної інфраструктури і зобов'язані забезпечувати захист своїх об'єктів, реагувати на інциденти та повідомляти уповноважені органи про них. Енергетика прямо включена до 17 життєво важливих секторів, порушення яких може завдати шкоди національній безпеці. Отже, на підприємство покладено особливу відповідальність за кібербезпеку та безперервність електропостачання.

Технологічна інфраструктура. Розподільча компанія експлуатує складну технологічну інфраструктуру, що поєднує інформаційні системи (IT) та промислові системи управління (OT/ICS). Корпоративна IT-мережа забезпечує офісні процеси, телекомунікації та взаємодію з зовнішніми мережами (Інтернет). OT-мережа включає автоматизовану систему диспетчерського управління та збору даних (SCADA/DMS), сервери та робочі станції оперативного персоналу, мережеві шлюзи та віддалені термінальні пристрої (RTU) на підстанціях.

IT та OT-сегменти мережі були розділені міжмережевими екранами (фаєрволами): один між корпоративною мережею і Інтернетом, другий – між IT і OT мережами. Така архітектура типова для енергетичних компаній: диспетчерський центр керує підстанціями через SCADA-сервери та шлюзи, що передають команди на комутаційне обладнання (високовольтні вимикачі тощо) у електричних підстанціях.

Кібератаки на українську енергетичну інфраструктуру (2015-2022)

Українські енергетичні компанії неодноразово ставали мішенню організованих кібератак, що дозволяє розглянути їх як реальний кейс для апробації принципів кіберстійкості. Найбільш резонансними і добре задокументованими є атака 2015 року (BlackEnergy) та атака 2022 року (Industroyer2). Ці інциденти продемонстрували як реальні загрози для критичної

інфраструктури, так і ефективність застосування запропонованих заходів захисту.

Атака 23 грудня 2015 року (BlackEnergy та KillDisk). Цей інцидент став першим у світі задокументованим випадком успішної кібератаки на електроенергетичну мережу, що призвела до відключення електропостачання для кінцевих споживачів. Атаку спрямували проти трьох регіональних розподільчих компаній в Україні, в результаті чого близько 230 тисяч споживачів тимчасово втратили електропостачання.

Хронологія атаки:

- Підготовча фаза (весна-літо 2015). Зловмисники провели ретельну розвідку, використовуючи фішингові листи для доставки шкідливого ПЗ BlackEnergy 3 на комп'ютери співробітників енергокомпаній. Фішинг був цілеспрямованим (spear-phishing): листи містили вкладення у вигляді документів Excel з макросами. Після відкриття такого документа макрос запускав завантаження троянського бекдору BlackEnergy на комп'ютер жертви.
- Закріплення (осінь 2015). Після початкового проникнення атакуючі використовували BlackEnergy для збору інформації про мережу, облікові записи та топологію систем. Фактично зловмисники близько пів року перебували в мережах компаній, збираючи дані та готуючись до фінальної атаки.
- Виконання атаки (23 грудня 2015, 15:30-16:00). У заздалегідь обраний час оператори зловмисників віддалено (за допомогою зламаних VPN-з'єднань та облікових записів) підключилися до SCADA-систем диспетчерських центрів. Вони вручну відкрили інтерфейс управління підстанціями і почали вимикати автоматичні вимикачі (circuit breakers), що призвело до знеструмлення десятків підстанцій. Паралельно зловмисники запустили шкідливе ПЗ KillDisk, яке знищувало дані на комп'ютерах (у тому числі на робочих станціях SCADA-операторів), ускладнюючи швидке відновлення.
- Додатковий деструктивний вплив. Атакуючі також провели DoS-атаку на телефонні лінії компанії (постійні дзвінки), щоб перешкодити споживачам зв'язатися з диспетчерською та повідомити про відключення. Це

демонструє комплексний характер атаки – не лише кіберскладова, а й інформаційно-психологічна (дезорганізація комунікацій).

Наслідки та відновлення. Більшість підстанцій довелося вмикати вручну на місці (оператори їздили на підстанції фізично), оскільки віддалене керування SCADA було порушене. Електропостачання було відновлено протягом декількох годин (за різними оцінками від 1 до 6 годин), але відновлення повної працездатності SCADA-систем та IT-інфраструктури зайняло тижні. Розслідування підтвердило, що атака була проведена організованою групою (яку приписують до APT-угруповання Sandworm, пов'язаного з іноземним державним спонсуванням).

Атака квітень 2022 року. Під час повномасштабної військової агресії проти України зловмисники здійснили повторну спробу кібератаки на енергосистему, використовуючи оновлену версію шкідливого ПЗ Industroyer (вперше застосованого у 2016 році). Мета – відключити електропостачання регіонів з населенням близько 2 мільйонів людей під час активних бойових дій, посиливши хаос та соціальну кризу.

На відміну від успіху 2015 року, атака 2022 року була виявлена та зупинена завчасно завдяки покращеному кіберзахисту енергетичних компаній та втручанню CERT-UA. Шкідливе ПЗ Industroyer2 було ідентифіковано в мережі однієї з енергокомпаній до того, як воно було активовано на виконання деструктивних дій. Компанія за підтримки кіберфахівців змогла локалізувати загрозу, ізолювати уражені системи та провести санацію мережі без масштабного відключення електропостачання.

Аналіз ефективності застосованих заходів кіберстійкості

Порівняння двох інцидентів – 2015 та 2022 років – дозволяє проаналізувати вплив запроваджених заходів кіберстійкості на здатність критичної інфраструктури протистояти кібератакам. У період між атаками українські енергокомпанії, за підтримки міжнародних партнерів та державних структур, суттєво посилили захист. Розглянемо ключові аспекти, що змінилися:

1. Покращена сегментація мережі та контроль доступу. Після атаки 2015 року підприємства впровадили глибшу сегментацію: ОТ-мережі були додатково розділені на зони (наприклад, окремі VLAN для критичних підстанцій), застосовано правило найменших привілеїв для облікових записів. Віддалений доступ до SCADA-систем обмежено застосуванням багатофакторної автентифікації (MFA) та VPN з посиленим шифруванням. У 2022 році це ускладнило зловмисникам горизонтальне переміщення по мережі – навіть маючи точку входу, вони не могли легко дістатися критичних компонентів ОТ.

2. Впровадження систем виявлення загроз (IDS/IPS для ОТ). До 2015 року багато енергокомпаній не мали спеціалізованого моніторингу для промислових мереж. Після інциденту стали впроваджуватися системи виявлення аномалій у ОТ-трафіку (ICS-IDS) та сигнатурні системи для виявлення відомого шкідливого ПЗ. Ці системи у 2022 році зафіксували підозрілу активність Industroyer2 ще на стадії підготовки до атаки, що дозволило вчасно відреагувати.

3. Підвищення кіберобізнаності персоналу. Фішинг був ключовим вектором проникнення в 2015 році. Після атаки енергокомпанії провели масштабні навчання співробітників з питань кібергігієни, розпізнавання фішингових листів, використання паролів та MFA. Це зменшило ризик успішного соціального інжинірингу у подальшому.

4. Регулярне резервне копіювання та плани відновлення. KillDisk у 2015 році знищив дані на багатьох робочих станціях, що затримало відновлення. Після цього підприємства почали робити регулярні офлайн-копії критичних конфігурацій SCADA та операційних систем, а також відпрацьовували сценарії аварійного відновлення (включаючи ручне керування підстанціями). У результаті, навіть якби атака 2022 року частково вдалася, відновлення відбулося б значно швидше.

5. Співпраця з CERT-UA та міжнародними партнерами. Після 2015 року Україна активно співпрацює з міжнародними експертами з кібербезпеки (зокрема США та ЄС) у сфері захисту критичної інфраструктури.

CERT-UA регулярно обмінюється інформацією про загрози з енергокомпаніями (індикатори компрометації, сигнатури). У 2022 році саме оперативний обмін даними дозволив швидко ідентифікувати та нейтралізувати Industroyer2.

Таблиця 3.3

Порівняльна таблиця результатів

Параметр	Атака 2015 (до заходів)	Атака 2022 (після заходів)
Результат атаки	Успішна, відключення ~230 тис. споживачів	Виявлена та зупинена, відключень не було
Час виявлення загрози	Після завдання збитків (постфактум)	До активації (проактивно)
Час відновлення	Декілька годин до діб	Не вимагалося (локалізація без збитків)
Використані вектори атаки	Фішинг, відсутність MFA, слабка сегментація	Спроба повторити, але заблоковано на етапі розгортання

Цей кейс наочно демонструє ефективність системного підходу до кіберстійкості. Застосування принципів Defense-in-Depth, Zero Trust, регулярне навчання персоналу та співпраця з CERT перетворили енергокомпанії з легкої мішені (2015) на стійку систему (2022), здатну витримати навіть цілеспрямовані атаки державного рівня під час війни.

3.5. Рекомендації щодо впровадження системного підходу на підприємствах критичної інфраструктури

На основі теоретичного аналізу міжнародних стандартів, емпіричних спостережень під час апробації та висновків із реальних кіберінцидентів розроблено практичні рекомендації для підприємств критичної інфраструктури України щодо побудови комплексної системи кіберстійкості. Рекомендації охоплюють організаційні, технічні, нормативно-правові та міжнародні аспекти, які взаємно доповнюють один одного у формуванні цілісної кіберостійкої екосистеми [58].

Організаційно-управлінські заходи

На організаційному рівні критично важливим є забезпечення належного управління та розпорядження ресурсами у сфері кібербезпеки. Рекомендується призначення на рівні вищого керівництва окремої посади Директора з

інформаційної безпеки (Chief Information Security Officer, CISO), або в разі недостатності розміру організації, делегування цих обов'язків компетентній особі з гарантованим прямим доступом до топ-менеджменту та виділенням окремої кошторисної статті для реалізації заходів кібербезпеки. У випадку малих та середніх підприємств, де функціонування окремої позиції CISO може бути неекономічним, можна залучати зовнішніх консультантів на постійній або проектній основі, однак відповідальність за стан кібербезпеки має бути чітко визначена та закріплена в організаційних документах [59].

Невіддільним компонентом організаційної структури кіберзахисту є створення команди швидкого реагування на інциденти (Computer Security Incident Response Team, CSIRT), що може функціонувати як на рівні окремого підприємства, так і на рівні галузі. Склад такої команди повинен охоплювати фахівців з інформаційної безпеки, інженерів промислової автоматизації, юристів та фахівців з корпоративних комунікацій. Періодичне проведення табл-топ вправ та практичних сценаріїв реагування на інцидент дозволяє команді знаходитися у постійній готовності та оптимізувати процедури. Окрім того, на постійній основі, не рідше одного разу на рік, повинна проводитися комплексна оцінка кіберризиків з використанням визнаних методологій, таких як NIST SP 800-30 або ISO 27005, що дозволяє вчасно виявляти нові вразливості та адаптувати стратегію захисту до змінюється ландшафту загроз.

Підвищення культури кібербезпеки у організації передбачає впровадження обов'язкових щорічних програм навчання всього персоналу, а не лише спеціалістів IT-відділу. Такі програми повинні охоплювати питання розпізнавання фішингових атак, безпечного керування паролями, правил використання багатофакторної автентифікації та процедур звітування про підозрілу діяльність. Для критичного персоналу, такого як оператори диспетчерських центрів та адміністратори промислових систем, необхідне розширене спеціалізоване навчання, присвячене особливостям захисту OT-середовища та процедурам реагування на сценарії компрометації.

Технічна архітектура та засоби захисту

З технічної точки зору, мінімальне базове вимога для критичної інфраструктури полягає у реалізації багаторівневої архітектури захисту (Defense-

in-Depth) з відхідом від традиційної моделі периметрального захисту. Це включає розділення внутрішніх мереж на чітко визначені функціональні зони (демілітаризована зона DMZ для публічних сервісів, корпоративна IT-мережа для офісних функцій, промислова OT-мережа для систем управління, та критичні підсистеми у максимально ізольованому стані), з суворим контролем трафіку між зонами на рівні мережевих шлюзів та міжмережевих екранів. Кожна межа між зонами повинна охоронятися не лише статичним фаєрволом, але й активною системою виявлення та запобігання вторгненням (IPS), здатною розпізнавати як сигнатури відомих атак, так і аномалії у поведінці трафіку [60].

Для критичної інфраструктури, особливо для промислових систем управління, науково обґрунтованим є постійний перехід до парадигми нульової довіри (Zero Trust), що принципово змінює припущення про безпеку. Замість вкладення довіри у периметр мережі, модель Zero Trust вимагає безперервної верифікації кожної комунікації, користувача та пристрою. Це передбачає обов'язкове запровадження багатофакторної автентифікації для всіх доступів до критичних систем та інформаційних ресурсів, мікросегментацію OT-мереж таким чином, щоб критичні пристрої (наприклад, RT на розподільчих підстанціях) могли комунікувати виняткова з авторизованими вузлами управління, та впровадження безперервного моніторингу та аудиту дій користувачів та пристроїв (Continuous Authentication and Authorization).

Специфіка промислових систем управління (ICS/SCADA) вимагає особливої уваги. Рекомендується фізична або логічна ізоляція SCADA-мереж від корпоративної мережі та Інтернету (застосування принципу air-gap або встановлення прикордонного фаєрволу з крайніми обмеженнями на обмін), впровадження спеціалізованих систем моніторингу для промислових протоколів (ICS-IDS), які розпізнають аномалії у командах Modbus, DNP3, IEC 60870-5-104 та інших специфічних для промислової автоматизації протоколів. Для OT-середовища доцільно запровадити whitelist-підхід до дозволу програмного забезпечення, де дозволено функціонування виняткова явно санкціонованих та перевірених програм, а будь-які відхилення автоматично блокуються. Крім того, управління уразливостями в OT-сегменті вимагає регулярного оновлення

прошивок та програмного забезпечення промислового обладнання, однак таке оновлення повинно попередньо тестуватися у ізольованому тестовому середовищі, щоб запобігти порушенню критичних процесів у виробничому середовищі.

Стратегія резервного копіювання та аварійного відновлення має бути розроблена та послідовно дотримуватися як на політичному, так і на технічному рівні. Критичні дані, конфігурації SCADA та параметри автоматизованих систем повинні копіюватися щоденно з гарантією офлайн-збереження на фізично ізольованих або криптографічно захищених носіях, недоступних для шкідливого ПЗ типу Ransomware. План відновлення після кіберінциденту має визначати чітко прослідковувані цільові показники часу відновлення (RTO) та точки відновлення (RPO) для кожної критичної послуги. Регулярне (щоквартальне) тестування процедур відновлення з резервних копій є не формальною процедурою, а істотною частиною перевірки їхньої придатності та актуальності [61].

Непідаючи значення централізованому моніторингу, рекомендується впровадження системи управління інформацією та подіями безпеки (SIEM – Security Information and Event Management), яка акумулює логи та алерти з усіх критичних компонентів інфраструктури: міжмережевих екранів, серверів, робочих станцій, промислових контролерів, систем виявлення вторгнень. Накопичені дані піддаються кореляційному аналізу для виявлення складних багатоетапних атак, що не проявляються у окремих логах. При цьому самі логи повинні зберігатися у захищеному сховищі, недоступному для видалення навіть адміністраторами скомпрометованих систем, щоб гарантувати неспростовність доказів під час розслідування інцидентів.

Нормативно-правовий та міжнародний контекст

На нормативно-правовому рівні підприємства критичної інфраструктури мають дотримуватися вимог Закону України «Про критичну інфраструктуру» та супутніх підзаконних актів, видаданих Кабінетом Міністрів та Держспецзв'язком. Ці документи вимагають розробки та затвердження План захисту критичної інфраструктури від кібератак, що має містити комплекс організаційних та технічних заходів, графік їх впровадження та механізми оцінки

ефективності. Крім того, вимагається проведення обов'язкових аудитів кібербезпеки та звітування про виявлені інциденти до уповноважених органів та CERT-UA у встановлені строки.

З метою підвищення якості захисту та отримання визнання на міжнародному рівні, підприємствам доцільно прагнути сертифікації за загальновизнаними стандартами. Для корпоративної IT-інфраструктури актуальною є сертифікація ISO/IEC 27001 (Системи управління інформаційною безпекою), що встановлює вимоги до організації процесів та контролів у сфері захисту інформації. Для OT/ICS-компоненти більш релевантним є стандарт IEC 62443 (Промислова кібербезпека), розроблений міжнародною комісією ISA (International Society of Automation), який специфічно розглядає архітектурні та функціональні аспекти захисту промислових автоматизованих систем. При розробці та впровадженні програми кіберстійкості доцільно використовувати NIST Cybersecurity Framework як методологічне підґрунтя, оскільки CSF забезпечує одночасно гнучкість у адаптації до локальних умов та загальновизнану структуру категорій та функцій (Identify, Protect, Detect, Respond, Recover).

На міжнародному рівні Україна має доступ до програм технічної допомоги та підтримки від Сполучених Штатів, Європейського Союзу та інших партнерів у сфері захисту критичної інфраструктури. Рекомендується активне залучення міжнародних експертів для проведення незалежних аудитів безпеки та пентестування, участь у спільних вправах та тренуваннях, організованих НАТО чи інституціями ЄС, та систематичний обмін найкращими практиками з іноземними колегами. Налагодження оперативної взаємодії з CERT-UA та одержання оперативних інформацій про нові або розвиваються загрози у режимі реального часу є критичним для забезпечення переважного виявлення атак. Можливість залучення передових технологій, таких як системи на основі штучного інтелекту для виявлення аномалій у мережевому трафіку та поведінці користувачів, здатні істотно підвищити можливості виявлення складних атак на ранніх етапах.

Насамкінець, забезпечення дійсної кіберстійкості вимагає культурної трансформації на всіх рівнях організації. Керівництво підприємства повинне демонструвати явну прихильність до питань безпеки через виділення достатніх ресурсів, схвалення інвестицій у кіберзахист та розповсюджування повідомлень про важливість безпеки. Створення середовища, де працівники відчувають та розуміють вплив своїх дій на безпеку системи, та де виявлення потенційних уразливостей заохочується, а не карається, сприяє формуванню екосистеми, у якій кібербезпека є спільною відповідальністю всіх учасників організації, а не прерогативою окремого IT-підрозділу [62].

Висновки до розділу 3

У третьому розділі досліджено програмно-технічні засоби запобігання та протидії загрозам мережевій безпеці підприємства, що дозволило узагальнити їхню роль у формуванні комплексної системи захисту інформаційних ресурсів.

Встановлено, що превентивні заходи мережевої безпеки, зокрема фізичний захист інфраструктури, контроль доступу до мережевих компонентів та управління активами, є необхідною умовою зниження ризику несанкціонованого доступу, пошкодження або виведення з ладу мережевих систем. Реалізація таких заходів сприяє ранньому виявленню потенційних загроз і забезпечує стабільність функціонування мережі.

Показано, що технічні засоби мережевого захисту, зокрема міжмережеві екрани, системи виявлення вторгнень (IDS) та системи запобігання вторгненням (IPS), відіграють ключову роль у протидії зовнішнім і внутрішнім загрозам. Їх застосування дозволяє здійснювати моніторинг мережевого трафіку, своєчасно виявляти аномальну активність і автоматично реагувати на спроби атак, що істотно підвищує рівень захищеності корпоративної мережі.

Дослідження засвідчило, що впровадження систем управління інформацією та подіями безпеки (SIEM) забезпечує централізований збір, кореляцію та аналіз подій безпеки з різних джерел. Це дозволяє підвищити

ефективність виявлення складних атак, скоротити час реагування на інциденти та покращити процеси управління інформаційною безпекою підприємства.

Виявлено, що планування безперервності бізнесу та аварійного відновлення (BCP/DRP) є важливим елементом забезпечення мережевої безпеки, оскільки дозволяє мінімізувати наслідки інцидентів та забезпечити відновлення критичних сервісів у встановлені часові межі. Регулярне тестування та актуалізація відповідних планів підвищує готовність організації до надзвичайних ситуацій і сприяє зменшенню потенційних збитків.

Розроблено системну модель забезпечення кіберстійкості критичних об’єктів із урахуванням гібридних загроз. Запропоновано комплекс заходів та методів протидії гібридним загрозам, що підвищують ефективність кіберзахисту.

Отже, результати третього розділу підтверджують, що ефективна протидія загрозам мережевій безпеці можлива лише за умови комплексного використання програмно-технічних засобів, організаційних заходів і механізмів управління безперервністю. Поєднання превентивного захисту, засобів виявлення та реагування на інциденти, а також планування відновлення забезпечує формування цілісної системи мережевої безпеки підприємства.

ВИСНОВКИ

У ході дослідження обґрунтовано та систематизовано теоретико-методологічні засади системного підходу до забезпечення кіберстійкості, яка розглядається як інтегральна властивість складної соціотехнічної системи. Встановлено, що кіберстійкість формується на основі принципів цілісності, ієрархічності, інтеграції компонентів, адаптивності та наявності механізмів зворотного зв'язку. Показано, що традиційні фрагментарні та реактивні підходи до кібербезпеки не забезпечують належного рівня захисту в умовах сучасних гібридних загроз, які характеризуються багатовекторністю та синхронізацією атак у різних доменах. Доведено, що застосування системного підходу забезпечує комплексне охоплення всіх аспектів безпеки та підвищує адаптивність системи до нових викликів.

На основі проведеного аналізу розроблено та описано архітектуру системи кіберстійкості, побудовану з урахуванням концепцій багаторівневої оборони (Defense-in-Depth) та нульової довіри (Zero Trust), адаптовану до специфіки функціонування підприємств критичної інфраструктури України. Встановлено, що запропонована архітектура враховує конвергенцію IT- та OT-компонентів і передбачає застосування мікросегментації мереж, спеціалізованих засобів моніторингу промислових систем управління, автоматизованих механізмів виявлення аномалій та реагування на інциденти, а також комплексу організаційних заходів, спрямованих на забезпечення безперервності надання критичних послуг.

У процесі дослідження проведено апробацію запропонованого підходу на прикладі аналізу реальних кіберінцидентів, що мали місце в енергетичному секторі України у 2015 та 2022 роках. Компаративний аналіз засвідчив підвищення здатності організацій протистояти кібератакам державного рівня за умов системного впровадження заходів кіберстійкості. Встановлено, що у 2022 році атака, здійснена з використанням інструментів, аналогічних тим, що застосовувалися у 2015 році, була своєчасно виявлена та локалізована, що

дозволило запобігти масштабним порушенням функціонування критичної інфраструктури.

За результатами дослідження сформульовано комплекс практичних рекомендацій щодо побудови системи кіберстійкості для підприємств критичної інфраструктури. Рекомендації охоплюють організаційні, технічні, нормативно-правові та міжнародні аспекти забезпечення кіберзахисту й орієнтовані на поетапне впровадження з урахуванням ресурсних та організаційних обмежень українських підприємств. Водночас запропоновані підходи створюють підґрунтя для досягнення рівня захисту, що відповідає провідним міжнародним стандартам у сфері кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовтня 2017 р. № 2163-VIII [Електронний ресурс]. – URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 02.11.2025).

2. Іванюта С. П. Критична інфраструктура: підходи до визначення та захисту [Електронний ресурс]. – URL: https://web.archive.org/web/20171031162449/http://www.niss.gov.ua/content/articles/files/KI_-Ivanyuta-3a331.pdf (дата звернення: 02.11.2025).

3. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовтня 2017 р. № 2163-VIII. Стаття 1. Визначення термінів [Електронний ресурс]. – URL: https://protocol.ua/ua/pro_osnovni_zasadi_zabezpe_vid_05_10_2017_2163_viii_stattya_1/ (дата звернення: 02.11.2025).

4. Russia’s cyberattacks and election interference [Електронний ресурс] // *The Washington Post*. – 2020. – URL: https://www.washingtonpost.com/national-security/russia-cyberattacks-election-interference/2020/10/19/51a84208-1208-11eb-bc10-40b25382f1be_story.html (дата звернення: 08.11.2025).

5. Хакерська атака Росії на українську енергосистему [Електронний ресурс] // *Texty.org.ua*. – URL: https://web.archive.org/web/20220225152407/https://texty.org.ua/articles/66125/ (дата звернення: 08.11.2025).

6. Greenberg A. The NotPetya cyberattack [Електронний ресурс] // *Wired*. – 2018. – URL: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (дата звернення: 08.11.2025).

7. Як хакери змогли зламати 70 урядових сайтів України [Електронний ресурс] // *Liga.Tech*. – URL: https://web.archive.org/web/20220116001943/https://tech.liga.net/ua/ukraine/article/

kak-hakery-smogli-vzlomat-70-pravitelstvennyh-saytov-i-kto-za-etim-mojet-stoyat (дата звернення: 08.11.2025).

8. Кібератака на Укрзалізницю [Електронний ресурс] // *Укрінформ*. – URL: https://www.ukrinform.ua/rubric-society/3977123-kiberataka-na-ukrzaliznicu-u-derzspeczvazku-kazut-so-buli-vikoristani-taktiki-specsluzb-rf.html (дата звернення: 08.11.2025).

9. Що таке гібридні загрози [Електронний ресурс] // *BBC Ukrainian*. – URL: https://www.bbc.com/ukrainian/articles/cz92xrkklwro (дата звернення: 08.11.2025).

10. TACS-23 Conference Proceedings [Електронний ресурс]. – URL: https://is.ipt.kpi.ua/pdf/TACS-23.pdf (дата звернення: 11.11.2025).

11. Cyber resilience vs cybersecurity [Електронний ресурс] // *AirIAM*. – URL: https://airiam.com/blog/cyber-resilience-vs-cybersecurity/ (дата звернення: 02.11.2025).

12. Cyber resiliency: preparing for and mitigating the inevitable [Електронний ресурс] // *TestPros*. – URL: https://testpros.com/cybersecurity/cyber-resiliency-preparing-for-and-mitigating-the-inevitable/ (дата звернення: 02.11.2025).

13. Cyber resilience in the EU financial sector [Електронний ресурс] // *European Commission*. – URL: https://finance.ec.europa.eu/digital-finance/cyber-resilience_en (дата звернення: 05.11.2025).

14. Україна та практичний приклад кіберстійкості [Електронний ресурс] // *InDevLab*. – URL: https://indevlab.com/uk/blog-ua/ukrayina-ta-praktichnij-priklad-kiber-stijkosti (дата звернення: 11.11.2025).

15. Countering hybrid threats [Електронний ресурс] // *NATO*. – URL: https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats (дата звернення: 05.11.2025).

16. Hybrid threats [Електронний ресурс] // *Council of the European Union*. – URL: https://www.consilium.europa.eu/en/policies/hybrid-threats/ (дата звернення: 05.11.2025).

17. Hybrid threats as a phenomenon [Електронний ресурс] // *Hybrid CoE*. – URL: https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/ (дата звернення: 05.11.2025).

18. The role of deepfakes in malign influence campaigns [Електронний ресурс] // *NATO StratCom COE*. – URL: https://stratcomcoe.org/publications/the-role-of-deepfakes-in-malign-influence-campaigns/72 (дата звернення: 11.11.2025).

19. EU policy on fighting hybrid threats [Електронний ресурс] // *CCDCOE*. – URL: https://ccdcoe.org/incyder-articles/eu-policy-on-fighting-hybrid-threats/ (дата звернення: 05.11.2025).

20. Cyber extortion vs ransomware [Електронний ресурс] // *ConsultNet*. – URL: https://www.consultnetinc.com/cyber-extortion-vs-ransomware-their-difference-explained (дата звернення: 11.11.2025).

21. Cyber threats overview [Електронний ресурс] // *ENISA*. – URL: https://www.enisa.europa.eu/topics/cyber-threats (дата звернення: 05.11.2025).

22. NIST Cybersecurity Framework (CSF) [Електронний ресурс] // *Strata*. – URL: https://www.strata.io/glossary/nist-cybersecurity-framework-csf/ (дата звернення: 02.11.2025).

23. NIST SP 800-53 compliance explained [Електронний ресурс] // *Titania*. – URL: https://www.titania.com/resources/guides/nist-sp-800-53-compliance-explained-how-to-be-compliant (дата звернення: 02.11.2025).

24. ISO/IEC 27032 explained [Електронний ресурс] // *DataGuard*. – URL: https://www.dataguard.com/blog/iso-27032/ (дата звернення: 02.11.2025).

25. Digital Operational Resilience Act (DORA) [Електронний ресурс] // *IBM*. – URL: https://www.ibm.com/think/topics/digital-operational-resilience-act (дата звернення: 11.11.2025).

26. Critical Entities Resilience Directive (CER) [Електронний ресурс] // *UpGuard*. – URL: https://www.upguard.com/blog/cer-directive (дата звернення: 05.11.2025).

27. ENISA risk management [Електронний ресурс] // *UpGuard*. – URL: https://www.upguard.com/blog/enisa-risk-management (дата звернення: 05.11.2025).

28. Cyber resiliency and the risk management framework [Електронний ресурс]. – MITRE, 2021. – URL: https://www.mitre.org/sites/default/files/2021-08/pr-16-0776-cyber-resiliency-and-the-risk-management-framework.pdf (дата звернення: 11.11.2025).

29. ISO/IEC 27005 risk management [Електронний ресурс] // *IT Governance*. – URL: https://www.itgovernanceusa.com/cyber-security-solutions/iso27001/iso-27005 (дата звернення: 02.11.2025).

30. ISO 31000 risk management [Електронний ресурс] // *Riskonnect*. – URL: https://riskonnect.com/business-continuity-resilience/the-basics-of-iso-31000-risk-management/ (дата звернення: 02.11.2025).

31. How to implement NIST SP 800-30 [Електронний ресурс] // *SaltyCloud*. – URL: https://www.saltycloud.com/blog/how-to-implement-nist-800-30/ (дата звернення: 14.11.2025).

32. Risk management standards [Електронний ресурс] // *ENISA*. – URL: https://www.enisa.europa.eu/sites/default/files/publications/O.7.2-T2-Risk_Management_standards.pdf (дата звернення: 05.11.2025).

33. Risk heat map [Електронний ресурс] // *TechTarget*. – URL: https://www.techtarget.com/searchsecurity/definition/risk-map-risk-heat-map (дата звернення: 14.11.2025).

34. Cyber risk quantification methods [Електронний ресурс] // *Scrut.io*. – URL: https://www.scrut.io/post/how-to-select-the-right-cyber-risk-quantification-method (дата звернення: 14.11.2025).

35. Operational technology risk management [Електронний ресурс] // *Hexagon*. – URL: https://aliresources.hexagon.com/cybersecurity/operational-technology-risk-management-safeguarding-critical-infrastructure-in-the-digital-age (дата звернення: 14.11.2025).

36. Cyber stress testing handbook [Електронний ресурс] // *Industrial Cyber*. – URL: https://industrialcyber.co/reports/enisa-releases-cyber-stress-testing-handbook-to-boost-critical-infrastructure-resilience-under-nis2-directive/ (дата звернення: 08.11.2025).

37. SIEM explained [Електронний ресурс] // *Splunk*. – URL: https://www.splunk.com/en_us/blog/learn/siem-security-information-event-management.html (дата звернення: 18.11.2025).

38. SIEM solutions overview [Електронний ресурс] // *SentinelOne*. – URL: https://www.sentinelone.com/cybersecurity-101/data-and-ai/siem-solutions/ (дата звернення: 18.11.2025).

39. SOC roles and responsibilities [Електронний ресурс] // *Palo Alto Networks*. – URL: https://www.paloaltonetworks.com/cyberpedia/soc-roles-and-responsibilities (дата звернення: 18.11.2025).

40. NIST incident response [Електронний ресурс] // *Cynet*. – URL: https://www.cynet.com/incident-response/nist-incident-response/ (дата звернення: 18.11.2025).

41. Threat intelligence overview [Електронний ресурс] // *CrowdStrike*. – URL: https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/ (дата звернення: 18.11.2025).

42. Types of threat intelligence [Електронний ресурс] // *ZeroFox*. – URL: https://www.zerofox.com/blog/types-of-threat-intelligence/ (дата звернення: 18.11.2025).

43. Telco SIEM framework [Електронний ресурс] // *Cisco*. – URL: https://www.cisco.com/c/en/us/products/collateral/security/telco-siem-framework-wp.html (дата звернення: 18.11.2025).

44. Cyber resilience research [Електронний ресурс] // *MDPI*. – 2025. – URL: https://www.mdpi.com/2078-2489/16/7/515 (дата звернення: 22.11.2025).

45. AI in disinformation detection [Електронний ресурс] // *ACIG Journal*. – URL: https://www.acigjournal.com/AI-in-Disinformation-Detection,200200,0,2.html (дата звернення: 22.11.2025).

46. Системний підхід до управління [Електронний ресурс]. – URL: https://mfppp.ru/news/fond/sistemnyy-podkhod-k-upravleniyu/ (дата звернення: 22.11.2025).

47. Система забезпечення кібербезпеки: сутність та призначення [Електронний ресурс]. – URL: https://goal-int.org/sistema-zabezpechennya-kiberbezpeki-sutnist-ta-priznachennya/ (дата звернення: 22.11.2025).

48. Cyber protection and cyber resilience [Електронний ресурс] // *EMSopedia*. – URL: https://www.emsopedia.org/entries/cyber-protection-cyber-resilience/ (дата звернення: 22.11.2025).

49. NIST Cybersecurity Framework [Електронний ресурс]. – NIST, 2018. – URL: https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf (дата звернення: 11.11.2025).

50. Cyber resilience analysis [Електронний ресурс] // *SCIRP*. – URL: https://www.scirp.org/journal/paperinformation?paperid=134422 (дата звернення: 22.11.2025).

51. Методичні рекомендації з кіберзахисту [Електронний ресурс] // *Державна служба спеціального зв'язку та захисту інформації України*. – URL: https://cip.gov.ua/services/cm/api/attachment/download?id=60293 (дата звернення: 14.11.2025).

52. Defense in depth [Електронний ресурс] // *Cloudflare*. – URL: https://www.cloudflare.com/learning/security/glossary/what-is-defense-in-depth/ (дата звернення: 14.11.2025).

53. Cybersecurity of critical infrastructure with ICS/SCADA systems [Електронний ресурс] // *IEEE*. – URL: https://publicsafety.ieee.org/topics/cybersecurity-of-critical-infrastructure-with-ics-scada-systems/ (дата звернення: 14.11.2025).

54. Faisandier A. *Systems Architecture and Design*. – Belberaud : Sinergy'Com, 2012. – 312 с.

55. Zones and Conduits [Електронний ресурс]. – URL: https://jaatun.no/papers/2024/Zones-and-Conduits.pdf (дата звернення: 22.11.2025).

56. Purdue model for ICS security [Електронний ресурс] // *Palo Alto Networks*. – URL: https://www.paloaltonetworks.com/cyberpedia/what-is-the-purdue-model-for-ics-security (дата звернення: 22.11.2025).

57. Cybersecurity in Industrial IoT [Електронний ресурс] // *Communications of the ACM*. – URL: https://cacm.acm.org/blogcacm/cybersecurity-in-industrial-iot-protecting-critical-infrastructure/ (дата звернення: 22.11.2025).

58. IoT infrastructure components [Електронний ресурс] // *FloLive*. – URL: https://flolive.net/blog/glossary/iot-infrastructure-6-key-components-and-practical-applications/ (дата звернення: 22.11.2025).

59. Defending critical infrastructure [Електронний ресурс]. – Hybrid CoE, 2022. – URL: https://www.hybridcoe.fi/wp-content/uploads/2022/06/20220602-Hybrid-CoE-Working-Paper-18-Defending-critical-infrastructure-WEB.pdf (дата звернення: 11.11.2025).

60. ISO/IEC 27032 overview [Електронний ресурс] // *DataGuard*. – URL: https://www.dataguard.com/blog/iso-27032/ (дата звернення: 22.11.2025).